CBRN Forensics

Forensics in a contaminated environment

Supported by GIFT Forensics
The World’s Only Manufacturer of BSL-3 Mobile Laboratories
Hugh Gregg, head of the Organization for the Prohibition of Chemical Weapons (OPCW) laboratory

The Merriam-Webster dictionary defines forensic as ‘relating to the use of scientific knowledge or methods in solving crimes.’ The well-developed field of forensics becomes considerably more challenging when additional hazards, such as chemical, biological, radiological or nuclear are present at the scene of an investigation. Protecting first responders from these hazards is a priority, as is preservation of the evidence. Awareness, training and tools are key elements for safe, successful outcomes.

Awareness that additional hazards may be present beyond what can be seen is the first step. This new journal will aid in raising the awareness of the additional risks of working in a CBRN environment. Training in a variety of scenarios will increase the capabilities and confidence of the first responders and forensic investigators in responding safely. Finally, tools, in the form of hardware - technology such as sensors, protective equipment, etc. - and procedures are needed to ensure the preservation of evidence while protecting the investigators.

The procedures and processes used in handling CBRN contaminated evidence need to be carefully thought out and implemented. Decontaminating an item may lead to loss of the forensic evidence necessary for the investigation. Additionally, information from the CBRN agent may, itself, be a key part of the investigation. This aspect of CBRN forensics has been, and is being researched to different degrees. Using the Chemical Abstracts Service’s SciFinder tool, searching for nuclear forensics returns 426 articles, while microbial forensics or biological forensics returns a total of 143 and chemical forensics returns only 11. Clearly, RN forensics is far ahead of CB forensics.

In 2015, the International Atomic Energy Agency, issued revision 1 of the implementation guide Nuclear Forensics in Support of Investigation. The authors state: “Nuclear forensic examinations have been successfully applied to a number of reported cases involving the illicit trafficking of high enriched uranium and plutonium, as well as events involving nuclear and other radioactive material out of regulatory control.”

Microbial forensics has come a long way in the past two decades. In the 2001 anthrax attacks in the US (the Amerithrax case), DNA fingerprinting proved fairly early that it was the Ames strain. Complete genome sequencing over the next few years enabled the FBI in 2008 to conclude that the anthrax used in 2001 all originated from a single flask of material.

In 2014, the National Academies Press published Science Needs for Microbial Forensics: Developing Initial International Research Priorities. This documented noted: "...that, at the time of the anthrax letters mailings, the tools and technologies that were readily available were not adequate and the science of microbial forensics was in its infancy and limited to a few pioneering laboratories." The document also highlights the need for this to be an international collaboration with both reference collections and accessible databases.

Where does this leave chemical forensics? A limited amount of research has been carried out and plans are underway for more research. A fourth symposium on chemical forensics will be held at the Spring 2017 American Chemical Society National Meeting. While there exists no international research effort on chemical forensics at this time, chemical production techniques have been used to attempt to determine attribution.

The third report of the OPCW - UN Joint Investigative Mechanism (24 August 2016) includes the following text: “Multiple sources suggested that the sulphur mustard in question was undistilled and had been generated through the Levinstein process. According to them, the bad smell (rotten eggs) and colour of the substance (dark green/blue) were consistent with sulphur mustard used by ISIL in other incidents … Some sources provided information that indicated that ISIL had the capacity to produce sulphur mustard through the Levinstein chemical reaction process. [The OPCW] confirmed that the sulphur mustard from the Syrian Arab Republic did not contain impurities such as polysulphides, meaning that a different process was used by the government. The OPCW also reported that the sulphur mustard used by ISIL in northern Iraq on several occasions in 2015 and 2016 was produced through the Levinstein process. ... There is not sufficient information available to draw conclusions on the origin of the sulphur mustard used during this incident.”

I look forward to more research on chemical forensics, and wish the new journal success!
Contents

1 Foreword

4 Welcome to GIFT

5 – 7 Meet the Team

8 – 9 Future dreaming
Ed van Zalen and Peter de Bruyn, from the Netherlands Forensic Institute on what the future holds

10 – 11 Gift wrapped
Ed van Zalen talks to Claudine Weeks on the GIFT legacy

12 – 13 A good sniff
Eric Moore, from Tyndall University, on some of the GIFT chemical detectors

14 – 17 Common approach path
Dr Jason Bannan, from the FBI Laboratory, on the genesis of CBRN forensics

18 Out of the darkness
Johan Sand, from STUK, on stand off alpha detection

19 – 20 The Searchers
Daan Noort, from TNO, on their work to improve forensic chemical detection

21 – 24 Theatre night
Adrien Sivignon, from CONSTOX, on pre-Bataclan developments in French forensics

25 – 26 Risky Business
Peter Den Outer, RIVM, and Govert Verstappen, NFI, on the need for a CBRN forensics risk assessment tool

27 – 29 CSI UK!
Karl Harrison, from Cranfield University, on the UK’s response to CBRN incidents

30 – 31 Analyse This!
Michael Madden, from Analyse IQ, on chemometrics in forensic analysis

32 – 35 Habsburg Hazmat
Gunter Povoden talks to Claudine Weeks about Austrian military forensics

36 – 37 Team effort
Lt. Col Martel and Katleen de Meulenaere on Belgian military forensics

38 – 41 CSI2
Dr Randall Murch on the blueprint for a CBRN forensics capability

42 – 43 Mind the Gap
The gaps in European CBRN forensics

44 – 46 Dangerous Clues
Steve Johnson on forensics, SIBCRA and WIT

47 Light fantastic
Silvia Lopez on the GIFT differential mobility analyser

48 Send for the fun police!
Iris Huis in ’t Veld at Eticas Research & Consulting on ethics in CBRN forensics
The successful interrogation of evidence, either at a crime scene contaminated with chemical, biological, radiological or nuclear (CBRN) agents, or of the agents themselves back at the lab, is an absolutely vital part of CBRN defence.

At present forensic investigation is hampered by a lack of protocols and training in carrying out forensic analysis on CBRN contaminated materials.

The generic integrated forensic toolbox for CBRN incidents, or GIFT CBRN, consortium, funded under the European commission’s seventh framework programme, is designed to close up the many gaps inherent in this complex area and provide an integrated law enforcement CBRN capability that is world class.

The GIFT consortium is developing the most advanced forensic toolbox for CBRN incidents in the world. Through the cooperation of Europe-wide research agencies, first responders, industrialists and subject matter experts, the toolbox will provide enhanced capability in three key areas of CBRN forensics:

- Procedures, sampling methods and detection of CBRN agents at the crime scene.
- Traditional forensic laboratory methods for dealing with contaminated evidence.
- Laboratory methods for profiling CBRN agents released at an incident.

The GIFT consortium will address the issue of conducting forensic analysis in a contaminated environment by developing novel methodologies and technologies which will enable forensic investigators to perform enhanced analysis at the CBRN crime scene. Some of the key innovations being explored are:

- Novel sensors for chemical and biological agents.
- Detection of alpha-emitting particles using UV.
- Development of decontamination methods that won’t impact on forensic traces.
- Micro-analytics on-chip to detect agents of interest.
- Attribution signatures for chemical, biological and radiological agents.
- An education and training curriculum.

In order to facilitate this work, the project has been broken down into specific work package areas, each led by a partner agency, with cross package working and cooperation as a key fundamental for success. The nine work packages are:

WP1: The management work package. Keeping the entire consortium on track and liaising with the commission, among other things.
WP2: Composed of threat assessments, gap analysis and toolbox design. It aims to define the forensics community’s needs, to allow identification of what must happen to allow responders to perform their tasks safely, quickly and properly.
WP3: Two central themes, one being the development of protocols for use in the crime scene; the other is the development of investigative methods for when the evidence is contaminated with chemical, biological or radiological agents.
WP4: Development of procedures and methodologies to enable traditional forensic science (DNA, fingerprint and electronic devices) to be performed on CBRN contaminated exhibits.
WP5: Looking at the CBRN agent itself, whether we can further develop analytical procedures on the agent and also whether we can identify signatures in the agent that could lead to methods of production and where key elements originated from.
WP6: Integration of the forensic toolbox, ensuring all the technologies can work together.
WP7: Validation and testing of the procedures and methods developed in WP3, 4 and 5.
WP8: Assessing the legal, ethical and societal aspects of the project in order to provide stakeholders with the appropriate guidance to avoid any negative impact during the project, execution or in an eventual future deployment based in this research.
WP9: Dissemination – this will create a CBRN forensics community that will be able to help guide and validate the whole project.

The Consortium
The consortium consists of 21 partners, from nine different European countries.

The NFI – The Netherlands
TNO – The Netherlands
M’L – UK
FERA – UK
STUK – Finland
NFC – Sweden
NICC – Belgium
Space Applications – Belgium
CEA – France
RAMEM – Spain
Nanobiz – Turkey

Tyndall University – Ireland
RIVM – The Netherlands
Falcon Communications – UK
AWE – UK
FOI – Sweden
Analyze IQ – Ireland
RMA – Belgium
JRC-ITU – Spain
Eticas – Spain
LGC – Spain
Meet the team

The consortium consists of 21 partners, from nine different European countries

The National Forensics Institute – The Netherlands
The Netherlands Forensic Institute (NFI) is one of the world’s leading forensic laboratories. It invests heavily in research and development to lay the foundations for innovative forensic methods and technologies that will play an important role in the coming decades. The NFI also maintains close relationships with industry, knowledge institutes and universities.

