Preserving the integrity of CBRN forensic samples is administratively and logistically burdensome.—Kaszeta

The Forensic Challenge

By Dan Kaszeta

The suspected use of chemical, biological, radiological, and nuclear (CBRN) weapons or materials adds complexity to any international or internal conflict. It is critical that responses to such use are based on good information. The relatively new field of CBRN forensics, which is emerging out of domestic terrorism investigations, seeks to establish scientific facts through analysis of rigorously collected evidence. CBRN forensics are important to establishing actual facts, but are inherently difficult for a variety of reasons. The question of whether military forces, particularly Special Operations Forces (SOF), can conduct CBRN forensics in an adequate fashion is debatable; however, there are numerous pathways to improve the status quo.

Why CBRN Forensics Matter

In their traditional setting the forensic sciences provide the government and the populace a degree of confidence that the courts are making informed decisions based on all available information. The notion that forensics are solely for legal processes and not relevant or important outside the courtroom, however, does not withstand serious scrutiny. The scientific and procedural aspects of CBRN forensics are important in the context of international security. Were CBRN materials used? If so, was their use deliberate, accidental, or some kind of natural phenomenon? Confirmed acts of CBRN warfare might be used as justification to drop a bomb or wage war on another country. Even the suspected use of CBRN weapons or materials adds complexity to any international or internal conflict. Not every CBRN incident is obvious or discernable from natural phenomena. When deployed soldiers turn up in the field hospital with injuries from exposure to toxic industrial chemicals, this could be an indicator of hostile attack. Alternatively, they could have been exposed to toxic waste or contaminated debris from a chemical factory that had been damaged earlier in the conflict. Skyrocketing radiation counts on detection instruments could mean a "dirty bomb" has been detonated. But it is equally possible that an old commercial or medical radiological source has been encountered.

CBRN forensics also help to identify provenance (where did the bad stuff come from?) and attribution (who did it?). This is especially important for distinguishing state action from that of non-state actors, or non-state actors who are state proxies. Terrorists might develop an indigenous capability—e.g. the Aum

The Managing Director at Strongpoint Security, Mr. Dan Kaszeta previously served as a physical security specialist with the U.S. Secret Service and as a disaster preparedness advisor to the White House Military Office.

Shinrikyo cult sarin attacks in Japan in 1995—or acquire abandoned munitions—e.g. Islamic State of Iraq and the Levant seizure of Saddam-era munitions. Provenance may also help to identify state proxies, as was likely the case in early 2017 with the assassination of North Korean leader Kim Jong Un's estranged half-brother in a Malaysian airport with the nerve agent VX.

Confirmation, attribution, and provenance help to calibrate judicial, policy, and operational responses. Use of chemical and biological weapons is against international law. Prosecution of war crimes and acts of terrorism should occur wherever possible if the rule of law and international norms are to be maintained. Justice requires trials; prosecution requires evidence. The collection, preservation, and analysis of physical evidence must offer a high-degree of assurance so that the prosecutor can defend the evidence.

Imagine a SOF team that visits ten different buildings and collects samples of material from each during a two-day operation. Trace evidence of anthrax from one of the buildings is subsequently used to prosecute a terrorist. A wise defense attorney will question whether the SOF operators changed their gloves and boots between buildings. Were they sterile when the operators entered the building? How can you prove it? What about the bag they put the sample into? Was it clean? Did they take that empty bag to the other buildings? If these simple questions are not answered satisfactorily, there is no way to prove the anthrax came from the building in question or from a different building or location previously visited by the SOF team. Perhaps the team has detained the wrong person. Or if they got the right person, charges may not stick because the evidence has been discarded.

CBRN forensics must also be ironclad to combat alternative narratives, fake news, propaganda, and conspiracy theories. Every instance of real or alleged use of CBRN materials in recent years has led to allegations, alternative explanations ranging from the plausible to the esoteric, denials, and conspiracy theories. Perpetrators of such attacks have every incentive to muddy the waters and sow discord in order to create doubt and allow for deniability. One need only look at the well-documented miasma of stories and opposing narratives that have surrounded each use of sarin nerve agent in the war in Syria to see how this can look.[1] Sowing diverse stories is a tactic in information warfare and serves various ends, such as diluting public support for armed conflict or reducing morale. Even the seemingly clear-cut case last year in Khan Sheikhoun, Syria wherein a bomb filled with nerve agent fell out of the sky in a conflict where only one side has airpower, spawned an amazing array of alternative explanations.

Hard facts are needed to refute alternative explanations. As one of the expected effects of CBRN warfare is psychological, military commanders may have to explain what is going on to their unit, in order to preserve morale. If military personnel start to believe conspiracy theories and myths, it will tax morale and discipline. Commanders armed with solid information in which they have confidence are better placed to combat this threat.