Tyndall National Institute, University College Cork – Ireland
The Tyndall National Institute is one of Europe’s leading centres for information, communications and technology (ICT) research. It is the largest facility of its kind in Ireland with 450 staff, students and academic and industrial visiting researchers. Tyndall’s research is guided by, and applied to, finding solutions that can be commercialised to meet the needs of society in communications, energy, environment and health through the development of new technology in the fields of photonics, micro/nano-electronics and microsystems.

TNO – The Netherlands
The Netherlands Organisation for applied scientific research (TNO) was founded in 1932 to enable business and government to apply knowledge. TNO is an independent research organisation focusing on five social themes:
• Industry - from economic stagnation to growth in high-technology industry.
• Healthy living - from illness and treatment to health and behaviour.
• Defence, safety and security - from a wide range of threats to controllable risks.
• Urbanisation – from urbanisation bottlenecks to urban vitality.
• Energy - from conventional sources to sustainable energy systems.

RIVM – The Netherlands
The Dutch National Institute for Public Health and the Environment (RIVM) carries out independent research and provides policy advice to help government authorities keep people and the environment healthy. RIVM works to prevent and control outbreaks of infectious diseases by promoting public health and consumer safety, and helps to protect the quality of the environment.

M’L – UK
A photonics technology company which designs and manufactures award winning lasers and photonics systems, and collaborates with research institutions and industries around the world to help develop new light-based applications that can make a positive difference.

Falcon Communications – UK
Falcon Communications publishes CBRNe World magazine serving the information needs of professionals around the world charged with planning for or responding to chemical, biological, radiological, nuclear or explosives (CBRNe) threats or incidents. Falcon also produces the world-leading CBRNE Convergence events globally as well as a leading CBRNE product directory.

FERA – UK
This company has been at the forefront of the UK nuclear deterrence programme for more than 60 years. AWE's outstanding nuclear skills and expertise means that it is able to provide intelligence and support to the UK government by developing innovative solutions to combat nuclear threats, terrorism and nuclear proliferation. AWE is recognised as a centre of scientific, engineering and technological excellence, equipped with some of the most advanced research, design and production facilities in the world.

STUK – Finland
Finland’s Radiation and Nuclear Safety Authority (STUK) operates under the country’s Ministry of Social Affairs and Health with the purpose of preventing and limiting the adverse effects of radiation, controlling the safety of the use of radiation and nuclear energy, and engaging in associated research, education and communications. It employs around 320 people, of whom just over 80% hold MSc or MA degrees.

FOI – Sweden
FOI is one of Europe’s leading research institutes in defence and security. It has 930 employees with various backgrounds – from physicists, chemists, engineers, social scientists, mathematicians and philosophers to lawyers, economists and IT technicians. FOI has expertise in many fields of application, such as security policy studies and analyses of defence and security, assessments of various types of threats, systems for crisis leadership and management, protection against and management of hazardous substances, IT security and the opportunities provided by new sensors.
Meet the team

**NFC – Sweden**
The Swedish National Forensic Centre (NFC) is one of Europe’s leading forensic laboratories with cutting-edge expertise. It was established as an independent expert organisation within the police authority with an overall responsibility for forensics and has 1,100 employees. The NFC performs forensic research and development, education and training, and analyses for incidents involving CBRNE materials.

**Analyze IQ – Ireland**
Analyze IQ Limited develops and sells an innovative, patent protected software suite for analysis of the composition of mixtures, based on molecular spectroscopy data. Analyze IQ uses a new model-driven paradigm for spectral data analysis, with proprietary new machine learning techniques specifically designed for spectral analysis, that is both quicker and more accurate than traditional analysis, and can be used by non-chemometrists in the field. The products have applications in fields as diverse as manufacturing inspection, law enforcement, emergency services, and the pharmaceutical industry.

**NICC – Belgium**
The National Institute of Criminalistics and Criminology (NICC) was founded in 1992 as part of the Ministry of Justice. With around 142 staff including 34 reporting forensic experts, its fields of expertise include: drugs and toxicology; analytical chemistry; paint, glass and safety ink; fire and volatiles; fibres and textiles; gunpowder; ballistics and digital information; mechanical ballistics and national database of ballistics; biology and genetics.

**RMA – Belgium**
The Royal Military Academy is a military higher education institution in charge of the academic, military and physical training of the officers of the Belgian armed forces.

**Space Applications – Belgium**
Space Applications Services is an independent Belgian company which aims to research and develop innovative systems, solutions and products, and provide services to the aerospace and security markets, and related industries. The company has a strong focus on research and development with partners across Europe, the US and the Russian Federation.
JRC-ITU – Spain
As the European Commission’s science and knowledge service, the Joint Research Centre’s mission is to support EU policies with independent evidence throughout the whole policy cycle. Its work has a direct impact on the lives of citizens by contributing with its research outcomes to a healthy and safe environment, secure energy supplies, sustainable mobility and consumer health and safety.

CEA – France
The French Alternative Energies and Atomic Energy Commission (CEA) is a key player in research, development and innovation in four main areas: defence and security; nuclear energy (fission and fusion); technological research for industry; and fundamental research in the physical sciences and life sciences.

Eticas – Spain
Ethics Research & Consulting works on the social, ethical and legal impact of security policies, innovation and technological development, as well as the interaction between changing social values, the possibilities of engineering systems and fundamental rights.

RAMEM – Spain
RAMEM focuses on the design and manufacture of mechanical and electromechanical equipment. RAMEM is backed by experience and technology acquired over 55 years of activity, and has over 40 engineers, doctors, graduates and technicians.

LQC – Spain
LQC sl manufactures radiation monitor and alarm equipment for military, police, airports, state borders and other sectors.

Nanobiz – Turkey
NANObiz Ltd is a technology company that emerged from the Middle East Technical University (METU) in Ankara. NANObiz’s team currently comprises 30 qualified researchers, academicians, engineers and administrative staff. The company has products and R&D operations in CBRN and homeland security; nanobiotechnology; biotechnology and other areas.
Picture the futuristic CBRN crime scene... People in sharp suits gather round a large screen looking at the 3D scan of the crime scene broadcast live to their control centre. To the left of the screen is a complete analysis of all the sensor data which has been collected by the artificial intelligence robotic system and was despatched immediately. The collected data was sent through to an automatic analysis system and the results are now being presented straight back into the command centre. The command team has a 360 visual view of the entire crime scene, along with clear identification of the location and the types of agents within the scene, without going anywhere near it.

Forensic teams now use the data and the images, following questions from the investigative authority, to assess where the best evidence might be, and where to look for fingerprints, DNA or other trace material to try to catch the perpetrators but also to identify used CBRN agent that might have been released during the incident. They then send in a robot optimised to lift latent fingerprints from the contaminated material, and to collect DNA, without suffering any contamination issues, and without having to move any materials from the scene. DNA test results are immediately generated through a lab-on-a-chip expert system, based on the DNA-profile the perpetrators are identified from a crime database and their details are passed to the investigative authority and local police. The perpetrators are arrested and all the evidence is securely and electronically processed and stored so there is no potential for discrepancy once the court case is ready. The security of the evidence is not in doubt, and experts are happy that it is safe from any breach, including a cyber attack.

Too good to be true?
Only time will tell – but that's the ambitious vision for CBRNE forensics in the very long term future. Currently, members of the generic integrated forensic toolbox (GIFT) consortium are exploring some of these new technologies, (sadly no robots just yet), to take that key first step towards enabling more work to be done at the crime scene, rather than having to transport everything to the laboratory. Work Package 2, for example, was tasked with assessing the needs of CBRNE forensics for the near future – many of which will have solutions thanks to the work of the consortium – and to predict what may be needed to counteract as yet unknown threats for the longer term.
Peter de Bruyn and Ed Van Zalen, from the Netherlands Forensic Institute, on the future of CBRN forensics

Throughout the EU member states, and also the development of more advanced capabilities within a few member states.

Countries with advanced capabilities should be able to deliver operational support to those member states with less advanced core capabilities.

Developments should be aimed at developing both a basic forensic response for the contaminated crime scene throughout Europe and on international collaborations. The latter need to be supported by the necessary arrangements and conditions to make that support feasible.

Contributing CBRN forensic experts should be prepared to work under different judicial systems (eg with respect to chain of custody or giving testimony). A high capability response will be more professionally developed (eg validated, supported by sophisticated technology and systems, etc) and the basic response will be broadened and better substantiated.

What about ensuring chain of custody?

Forensic activities in the hot zone, still rather ad hoc or improvised for the near future, will be further developed into professional, integrated and harmonised processes with validated guidelines and procedures.

It is always crucial to make arrangements for a guaranteed chain of custody for forensic evidence and data gathered from sensors and detection equipment at the crime scene. Due to safety constraints it is important to select and prioritise forensic activities in the hot zone; establishing which exhibits and forensic traces are being investigated onsite and which are being collected or sampled for laboratory investigation.

Priorities in the forensic investigation will therefore focus on the identity and role of related individuals (eg perpetrators, makers and other potential actors); this includes, for example, the investigation of fingerprints, DNA, digital data and the provenance of CBRN materials used in an attack.

These investigations are important not only for finding the responsible individuals and for preventing other attacks, but also for providing the prosecutors and judges with forensic evidence in court.

Technology and technological applications in general, and in the IT area in particular, can be expected to develop dramatically. This will definitely influence future forensic investigation capabilities.

And the key differences, longer term?

While most of the information might still be available as separate (electronic) documents in five years’ time, in 15 years the information should be accessible through expert systems and actions taken with the aid of decision support systems.

This will mean that the decisions made during the investigation process will be substantiated, validated and traceable, improving the quality of the case in court.

Detection and identification techniques will shift from the laboratory to the field, eg through miniaturisation and lab-on-a-chip technology. Individually applicable detection capabilities, from the near future, will be developed over time into more holistic remote/robotic sensors in the far future.

Some forensic characterisation and individualisation methods will still be too complex and sophisticated for field application and will need to be done in a laboratory, albeit with new tools and techniques.

Trends are emerging in the application of forensic investigation to CBRN crimes. At first the focus will be on developing forensic capabilities at existing CBRN labs and on decontamination of exhibits for investigation at traditional forensic laboratories. In the long term the emphasis will be more and more on performing forensic investigations and analyses at the crime scene/hot zone.

Advantages and developments should be taken from innovations in other scientific areas eg medical science, where experiments with remote surgery are already ongoing. This has the potential to lead to remote operation of unmanned (robotic) systems at a CBRN crime scene by forensic experts from a safe command centre.

The main advantages of these developments will be a faster, better and safer delivery of results for the criminal investigation under the required conditions (eg chain of custody, quality assurance).

Profiling methods for CBRN agents – for provenance and comparison – and the development of supporting forensic reference databases will also be developed.

Furthermore individualisation methods should be adapted to contaminated materials.

Finally, a European network for CBRN forensics should be developed over the years. This should evolve from an informal network in the near future into a well organised and structured official CBRN forensic network, under the responsibility of the European Commission and supported by the European Network of Forensic Science Institutes.
The GIFT that goes on giving

Ed Van Zalen, GIFT programme manager, talks to Claudine Weeks about the need for GIFT and the difference it will make to CBRN forensics

EVZ: Forensic investigators are always looking for ways to improve and develop their work and techniques but often when I meet traditional forensics colleagues they are all following the same path.

That’s what excited me about the opportunities with the generic integrated forensic toolbox (GIFT) consortium – we are working with small and medium sized enterprises (SMEs) and researchers outside the forensics field to see where new and innovative technologies can be applied to the niche world of CBRN forensics.

There are lots of ways we can improve and learn and by looking beyond our sector we can make sure we are keeping up to date and moving forward. In the GIFT consortium we are now working together with colleagues from a whole variety of industries to help take CBRN forensics to the next level.

CW: So what does that next level look like?
EVZ: We need to be able to do far more at the crime scene – more measuring and recording safely at the crime scene so that the laboratory is left with the high end work to do.

This is one of the most exciting parts of GIFT. We are working to create new equipment and protocols to bring more of the laboratory work safely out in the field.

GIFT researchers are developing on-scene technologies, methods and instruments so we don’t have to take so many materials back to the labs, as well as looking at ways to carry out traditional forensics on the contaminated materials.

We want to develop new and innovative technologies such as robotics and more automated techniques which can be used within contaminated crime scenes, allowing us to do more on the scene with less risk to our staff.

CW: So why is there a need for this now?
EVZ: At the Netherlands Forensics Institute (NFI) we have been running CBRN forensics as a specialism since 2003, largely as a reaction post 9/11. We started out just looking at how we could react to threats that might occur, but from 2008 we moved to consider other kinds of incidents where CBRN agents might also be released and how we can identify and characterise them.

So while the institute has been running a CBRN forensics programme since 2008, it wasn’t until 2012 that we could clearly see the need to extend this across Europe; to grow the learning, share what we have been working on with other countries and extend our knowledge further. That is what led to GIFT.

CW: So what will GIFT ultimately deliver for European CBRN forensics?
EVZ: GIFT is just one step, after this project is completed, the work will continue and we will be seeking for funding for further research and development.

The challenge for Europe is that not every country has the same CBRN forensic capabilities available. My aim for GIFT is that we use it to set a gold standard across Europe and raise the bar so that every country is able to develop a minimum core capability for CBRN forensics.

I would like to see a network whereby all advanced capability countries partner with...
the other countries and work together across the continent on training and education.

**CW: What would this network look like?**

**EVZ:** My dream would be to see the creation of a joint European centre of excellence in CBRN forensics, set up with some of the GIFT consortium partners.

This centre would be the main point for training, research and innovation in the field, across the whole of Europe. We would bring together all the techniques for working at the crime scene, which are being looked at as part of GIFT, and train and offer them to all countries in Europe through this centre of excellence.

The centre could then provide very high specification laboratory work to support countries without the capabilities themselves. It would deal with high end case work and support innovation, training and education, and research and development in CBRN forensics for all EU countries.

**CW: Why is education and training so important?**

**EVZ:** GIFT explores new procedures, technologies and techniques which will enable us to carry out traditional forensics in very difficult circumstances, either through decontamination or through containment processes. Clearly it will be very important for anyone involved to be trained in how to carry out these processes.

That's why as part of GIFT, we will be running exercises and using these to develop a curriculum, an education and training programme to help support the roll out of the toolbox across the EU. The toolbox will provide the procedures, protocols and equipment all in one place, for the first time ever, setting a world-class standard, so we need to train people to use them.

I would also like to see cross training for first responders and forensic specialists in the CBRN field so we can understand each other's roles better and work more effectively together at a crime scene. Generally, the two streams are separate at an incident. The priority for the safety stream, who are the first responders, is to rescue people and make the place safe again, while the security stream, who are the investigators, want to prosecute the perpetrators.

I want to bring the safety and security streams together, to work in partnership and understand each other's roles. If we understand each other and we train together, then responders could use some of our equipment in the early stages to help shape their initial response and we can use the information they gather to help shape our investigations.

Within GIFT the aim of the toolbox is that it will connect with existing and future technologies so future developments in the programme could include sensors and technology for first responders, which then link through to the forensics team, but this is a very long term cooperation goal.
The software story
Tyndall National Institute, University College Cork in Ireland has several roles within the GIFT consortium. As the scientific lead for the consortium, one of my main roles in the GIFT project is to ensure that the science and technology being developed is on track and aligned to the objectives of the project. Obviously this is vitally important generally, but in terms of the GIFT project it is essential that we can demonstrate proof of principle, as our final forensic toolbox will successfully provide the teams who are making decisions on the ground at a CBRN forensic scene, with all the information they need.

The aim of the GIFT consortium is to develop a gold standard for CBRN forensics, through technology, protocols and procedures and make the processes at the scene quicker and more efficient.

Tyndall leads work package 6 (WP6), the toolbox part, to make sure all the technology is integrated and ultimately works together.

The institute is creating new knowledge that will contribute to the overall forensic toolbox with a particular focus on the integration of sensors and detectors to provide real time information on chemical analysis. These technologies will also contribute to new methods to ensure the safety, security and chain of custody for that data throughout the process. We are also working with partners on an information hub. This will facilitate best practice in terms of operating procedures and protocols, so that everyone across Europe can tackle a CBRN forensic scene in the same way.

GIFT will be creating the toolbox with all the elements for detection, analysis and information, which will enable anyone at the scene to make informed decisions about key actions to take or how to approach the scene. It’s about having the right information at the right time.

We are developing specialised sensors and detectors for CBRN forensics and the idea is that the software element of the toolbox will be able to connect with both existing technology and the new technologies being developed within the GIFT project.

It is expected that existing and future CBRN forensic teams will see the GIFT toolbox as a fundamental part of their kit. It augments what they have already, provides an easier way of doing risk assessment, suggests future capability roadmaps and also acts as a starting basis for newcomers that might want to understand how to sample efficiently. It also needs to be flexible enough to connect with future technologies.

We are mixing past, current and future generation capabilities to create a flexible and adaptable CBRN forensics toolbox. It is not meant to be a static delivery; it will evolve over time as current databases are augmented with new information. We are going to prove the value of a truly integrated system. This is not about reinventing the wheel but truly doing something important for forensic scientists.

Our project team at Tyndall is helping to increase the efficiency of response, to make the process quicker. The information provided by analysis of the sensors and detectors will mean that people understand what they are dealing with faster and can take appropriate action quicker. The protocols and guidance from the information hub will inform people how and when to deal with the situation, for example, what personal protective equipment (PPE) to wear and how to treat those exposed.

For all data going into the toolbox, every element will be logged, date-stamped and only accessible by those who require it, supporting the chain of custody for all potential court case evidence.

The Tyndall National Institute also has key competences that specialise in creating miniaturised systems for a wide variety of end users. I am the Principal Investigator of the Sensing and Separation group, we focus on miniaturised integrated sensing for the end user. We are using that technology and sensors expertise in WP3 to explore ways of improve CBRN forensics at the crime scene.

We will be developing a new chemical sensor for detecting nerve agents in liquid form. The instruments currently used for onsite chemical speculation do not have sufficient sensitivity or resolving power, or both, and therefore have a very high false alarm rate or are too selective and only detect a certain family of compounds. Such instruments include ion mobility spectrometers, Fourier transform infrared spectroscopy, photo-ionisation detection and flame photometric detection.