CBRN forensics also have important implications for force protection. Knowledge of the physical characteristics of the CBRN materials actually used in attacks will allow defense measures that are based on practical first-hand knowledge rather than generic guidelines. For example, artillery shells filled with a nerve agent may be poorly designed and destroy much of their contents, and many of the shells are duds, and therefore do not disseminate the nerve agent. Therefore, the hazard area associated with such an artillery strike will be much smaller than the generic warning template in a manual that was written during the Cold War and assumes a high degree of munition efficiency. In practical terms, this means a much smaller hazard zone on

the commander's map and more mobility options as there are fewer areas to be avoided. But this is the sort of information that requires knowledgeable forensic analysis, with someone actually looking at the site of an artillery strike and assessing the impact craters and fragments of the shells.

CBRN Forensics is Challenging

The CBRN forensic discipline is difficult for environmental, technical, procedural, and organizational reasons. First, the nature of CBRN materials is such that the environments where they are present are inherently dangerous. Forensic operations must be performed while wearing protective clothing and respiratory protection commensurate with the threat, which if previously unknown, first requires an initial survey or reconnaissance to characterize the threat environment before detailed work can even begin.

"Time versus safety" is a paradox inherent in CBRN forensics. Much of the evidence at the crime scene is either fragile or short-lived. Gas and vapor can waft away without leaving a trace. Liquids can evaporate or react with the environment; for example, the nerve agent sarin is a liquid that can quickly evaporate from a liquid into a vapor and blow away with the wind. Powders, such as spores, can blow away. And sunlight can destroy bacteria and viruses. The bodies and clothing of victims may also contain evidence that is degraded by life-saving decontamination procedures.

Each CBRN material requires different sample collection techniques. Sample categories can be broadly divided into gas and vapor; liquid; and solid, which includes soil, surface trace, and biomedical as subcategories. It is not always obvious where a gas or vapor might reside since some are lighter than air. Liquid and solid sampling are relatively straightforward conceptually, but sampling while wearing cumbersome protective gear or conducting the operation in the wind or on the water can be a challenge. Additionally, trace samples are usually taken with wipes or swabs, which can require numerous different techniques and solvents, depending on the nature of the surface and material being tested. Biomedical samples—e.g. body fluid, hair, and tissue—are taken from live or deceased hosts, which is inherently complex. Samples from dead animals and body fluid samples from surviving victims have been probative in investigations in Syria.

CBRN forensics also requires the collection of conventional evidence. In many scenarios, this evidence will be more useful than the actual CBRN materials. For example, documents and fingerprints collected from a suspected clandestine laboratory may have far more investigative or intelligence value than a vial of a chemical warfare agent precursor compound. The explosive components of a "dirty bomb" may prove to have evidence value, post-detonation.

Preserving the integrity of all samples is administratively and logistically burdensome. Used and unused sample tools and containers need to be sterilized, documented, and analyzed. Protective gear must be changed frequently—a technician can use 50 pairs of gloves in one day—and the gear must be disposed of, treated as evidence, or cleaned before reuse to reduce the threat of cross-contamination.

Conventional evidence that may be contaminated by CBRN materials is problematic. A laboratory that can process chemical warfare materials may not be suited to collect fingerprints from a bottle, or exploit a smartphone, and vice versa. The laboratory that can exploit a laptop or mobile phone is not likely to be able to do so if the item is contaminated, or even suspected to be contaminated. This conundrum is poorly resolved in most parts of the world.

Finally, CBRN expertise and capabilities reside in disparate organizations. In many parts of the world, CBRN response is a fire department function, very similar to responses to industrial and commercial hazardous materials accidents. Fire services are

indeed well-equipped for most aspects of CBRN response; however, apart from arson investigation, fire departments do not collect forensic evidence.[2] In the United States, much of our expertise resides in clandestine narcotics law enforcement teams and environmental regulatory agencies that pursue criminal and regulatory enforcement of pollution and toxic waste rules. State and local law enforcement (and indeed most other countries) have very limited capability for CBRN forensics, for which the National Guard only recently started to develop and provide military support to civil authorities. There is the real question as to whether the level of care and precision required for CBRN forensics can reasonably be expected in a non-permissive environment, such as an active conflict zone.

CBRN Forensics in the Military Environment

CBRN forensics barely fits into the classic military CBRN mission set, which includes contamination avoidance (detection, hazard area prediction, warning, and reporting), individual protection (suits, gloves, and boots), collective protection, decontamination (of people and equipment), reconnaissance, and medical countermeasures. Military CBRN protective equipment is designed to keep the soldier in the fight for days or weeks, not for rapid changes of garments and gloves upon every entry and exit from a contaminated building. Conventional CBRN units, such as the U.S. Army Chemical Corps, are not equipped or trained for evidence collection to a forensic standard.[3] Soldiers are issued one, perhaps two sets of gloves—far short of the 20 or more required in an evidence collection mission. Additionally, military decontamination is all about "good enough" and not about "sterilized to a legal standard" for evidence collection. When is the last time, if ever, a soldier sterilized a tool (shovel) in the field? Military detection equipment is designed to provide rapid warning to military personnel, not for the collection of samples in sterile containers. CBRN reconnaissance is focused on finding the extent of contamination and checking if routes and axes of advance are safe, rather than the painstaking work of evidence collection.