There is a need for complementary technologies that can be used for onsite detection of chemicals that enable preliminary testing to be done at the crime scene:

- Micro total analysis system (μTAS) devices that will enable flow through miniaturised capillary electrophoresis (CE).
- Chemical sensors that can be used to provide a chemical profile in the development of a robust and extendible portable sensing platform.
- Molecular sensors for the disclosure of chemical agents on surfaces.
- Associated software for all the sensing technologies.

We have been developing a custom-made capability by integrating a commercially available contactless conductivity detector (C4D), a printed circuit board (PCB), copper sensing electrodes and a hybrid polydimethylsiloxane/glass microchip. The microchip sits on the PCB and four platinum electrodes are located into four wells. This microchip system is being developed to help with the detection of chemical agents and so far we have been testing it on organo-phosphate nerve agents. We have already had promising results testing the prototype and will be validating it at the GIFT exercise in March 2017.

At present we are focused on nerve agents as our proof of concept targets with other project teams in GIFT doing likewise, but there is no reason why this couldn’t be expanded out to other chemicals of interest in the future.

The big advantage of our system is that it can all be contained within a wheeled suitcase. It’s battery operated so it can be easily used out in the field. This is the first time a portable capillary electrophoresis (CE) system has been available to do chemical analysis in the field and it enables scientists to bring their lab to the crime scene – this is a key focus for the GIFT consortium and for the forensic toolbox in general.
Common approach path

Dr Jason Bannan, senior scientist at the FBI Laboratory tells Gwyn Winfield about developing CBR forensic science

There is a suggestion that CBRN events are about as common as unicorn poop. Many individuals think that a CBRN incident has to cause fatalities in several orders of magnitude, but this only focuses on one end of the scale. At the opposite end are many incidents ranging from attempts to create CBR devices, to people making substances but unable to use them, through to individuals selling or using viable substances. To focus on the upper end of the scale is to miss all the work that forensic technicians are doing on CBR crime scenes every month.

Admittedly much of this is not at the super toxic chemical warfare (CW) or category A biological warfare (BW) stage, but it provides a considerable amount of casework and a growing understanding and professionalism in CBRN forensics. It has to be remembered that CBRN forensics is arguably the most recent of all the forensic fields. Only born in the aftermath of the Amerithrax letters in October 2001 (and both David Willman’s Mirageman and Dr Majidi’s Spore on the Grassy Knoll are worth reading), it had a lot of work to do in a short time. An analogy might be trying to find John Wilkes Booth (or John Bellingham for those with more of a UK focus) purely on gun/proof marks.

In retrospect, it is hard to find a better case for CBR forensics to have begun with. A high profile series of attacks/murders done with an esoteric weapon, a mistaken/framed individual, an investigation lasting years and finally a suspect that committed suicide – it’s a murder mystery dream. If, as with the current crop of CBR attacks (cf Everett Dutschke) the person behind it had been a changer or lunatic, there would never have been enough oxygen to have created the science. Simpler investigative analysis or good police work would have closed the case. Had it been a more mundane weapon, an arsenical or cyanide for instance, it would never have caught the imagination.

Dr Bruce Ivins’ motive was always claimed to be his desire to see more research into anthrax and CBR agents, and ironically his very desire might have been his prosecution.

Dr Jason Bannan, senior scientist in the Forensic Response Section at the FBI Laboratory in Quantico, stated that it didn’t feel like a great opportunity to the people on the ground at the time, but the complexities of the case started the ball rolling. “It was a complicated case. The crime scene extended from Connecticut to Florida and over the years we needed to work out how to exploit a lot of evidentiary material in support of the investigation. Much of that turned out to be trying to exploit conventional evidence, but early in the case it was decided that some of the most valuable evidence needed to be decontaminated, or rendered safe, with radiation. That reduced our ability to bring to bear some of the other disciplines like DNA analysis and prints as the material changed when exposed to that level of radiation. Through its successes and mistakes that case helped shape where we are today.”

The good news for the forensics team was that while some of the technology needed work, some of the tactics, techniques and procedures already existed. Although it was never designed to be challenged in court, the military had been practising sampling identification of biological, chemical and radiological agents (SIBCRA) for years. This ensured that there were procedures for the successful collection of agents, meaning that a viable sample could be taken to a laboratory at no risk to the individuals around it.

Dr Bannan suggested that it was not just at the start of the Amerithrax case that the military had played a vital role, but throughout the development of CBRN forensics, and on into the future too. “We have worked closely with military components here and abroad. We have liaised with the SIBCRA programme in the UK as well as the US Army’s 20th CBRNE command and exchanged information over the years through AUSCANUKUS [the quadripartite agreement involving Australia, Canada, the UK and US. Ed]. We also worked with other organizations such as ASTM to develop standards for collection.

“We exercise every two years with all four countries on a CBR scenario where we can observe each other, including a science day where we share scientific advances, or tools that we employ or have developed. Much of the technology, the suits, powered air-purifying respirators (PAPRs) and other advances have been in partnership with our defence colleagues here in the US through the combating terrorism technical support office (CTTSO). It does a lot of work for the military and plenty of the testing and evaluation that supports...
the FBI. The great thing about the international CBRN community is its willingness to share and that has benefitted us a lot.”

It is just as well that the FBI had the start it did plus assistance from partners, as the case load built rapidly. The FBI has responsibility for all forms of CBRN terrorism, ranging from threats through to ‘white powder’ letters and finally to viable devices. As such, it had to manage the enormous case load that followed Amerithrax when the world and its wife thought that it would send suspicious powder to its former spouse/bank manager/high school PE teacher/gynaecologist…

Among all the talc, soap powder, plaster, starch and powdered potato there was occasionally something more lethal, and this kept the capability on its toes. Dr Bannan explained: “In the years before Amerithrax the science involved was mostly first responder based. The FBI was geared up to deal with environmental crimes like dumping hazardous waste, so we had to respond and provide assistance to other federal agencies. Once Amerithrax opened up we realised we needed traditional forensic investigative support to put behind those kinds of cases and it was eye opening. At the time we were working the anthrax investigation, however, we were also getting ricin cases like the Fallen Angel letters. So while we built the new programmes we had no shortage of cases to follow up.

Thankfully, the science has expanded in the last decade in our law enforcement capability to exploit evidence in dealing with CBRN crimes.”

The science has had to expand in at least two directions. The first is the ability to forensically interrogate samples. Current identification techniques will quite likely tell you what the agent is, but they might not be able to indicate the strain, or the concentration of the various elements. Forensic interrogation needs to go further than this. It will want to know what medium the agent has been grown in or exactly what the precursors were. All of this provides information based on the methods and ingredients used to create the payload, and gives the investigator useful evidence on the suspect’s level of skill and the possible sources of the necessary elements and equipment.

The second direction is the ability to extract information from conventional trace (DNA, soil, cosmetics, paint etc) evidence either in a CBRN environment or from a substance that is in itself contaminated. An example of this might be a fingerprint taken from an irradiated phone screen, or a sample of paint that has absorbed chemical agents. Both items are of interest but pose collection challenges or latent threats. As Dr Bannan looks at these two fields which does he think the most challenging and rewarding?

“When we talk about attribution of chemical weapons (CW) material we can look at the R&D that is going on in both those areas. In Amerithrax we looked at the components within the spore powders to try to work out how it was grown, and which region of the country it came from, based on any chemical signatures. Those were challenges in that case and they remain challenges. We don’t have great libraries of all biological and chemical precursors, so the signatures we would like are not always available for comparison.”

“These types of challenges mean we have to rely heavily on our investigators as you can’t replace good old investigative methods, putting the shoe to the pavement, asking questions and utilising traditional forensic evidence that can support them and provide leads. The view over years of CBRN investigations was: ‘How much can we exploit the agent itself?’ Now we have learned that you can’t discount good investigative strategy and scientific support to provide leads in the investigation. That has been a lot of our focus.”

Another element of focus has been the development of analytical capabilities within the American laboratory response network. Except in the rarest cases the FBI is unlikely to be first at the scene. Instead, local first responders are likely to have discovered the situation and, should their own teams not have the
Common approach path

requisite skills, the CBRN evidence will be recovered by local teams mainly composed of the civil support team, local FBI WMD coordinator and local hazmat (for more information see CBRNe World April 2015). These would then take a sample, bag it according to chain of custody and move it up the chain to the appropriate lab.

Dr Bannan explained the procedure: “If it has been decontaminated before we get there as someone has taken the initiative to decon it, then the FBI lab can receive it as long as it has been tested and shown to be non-hazardous. In a real incident, however, we prefer that samples are not decontaminated. Biological samples go to the national bioforensic analysis centre, chemical samples go to our partner lab at Edgewood chemical biological centre (ECBC) and if it is radiological we have our radiological evidence examination facility at Savannah river national lab in South Carolina. We have full forensic capability at all three locations.”

Yet it is not just the facilities that have been upgraded, but also the people working in them. The FBI has invested in building up both its hazardous evidence analysis team (Heat) and its hazardous evidence response team unit (Hertu [pronounced hurt you! Ed.]) and it is also developing further teams that can assist.

Dr Bannan explained how the teams mesh together: “In terms of the crime scene response the forensic response section contains our traditional evidence response team, which trains and equips all the evidence response teams at our 56 field offices. We have a cadre of agents called Hertu who do a job similar to that of the hazardous evidence response team unit, including training and equipping of our hazardous evidence response technicians at our field offices to respond to hazardous crime scenes. We also have the science response unit (SRU) comprising subject matter experts in CBRN, real scientists who are deployed to the crime scene to provide scientific support. Then we have our technical hazard response unit (THRU), who come from the first response community and are very experienced firefighters, technical experts and paramedics that can support our work at a hazardous crime scene and provide medical support and safety officer support.

“Finally we have our WMD coordinators and our agents in the field office where the crime scene is. In an incident our deployable assets from the FBI Laboratory at Quantico, supervisory special agents from Hertu who can deploy to the crime scene along with scientists from SRU and technical specialists from THRU, form a team who will give us a technical intelligence base and informative capability. Unlike other agencies we don’t immediately suit up in Level A and do a recce and come out. Typically, there is a lot of up front work gathering information that guides our risk based response plan. In the 20 years that the programmes have existed we have only required a level A response at two crime scenes.”

In addition to the hazardous crime scene response capabilities, the FBI Laboratory has developed the Hazardous Evidence Response Team (HEAT). HEAT is composed of forensic scientists from the traditional forensic disciplines within the FBI Laboratory. The Heat members receive additional training in various safety elements of CBRN. For example Heat members will be sent to the FBI Radiological Evidence Examination Facility (REEF), at Savannah River National Laboratory, for the radiworker II course that employees need before they are allowed to work in a Department of Energy (DOE) facility and similar courses for bio and chem are also done other at partner laboratories. They are then given mock evidence to work

Sample interrogation is fine, but it needs to be complemented by traditional investigative techniques ©CBRNe World
on in the labs to enable them to link together their subject expertise with evidential and safety awareness (this is in addition to the case work that they will already be getting). They get to mitigate the challenges of applying their forensic discipline to the examination of evidence potentially contaminated with CBRN materials. It is not a small undertaking either, there are approximately 60 forensic technicians trained up and Dr Bannan stated that there were experts queuing up join.

“It is a voluntary collateral duty to be on the Heat but they are eager to do it. We have more people asking to join the Heat than asking to leave. It is exciting, it gets them into these other labs where they get some additional biological, chemical and radiological training and then they feel good when they can support a challenging case.”

So what does the future hold for the FBI and CBRN forensics? In terms of manpower and doctrine it is a shift closer to the crime scene. Due to deployment times, and the potentially volatile nature of the threat, the FBI previously worked in a support role, but Dr Bannan suggested that this might evolve to include triage of evidence.

As with any other triage, this facilitates the selection of what needs to be dealt with first. It calls for an impressive understanding of both forensics and CBRN: which evidence is the most important, now, in 10 minutes, or an hour from now? The blood and hair under the victim’s fingernails or attempting to take a viable sample of sarin? “Forward field forensics is a concept that we are now exploring, which allows more triage and forensic science at the CBRN scene. It helps us to better determine what evidence may be contaminated and require transport to a specialty lab and if we are actually facing a real hazard that requires that specialty lab.”

What equipment, then, is going to make the difference in the lab or the field? Is it better to have forensic technicians with field deployable mass spectrometry, or is it more valuable to have better libraries for the devices they have? Does stand off detection/identification hold more attraction for CBRN forensic techs? What about the ability to interrogate a hazardous crime scene safely and not disturb vital evidence? Dr Bannan suggested that it was hard, but the future was not lots of bespoke CBRN forensic equipment. “Every year it changes and becomes a little different. There is a plethora of kits out there in the commercial sector and we don’t use a lot of bespoke items. Every once in a while we request a bespoke item, such as a telescoping collection tool where we can retrieve a very hot rad source while maintaining safe distance, but it is rare, it is mainly commercial off the shelf (COTS).”

Regarding the future of CBRN forensics, Dr Bannan stated that it was likely to continue in a similar vein to where it started, with healthy cooperation across a range of international partners. As an example he pointed to the work the FBI has done with RCMP and their decontamination work and the ongoing relationship with AUSCANUKUS. “We are never complacent, we are always looking to hone skills further and do a better job. That is why the participation with the international community is important as we are always learning.

“Crime scene response is constantly evolving, not just for CBRN but also normal crime scenes, with new tools and technology coming out every year. We need to keep abreast of them, which is a challenge. Exploiting CBRN material remains another challenge: ‘what can we learn from it that will support the investigation?’ Our goal is to provide as much information to our investigators as possible and that is one of the things that we will struggle with, not just in the FBI but throughout the law enforcement community. How can we exploit these materials not just for traditional forensic evidence but also the CBRN material? It is one of the areas in law enforcement and defence which needs the most sharing.”
Johan Sand, of Finnish research institute STUK, published a GIFT funded paper on the stand off mapping of alpha emitters under full light. This is an edited version.

Crime scenes involving radioactive material have always presented a major risk and a high level of skill and expertise is required in handling them. This is due, in part, to limitations in current methods of radiation detection, in specific for α-radiation, and the equipment available.

Crime scene investigators in full personal protective equipment (PPE) would traditionally enter the scene and scan manually, using a hand held detector. They would have to scan, within a few centimetres, every section of the crime scene, to ensure there was either no alpha radiation, or if there was, to identify the exact source location.

This is very laborious and time-consuming, not to mention laden with risk; it also brings with it the added complication of PPE with all its time/physical limitations. To make matters worse, most regular cameras used for alpha detection, need to work in a darkened room.

As part of the GIFT consortium, researchers at the Finnish Nuclear and Radiation Safety Authority (STUK), have achieved a breakthrough in developing a new approach for remote detection of alpha contamination and have published a paper on their project success: Stand-off Radioluminescence Mapping of Alpha Emitters under Bright Lighting.

The detection is based on the optical measurement of radioluminescence light that is produced by the absorption of alpha particles in air. The faint light emission is observed in UV wavelengths and this is managed in daylight, rather than the darkness required in other alpha imaging experiments.

While scientific grade cameras have been successfully applied in previous experiments, due to their low noise characteristics and good sensitivity to UV light, this project used a scanning photomultiplier tube (PMT) system redeveloped as an imaging system. The STUK team used an optical system, based on the Galilean telescope, and constructed it using commercial components giving it a high efficiency while keeping the costs down. The performance of the alpha particle detection was studied using well characterised alpha emitters at the Institute for Transuranium Elements in Germany.

The researchers reported that one of the key benefits of the new approach was that the spectral response characteristics of a PMT are not as prone to visible light as silicon based camera sensors. This created their key breakthrough – measurements in environments which don’t have to be dark, a far more common approach!

The STUK researchers said: “This is a key breakthrough for operative use since the time consuming total light shielding is not required. The observed photon count rates verify that a careful combination of detector response and optical filtering can enable optical alpha particle measurements under normal lighting.”

According to the team, the idea of using radioluminescence light for the detection of alpha particles, has been around for more than a century but using it for remote purposes has only recently been explored by several research groups around the world.

The GIFT research has concluded that radioluminescence mapping with a scanning PMT system is very affordable compared with a specialist UV camera. It is also more straightforward to use as it doesn’t require light shielding, and can be operated with very little training as it only requires a laptop to work.
Dr Daan Noort, from TNO, on their work to improve identification of CBRN agents and their manufacture

Methods to speed up the identification of toxic chemicals used in a CBRN attack on society are absolutely key to dealing with the crime scene and also for treating anyone who may have been contaminated. Even more crucial for the forensics aspect is the ability to identify the potential source of the CBRN agent to help in catching the perpetrator.

The Netherlands Organisation for applied scientific research (TNO) is currently working on Work Package 5 within the GIFT consortium – looking at chemical threat analysis – assessing if people have been exposed to chemical agents. Alongside this, it is working on chemical profiles, looking to develop tools to identify chemical attribution profiles.

Attribution profiles consist of data on the presence of chemical attribution signatures (CAS) which are byproducts from synthesis and impurities in starting materials.

CAS are known for limited sets of chemicals and new knowledge of profiling methods on a set of chemical threat agents would represent major progress. The GIFT project is looking at the development of analytical tools to determine a broad range of hazardous chemical agents in environmental and human samples.

TNO is working alongside FERA (UK), DLD (Belgium), FOI (Sweden), DSTL (UK) and NFI (The Netherlands), to develop methods for the analysis of biomedical samples and environmental samples, focussing on three model compounds:
- Phorate – a substitute for nerve agents.
- Acrylonitrile – an industrial agent.
- Fentanyl – a potent opioid – non-traditional agent.

The decision to use phorate was made in the very early phase of the project. Although some of the partners have vast experience in working with live chemical warfare agents, they considered it easier for various reasons to work with phorate as model compound for a cholinesterase inhibitor. Eventually the organisation wants to end up with a recommended operating procedure for biomedical analysis from a casualty who has been exposed.
TNO has also been looking at the impurities appearing in fentanyl so it can see indications of how the opioid has been produced, with the idea that we might then be able to say that isotopes from a specific batch of compounds are traceable from the end product.

For example, if the batch at the crime scene, compared with a batch from an illicit factory, had the same isotopes, it would enable the forensics team to prove a correlation. The results, so far, have been successful.