The Defense Department recently gave the U.S. Special Operations Command (USSOCOM) more responsibilities in countering weapons of mass destruction, a term that generally implies all of the CBRN threats. However, CBRN forensics run contrary to key SOF axioms. CBRN forensics are slow, heavy, and manpower-intensive, while special operations generally are fast, light, and emphasize economy of force.[4] It is one thing to send in a small team to enter a house and seize a prisoner and a few laptops. Such a mission might be accomplished in minutes. If the same house had been a suspected clandestine laboratory, a thorough forensic exploitation might last a day or longer and require five times the personnel, as well as several cargo pallets of equipment.

Additionally, while domestic law enforcement operations that collect CBRN evidence may be an hour or two from the laboratory that will process the evidence, SOF often operate at some distance from their support. The transport of prohibited substances (potentially found on corpses) across international boundaries presents moral and legal issues. Also, any chain of custody document for a covert operation is likely to be highly classified and will never see a courtroom. Such evidence could still be made available to policymakers, but they will be in the position of telling the public to "trust us, but we cannot show you the paperwork"—that could help to promulgate the very propaganda, fake news, and conspiracy theories that CBRN forensics aim to combat.[5]

The Way Forward

If CBRN forensics are to be done, they need to be done well or not at all. An effort that is performed at an 80 percent standard might as well not have been

undertaken. Evidence that is tainted, cross-contaminated, spoiled, or mishandled could support erroneous conclusions.

There is no insurmountable reason why military forces, and especially SOF, could not conduct CBRN evidence collection. As a first step, military doctrine should express a requirement for forensic operations. CBRN forensic evidence collection will otherwise remain in the unfunded requirement or "nice to do" category and SOF units will not prioritize CBRN training.

Competent military CBRN specialists and SOF operators could easily be trained in CBRN forensics. Specialty courses offer the necessary skills and already exist within the civilian sector, but the military needs to commit to sending its personnel through this kind of training. Another way to bridge the expertise gap is to embed law enforcement or regulatory personnel within SOF. This likely will raise a host of other concerns, but might still be easier (and more effective) than the alternative of trying to turn SOF operators into CBRN forensic technicians.

Similarly, while existing military gear is indeed largely inadequate to the task of CBRN forensics, adapting existing forensic equipment to a military environment is certainly feasible. This has been done extensively in the realm of counter–improvised explosive device operations and biometrics, and there is no technical barrier to adapting the wide variety of commercial off-the-shelf equipment for SOF operations.

Traditional forensic labs need to be equipped with CBRN capabilities and traditional evidence collection technicians need to learn how to operate in a CBRN environment. There is no fundamental technical obstacle preventing the development of CBRN forensics laboratories that can be moved closer to the samples. Mobile CBRN laboratories already exist, albeit not specifically for forensic analysis. The skills and equipment exist. Training is available. The key issue is putting capabilities together into specialized teams and training and exercising these teams so that they can achieve competence. SOF have the justified reputation for quickly adapting to new missions and integrating new technologies into their operations, so adapting to CBRN forensics should not be too far a stretch, as long as command emphasis is given to it. PRISM

Notes

[1] George Monbiot "A Lesson from Syria: It's Crucial Not to Fuel Far-Right Conspiracy Theories," *The Guardian*, November 17, 2017, available at <https://www.theguardian.com/commentisfree/2017/nov/15/lesson-from-syria-chemical-weapons-conspiracy-theories-alt-right>.

[2] The author has seen training exercises where valuable evidence was literally flushed down the drains by firefighters.

[3] There are pockets of competence, however, including the U.S. Army's Technical Escort unit. Comparable capabilities in other militaries are exceedingly rare. As a disclaimer, the author cannot categorically state that there are or are not specialized units within USSOCOM or the Intelligence Community that are already well-trained for CBRN forensics, given the secretive nature of this line of business. There may be special teams unbeknown to the author because of secrecy and classification. If there are, then the United States is ahead of the curve and has taken the advice of this article already. The author's own experience is that these capabilities barely exist with some of the United States' European allies. CBRN forensics was never mentioned during the author's Chemical Corps training in the early 1990s.

[4] A colleague at the U.S. Secret Service had been a noncommissioned CBRN officer with a Special Forces group. CBRN protective equipment was often at the very bottom of the priority list for missions. Where the load is heavy and every ounce counts, and speed is of the essence, masks, suits, and gloves got left behind. And if you habitually leave it behind, training with it will not be a high priority.

[5] Critics and conspiracy theorists have criticized the apparent lack of chain of custody in the Syrian sarin investigations, although the Organization for the Prohibition of Chemical Weapons clearly did the best that they could under the circumstances.

Photos

Page 84: Stock photo ID:479256460