TNO is now developing generic protocols to go into the toolbox. So if there is a particular compound, for example, the protocol can still be used in the same way as with another compound, so it is quite interesting and new and will definitely help the entire chain of a CBRN event. This will also enable some work to be carried out faster on other chemicals in the future. The spectrum of reference compounds for the toolbox will help to speed up the recognition of certain chemicals involved in the first response to an incident.

In Work Package 3, the organisation also worked on detecting agents at a crime scene – visualising the presence of chemical agents on the spot. TNO has been exploring three options for visual identification of some kind of contamination – with considerable success:

- Colour reagents.
- Metal organic frameworks (MOFs).
- Miniature mass spectrometry for on-site analysis.

It has already seen several successful results from the project including successfully demonstrating that colour reagents react well with organophosphates and fluoresce very easily so they can then be detected under UV lamps. So far the researchers have had good results testing on pesticides, which is a very helpful indication for nerve agents as well. Future developments could see this work developed into an enzymatic assay.

In terms of the fluorescent labelling of MOFs, this was found to be indicative for the presence of nerve agents as they detect the fluoride ions which are found in nerve agents. While it would be easy to do this on site the research has shown that unfortunately external interference can be a problem.

As regards miniature mass spectrometry, TNO has been experimenting with the first Detect MMS1000, a field rugged version of an instrument which is routinely used in labs. This proved successful and the organisation is confident that all of these technologies could fit well in the toolbox.

All three techniques have the potential to help improve chemical detection at the scene. A CBRN forensic investigator would take the devices with them to apply these techniques on site. For example, they would see the colour change and fluorescence results and input that data into the toolbox, the data would then be analysed and the relevant information would be sent back. This would generate a warning that personal protective equipment is required, or it may show up particular areas of the crime scene which should be avoided due to the strength of the contamination, or where responders might need more complex scanners to deal with the situation.
Before the theatre

Adrien Sivignon, crime scene officer within the Police Technique et Scientifique and CONSTOX, talks to Gwyn Winfield about bolstering France’s capability to identify CBRN terrorists

[This interview was done three days before the dreadful events of 13 November in Paris. Our thoughts and condolences are with the victims’ families all around the world, and we salute the bravery of all arms of the French response system that had to deal with the circumstances of that cowardly attack. We are sure that the French first responder system, described below, will learn and evolve from this outrage to become stronger and more capable than ever. Gwyn Winfield]

There is always a dichotomy at the heart of any civilian CBRN response. Unless the terrorists have done the emergency services the favour of announcing their attack, it is unlikely to become apparent that it is a terrorist chemical attack in the first few minutes. The initial calls into emergency response will most likely resemble those for a mundane gas leak. While police might respond to help with public order, the detection, identification and monitoring task, which will probably give some of the early clues as to the nature of the event, is likely to be a fire brigade (FB) task.

This presents a challenge to fire and rescue services of understanding what constitutes evidence and forensic traces, and trying to ensure that they don’t destroy or compromise what might be vital clues. Some nations endeavour to manage this by creating multi-role first entry teams, training fire fighters in forensics or bolstering police CBRN detection capability. There is no right answer, but what there can’t be is an element of ‘we’ll sort it out on the day’. Forensic technicians can’t be expected to don personal protection equipment (PPE) the first time they enter a contaminated crime scene, neither can FB officers be expected to know what constitutes evidence by some weird form of osmosis (or watching CSI New York).
France opts for fire brigade control of CBRN incidents, they will enter the scene, help extract casualties and perform their detection, identification and monitoring (DIM) duties. Police will keep the cordon and once a CBRN terrorist incident has been acknowledged they will inform the Prime Minister who will then activate his Détachement Central Interministériel (DCI), a senior level advisory board with scientific and operational assets. CONSTOX is one of these assets and is a collection of forensic specialists and investigators trained to go into the hotzone and recover the evidence. It is headquartered in the town of Ecully, just outside Lyon, but has operatives located in a variety of major cities and regions.

Adrien Sivignon, a CONSTOX management team member, explained. “Ecully is the French police forensic HQ and our heavy equipment is also there. In addition we have 70 people spread over the country working in local judicial police services. They are mainly in Paris with the counter terrorist command, and with the judicial police of Paris. In addition there are people in Lille, Bordeaux, Marseille and elsewhere in France, so if there is a CBRN incident then the local people will go and make a first assessment, according to what their FB says and what the CBRN agent is. They will make a call to the HQ, ask them to come to the scene and deploy with all the equipment from Ecully. We have trucks that can drive the equipment 24/7 but we can use helicopters or planes if needed.”

CONSTOX, an acronym for investigation in a toxic environment, has been around for a while. The idea was born in 2007, first training happened in 2009 and the team reached initial operational capability in 2011. The CONSTOX team only deals with conventional traces (the forensic three Ds - DNA, data and dactyloscopic traces) in a CBRN environment. The samples of the CBRN agent will be taken by either the local fire brigade (if they are capable) or by military or scientific assets of the DCI (the Sapeur Pompier de Paris, 2nd Dragon regiment or the Commissariat à l’Energie Atomique, the CEA) and this is assumed to have happened by the time the CONSTOX assets arrive.
M. Sivignon explained: “Local people will pick up initial information and, once agreed by the operations chief, they make a first assessment and give us information. We are not first responders, we won’t deal with sampling, the FB has the capability to do that, and we work with them and DCL. The investigative part is CONSTOX, for decon it would be the Dragon regiment or local FB, for any rad or nuke expertise it is the CEA, and if we need any information we just go through them.”

Law enforcement in France is not straightforward. If it happens in a major conurbation investigation is the role of the police, if it happens in a smaller city or the country it belongs to the gendarmerie [for

US readers: think county vs city, ie LAPD vs LA county sheriff]. The investigation routes are also different, in that the police will use the FB to provide CBRN scene assessment and characterisation, whereas the gendarmerie has its own assets and will generally keep fire outside. CONSTOX can deal with terrorist, criminal and major technological incidents, but city and rural law enforcement have to use them for terrorist incidents. That isn’t to say that they will stop work on other cases where things looked terrorist at the start might turn out to be something more benign, once they are requested by the judicial authority for a terrorist CBRN case they are committed.

M. Sivignon gave an example: “We had a case in 2013, it was in an apartment in the south of France where a guy had died. The first responders through the door were the local fire brigade, they detected something as they started developing headaches and had to go to hospital. They sent in a fire hazmat team that detected chemicals, which were identified as acids. We were called out as this guy was known to be part of a terrorist organisation, or at least he had a ‘past’. We found a lot of writings in different languages, and we were quite suspicious, but when we conducted a search we found out that he was a poor guy and was refilling batteries with acids. At the end of the day it was nothing special, but we have not had a counter terrorist case in France, not even a criminal one, since 2011, and hopefully it will remain only training. We participate in a lot of local training organised by the prefectures in France, so even though we are a national unit we do 15 training exercises a year and then real training with CEA, Laboratoire Central de la Prefecture de Police (LCPF) etc.”

Most of what CONSTOX brings is lots of experience of doing delicate forensics work in level A suits and other PPE. Much of its equipment is traditional forensics kit, and its PPE has not been modified in anyway, if needed they can grab extra hazmat suits from the local fire brigade. That said, the skill set of the team is high, they are all experienced crime scene investigators, rather than laboratory personnel, and expert in being able to defend a trace or activity in a crime scene to lawyer in a court of law.

“Half of the team is composed of highly qualified investigators, working counter terrorism in France and the second half are forensic specialists. These people are used to working together on conventional scenes, on non-CBRN things. Investigators take pictures of evidence and all the usual judicial aspects of procedures are taken into account and all done in a CBRN environment. While the gendarmerie has the capability to decontaminate to take samples of evidence they don’t have any investigators in their team.” said Adrien Sivignon.

“Our team is unique in that we build CBRN scenarios and train for them in Ecully. We have done live agent training in Cazaux, near Bordeaux, to make sure that what we wrote in our protocols was correct for a live environment. Two colleagues have also done sampling and identification of biological, chemical and radiological agents (SIBCRA) training and from all of that we built our own training for our people. When they come here they are trained on CBRN risk and how to wear PPE, protocols such as clean man, dirty man etc. We also participate in international training and cooperation, so I am an International Atomic Energy Agency (IAEA) trainer for radiation crime scene investigation.”

The fact that CONSTOX comes in and only does the crime scene investigation helps it avoid some of the differences in capability between different areas. Once the DCI has been activated it might well send decon or DIM support to the affected region/area, but since CONSTOX is focused on only one task it might be working seamlessly with 20 agencies or only one, it makes little difference to the day to day.

One question and answer that immediately became superseded by events is “what is next for CONSTOX?” It is hard to see that the aftermath of the Bataclan won’t have an impact on the future business of the team, but it is worth including the original response as the revised answer is not likely to be known for quite some time.

Adrien Sivignon’s original response was that the team has no desire to build its own fleet of mobile labs. They prefer to work with fixed facilities and are evaluating improvements to them. “We have a lab for chemicals and are currently working on improving our nuclear forensics. We have taken the decision to recover evidence and not work on scene and as such the best job will be done by working in a fixed lab rather than a mobile one. The idea is to build a similar lab to the UK’s Atomic Weapons Establishment, with glove boxes etc. We don’t think that the work on scene will accomplish the job, you might have quicker results but they won’t be the best.”

Despite the fact that the recent attack was not a CBRN one it will be interesting to see what lessons are learned from working such a variety of large intensive scenes. There is little doubt, in my mind at least, that future attacks are likely to have a non-conventional overlay as well, to further complicate matters and slow responders. I suggest that so many of the lessons learned from Bataclan et al can have a dotted line drawn from them, in much the same way that Mumbai and 7/7 can. We hope, in time, to talk to CONSTOX again and see whether we can learn what those might be.
The Most Flexible GC/MS
Now with Real-time
Vapor Threat Detection

FLIR
GRIFFIN®
G465 GC/MS

www.flir.com/G465
A lot of the work in the GIFT consortium will enable responders to measure levels of contamination safely at a scene using the new technologies being developed. The idea of the risk assessment tool is to then take that information and assess the risk to forensic investigators before they enter the contaminated crime scene. Operatives will need to know the threats they are facing; these can be from the CBRN agent itself, other hazards on the scene and any general safety risks.

With CBRN, there is also a risk that while in a protective suit, the investigator could damage evidence as suits make them quite clumsy and cumbersome. Picking up small bottles for sampling can be very tricky when wearing big gloves, for example, as they could be dropped and broken. Using personal protective equipment (PPE) to protect from a CBRN agent, brings its own risks, particularly in terms of the personal safety of the wearers, as they have a limited time in the suits.

All these elements need to be considered as part of a CBRN crime scene risk assessment, before a forensic investigator can consider entering the area.

Why CBRN particularly?
What makes a CBRN crime scene different from a normal crime scene is that there is the addition of a whole new level of risk to be considered:
- The risk of exposure to the CBRN agent from the scene.
- The risk of exposure to the CBRN agent from the evidence.
- Dealing with and handling contaminated evidence.
- Sampling of the CBRN agents themselves for processing.
- Working within PPE restrictions.
- Removing contaminated evidence from the crime scene safely.
- Decontamination.

So how will it work?
The risk assessment tool will be an electronic system of questions, accessed via the graphic user interface of the GIFT toolbox. Once initial information has been gathered by first responders at the scene, the officer in charge of the forensics team, will access the risk assessment tool and input the information available, to assess the risk of harm to the team.

The tool will run on a series of yes/no questions and will return suggested actions as a result. If, for example, you input the type of agent detected, it would advise on the correct type of PPE required to enter the scene, any necessary respiratory protection or skin protection, or a particular type of glove.

The CBRN risk assessment tool would be quite versatile and could be used either after an incident to check on the live issue and give advice, or it can be used if there is a perceived risk of something happening.

Why do we need this tool?
The biggest risk at any scene is the unknown, particularly with a CBRN scene. The idea is that this tool will be very quick to use because it is specific to CBRN risks. A regular risk assessment at a crime scene can take at least 20 minutes. We envisage that this tool will return a CBRN risk assessment within 10-15 minutes so it will speed up the whole process.

The tool is not a monitoring device for assisting at the scene. Any change in the environment, such as an active new release of CBRN agents would be a reason to leave the scene as it would create a new uncontrolled situation.

In that case the forensics teams would have to come away from the scene and do a new risk assessment starting all over again. These checks and controls are important in the
prevention of contamination of personnel and also to stop them from bringing contaminants out of the crime scene.

What about future developments?
The idea of the current tool is to help the officers in charge to make a decision about sending their forensics teams into a crime scene. The tool doesn’t alert you to any changes in risk level once you are in there. But with all the portable sensors being investigated as part of the GIFT programme, it could be developed further into a risk monitoring tool.

Equally there could be an ongoing research project to look at linking up the risk assessment tool with the live sensors to provide ongoing alerts and assessments on scene, but that’s for a future work plan.

Currently, the planned prototype is focused on forensics investigators and the idea is to use it in addition to the normal risk assessments that would have already been carried out at the scene, as it is only focused on the CBRN aspects.

Forensics teams would use information already gathered from the scene by the first responders and equipment at the scene, and then input data into the tool and work out the best course of action from there.

It is hoped that by using the tool consistently at CBRN-related crime scenes, it will help to educate investigators about the unique risks they face and will help to make things more uniform across all European countries, providing a gold standard for all CBRN risk assessments.
The challenges posed by the post-event forensic examination of a CBRNE incident are many and varied. The response of scene examiners may be limited due to operational constraints or interventions required to ensure safety. To complicate matters further, forensic response capabilities face another set of challenges that have little to do with the hazardous nature of the scenes encountered in CBRNE incidents and a lot to do with the politics that surround forensic provision in England and Wales. Some consideration of these problems might prove to be a useful exercise in forewarning the responder. Of even more benefit might be some consideration of what value forensic intelligence might have in advance of a CBRNE-related act of criminality. Exploring current structures to find solutions in advance of catastrophic events can surely only be a good thing.

In terms of the challenges, we live in interesting times in UK forensic service provision. Whilst the Forensic Science Service (FSS) had nominally been part of a landscape of commercial providers, its ‘govcorp’ status allowed it to endure swinging financial losses month-on-month for years, even whilst servicing something like 65% of the domestic forensic market. To put this business model failure into a wider context, the next two largest (and private held) forensic service providers, LGC Forensics and Cellmark, are both viewed by the market as being buoyant and energetic. The former is developing its current status through LGC’s acquisition of Forensic Alliance, whilst the latter was recently subject to a pricy buy-out by US-firm Labcorp.

From the perspective of forensic support for CBRNE incidents in the UK, the much publicised encroachment of sharp-suited privateers may well prove to be something of a paper tiger, having a relatively limited effect on the practicalities of submitting exhibits for analysis after the fact. It may yet mask other, more pernicious risk such as the...
because the SoCO occupies a strange little no stab vests, no CS gas, no baton and no 'front-line'. Despite this exposure, SoCOs not take statements, make arrests or chirruping airwave radio handset. They do driving a marked-up vehicle and carrying a from that of a warranted police officer, whilst wearing a uniform not dissimilar examine scenes and interact with the that is still playing out today.

CBRNE response as a Latin lesson, but bear氾 in the world of crime scene investigation. Here I feel old enough to be played on screen by Peter Ustinov, hobbling around an ivy-choked Lincoln Memorial. In 2001, scenes of crimes were a trade shared pretty much in even numbers between civilians and detectives. Some forces, such as West Midlands Police, have been early adopters of the civilianisation of SoCOs and featured a relatively small number of warranted officers still in the role. Other forces, notably Gloucestershire and Essex, resisted the appointment of civilians to SoCO roles well beyond 2001.

This may seem about as relevant to CBRNE as a Latin lesson, but bear with me: this is the beginning of a fault line that is still playing out today.

Civilian SoCO respond to reported crimes, examine scenes and interact with the public, more often than not these days whilst wearing a uniform not dissimilar from that of a warranted police officer, driving a marked-up vehicle and carrying a chirruping airwave radio handset. They do not take statements, make arrests or respond under blue lights, but in any other sense of the term, they are very much 'front-line.' Despite this exposure, SoCOs lack any routine form of police protection: no stab vests, no CS gas, no baton and no protection training. The reason for this is because the SoCO occupies a strange little twilight zone of police policy: to equip a SoCO to deal with hazards is to admit that they face them. Give them no mitigating equipment or training and you can continue to treat them as if the level of risk they face is the same as any other police-employed civilian.

It is into this twilight zone that CBRNE scene forensics falls, along with an interesting, mixed bag of anomalous crime scenes including hazardous materials handling, scenes at heights, scenes in confined spaces, scenes in water and, to a great extent, mass fatality scenes where disaster victim identification (DVI) protocols are required. It is culturally easier and politically more expedient to equip warranted police officers, frequently drawn from search serial units, to respond to these specialist scenes, despite the fact that over the past decade, many such officers have had very limited exposure to developments in forensic science or current thinking on the creation and implementation of a strategy of forensic scene examination. The police CBRNE responders are well trained and equipped to stand alongside other such specialists but they are not the best people in their services to manage the complex forensic investigations required. That is likely to be a civilian crime scene manager or co-ordinator who may not even have been considered for such a role.

Knowing my place: scenes of crime officers versus forensic scientists

In addition to a cultural divide between warranted police and SoCOs, a similar one exists between SoCOs and forensic scientists. Whilst SoCOs are trained and developed as general practitioners of crime scene examination and exhibit recovery, their ability to interpret complex scientific evidence on the crime scene is limited. Fire and explosive damage, blood spatter patterning and the excavation of buried human remains from individual or mass graves are all examples of the sometimes vital evidence types that are impossible to seize and export from the crime scene. Should they play a role in the examination of a CBRNE crime, in the interpretation of post-blast fire damage or the recovery of human remains buried following a chemical weapon attack, we currently lack a comprehensive system of response. This lack stems from a disconnect between professions rather than any insurmountable obstacles.

The brains trust: Research versus practice

If the practice of forensic examination and scientific interpretation on the CBRNE crime scene raises a number of issues of specialist resource, the research required to improve this situation is much the same. It was suggested in some sections of the press that the demise of the FSS would herald the end of forensic science research in the UK. Whilst I don't believe this to be the case, it is certainly true that the remaining providers are in the process of adapting to engage with forensic science academics in a constructive manner. Worse still, government-directed science, as funded through the Research Councils UK, has so far allowed forensics to plummet so comprehensively between its various stools that academics have been forced to direct their creative energy into devising newer and more agile ways to avoid use of the 'I word in research grant bids.

Where the forensic service providers do engage in concerted research efforts, they rarely target scene-based disciplines as these are generally peripheral to their core business model of bench-based forensic analysis and are hard to cost and resource in a sector dominated by high-volume, quick-turnover and fixed-price services.

Watching the detectives: intelligence versus evidence

Whilst the domestic security services routinely conduct forensic examination of scenes on the basis of intelligence received, and military intelligence gathering has developed to accommodate field-based analytical techniques, neither has yet fully grasped the potential offered by forensic intelligence exploitation. The stakeholders that might be best placed to assist are hampered by a range of issues and civilian SoCOs are largely excluded from any such intelligence-based activity. Experienced they may be, but their deployment is almost wholly reactive and investigative rather than intelligence-led. The forensic service providers are largely focussed on bench analysis and their close involvement in forensic intelligence exploitation might be hampered by the high-throughput nature of their business models and the customer/provider relationships that dominate their work with police and security services. Academic institutions professing interest in forensic science are, in most instances, hampered by their concentration on undergraduate teaching, as well as lack of time and resources to invest in extended research.

Is this as bad as it sounds?

Categorically not, I believe. The UK possesses all the elements required to be a world leader in terms of both the forensic intelligence exploitation required to combat the risks of CBRNE incidents and the specialist forensic techniques required to examine such scenes following their use. Despite recent cuts to police forensic budgets nationwide, we still possess a large number of highly-trained SoCOs, an energised and well-financed stable of forensic science providers and a university sector led by a small number of the highest quality research institutions that would happily facilitate this work.

The challenges outlined here are largely tribal in nature and are eminently surmountable. Tensions between the roles of police CBRN responders, civilian SoCOs, forensic scientists and university researchers currently compromise our ability to develop a comprehensive forensic response to CBRNE risk, but the methodological advances of the last ten years that represent routine best practice on the standard major crime scene are readily adaptable to CBRNE intelligence and scene response.
Hey! I'm trying to eat here!
Analyze This!
Michael Madden, CEO of Analyze IQ, talks to Claudine Weeks about getting more information out of existing samples

Using miniaturised sensors to detect CBRN agents at the scene is just one step in the toolbox journey being explored by the GIFT consortium. The aim of this project is to bring all the component parts together and Analyze IQ is working on the second step – providing immediate analysis of sensor data to help those on scene with their decision making.

Michael Madden, CEO of the Irish company explains:

At Analyze IQ, we already have the world's most advanced analytical software for spectroscopy data, including algorithms that work well with mixtures and complex data for library software. Within the GIFT project, we are developing:

• **Data Communications protocol** – structured messages sent securely over the internet.
• **Information hub** – to route the messages as needed. This takes all the messages from the sensors and sends them through to the analytics service.
• **Analytics service** – performing chemometrics and/or library searches to analyse the sensor data received into the toolkit.

We are working with the Belgian company, Space Applications, and the Turkish company, NANObiz in Work Package 6 (WP6), to create the information system part of the toolkit. This will take data from all the technical tools being developed, and turn it into useful decision making information at the scene.

The added value we provide is the analytical software – pattern recognition, labelling the information in real time and adding functionality into the sensor data. For example, the sensor will produce a graph, which will then automate the analysis of the data within that graph, which will enable the commander to make better decisions.

If, for instance, radiation is detected by a sensor at the scene, that information will be analysed and, via the toolkit, advice will be provided on which PPE to put on or what procedures to take. It all fits into the data and supplies vital information to the scene.

The advances in miniaturised chemical sensors that are explored within GIFT, and elsewhere, open up massive opportunities in chemometrics and provide interesting options beyond CBRN forensics. Chemometrics is an analysis model which uses hundreds of variables to allow a non-expert to extract data from a sample that, in our case, would usually only be available to an expert in the lab. The experts can build the models and the knowledge on the software system we are creating and then the information can be used out in the field by non-experts.

We are trying to ensure we can get chemometrics information directly to the scene. For example, a Ramen detector will send the data to the analytics hub and then the research will be carried out through chemometrics and library searches, and the results will be sent straight back to those on the scene. Even if the chemicals are 50/50 mixtures or even 10/70/60 mixtures, which is when most library searches would fail, our chemometrics system can come in and get a result in a few seconds.

End users can run the chemometrics directly on small mini processors, which is a significant feature of this GIFT project. An investigator could do the chemometrics on a Raspberry Pi and then stream it to another computer so they could even have someone viewing it at home live, should that person be on call as part of the incident management.

Any information from detectors or devices at the scene will be stored securely and made available to those who need it. It's about presenting information in a usable fashion via a good user interface.

There are some procedural questions still to be figured out but we can enable sketches and scene photographs to be captured by the tool box from a technical point of view. We are still working on a protocol for how this would all work and how to store information from the first responders which may not be admissible as evidence. Every piece of data in will have data stamp and time stamp on it for the chain of custody.

While working on the analysis side of the toolbox, we are collaborating with Space Apps who are developing the graphic interface for the people who will be using the toolbox, and also with Nanobiz who are creating the information hub which will store all of the protocols and operating procedures. The three companies working together, will create the software aspects of the toolbox, ready to connect to the physical sensors and take the data they supply from the scene, to turn it into useful information to help support decision-making. The vision, post GIFT, is to try to commercialise the system for people to use out in the field once the principles have been proven from the project.
Austria's take on CBRN forensics

Austria's collaborative approach to CBRN forensics is paying dividends. Guenter Povoden, head of section, chemistry and development at the Austrian armed forces' CBRN defence school talks to Claudine Weeks about the achievements and challenges.

CW: What makes Austria's approach to CBRN forensics outstanding in Europe?  
GP: Over the past two years, the Austrian armed forces have improved cooperation and interoperability between forensics experts and other military units, by offering forensics training for specialised CBRN and explosive ordnance disposal (EOD) experts so they understand what is required.

Our sampling and identification of biological, chemical and radiological agents (SIBCRA) teams were already able to sample in very professional ways under CBRN conditions, so we have been working to link forensics teams with our SIBCRA teams to share knowledge.

Special investigators from the military police, EOD personnel and the weapons intelligence teams (WIT) have all been trained in forensics and share their knowledge with the CBRN specialists. All the experts understand each other and the roles everyone plays in any incident.

Our EOD personnel are also trained to make sure they don’t destroy evidence as far as possible when dealing with the devices, although their priority is to render devices safe. The WIT teams also share their knowledge with CBRN experts as they will be dealing with post-blast scenes and need to know what issues they may face from explosives.

It’s all about interoperability between the EOD teams, military police and the CBRN specialists. We have been working together to develop SOPs (standard operating procedures) across all of the branches so that we have a procedure to follow if a CBRN expert joins a military police team for an incident, or if an EOD military expert is called out. The culmination of the past couple of years of cross-specialism training will be a finalised CBRN EOD doctrine which is due to be published very shortly.

CW: What else makes Austria stand out?  
GP: We are assessing some state of the art equipment for the identification of explosives. The same equipment is used in other countries and we are planning to harmonise the data, especially with Germany, which will enable us to detect patterns in explosive composition, but we are at the very early stages of this project.

We are also participating in the JDEAL project – the joint deployable exploitation and analysis laboratory – located in The Netherlands. It is a level 2 WIT in theatre laboratory capable of screening fingerprints, exploiting electronic data and has an explosive analysis capability. There are two labs, one for training and one for deployment to the scene. We will continue to participate in this next year, to look at forensics in theatre.

We have also been working on a sample control site container with a containment system for bio/chem hazards that can handle contaminated samples and secure them properly. Once we know that samples are clean, they can go on to the normal forensics lab, or if they are contaminated a CBRN forensics expert can work safely on the sample directly in this container.

The ideal would be to attach the container to the JDEAL and work with both at the scene of an incident. You would use the sample control container to assess the contamination of the samples, and then use the JDEAL lab to work on the evidence on site, a highly sophisticated screening tool for unknown/CBRN samples.

CW: Can you explain the composition of your CBRN forensics team?  
GP: We have no dedicated CBRN forensics team per se but with our cross operational skill set we can tailor make a team for any incident. That’s why it’s so important to have the cross force integration and skills training – it ensures everything comes together.

The challenge, however, is to make sure the teams all speak the same jargon and language so they all understand each other’s roles. Special investigators from the military police for example could identify which is the best fingerprint powder to use in a CBRN environment. It’s all about learning each other’s procedures as normal powder would go everywhere and spread contamination. A forensics team with some CBRN knowledge would know to use magnetic fingerprint powder whenever possible to avoid the contamination issue.
Weapons Intelligence Teams, CBRN experts and forensic technicians all need to work together to create a military CBRN forensics capability.
RAMEM: Specialist in Prototyping
Increase the TRL of your technology

http://www.ramem.com/prototyping
The forensics team also needs to understand the CBRN side, for example the clean/dirty man protocol on how to approach possible contamination. They need to know that within a CBRN incident, the sampling won’t be done by them but by the SIBCRA teams, but under their supervision. So the forensics expert can advise on what needs sampling and why, and the SIBCRA team has the skills to do it in CBRN safe way. In case the forensics specialists are taking or preparing a sample, the procedure will also follow the clean/dirty principle.

CW: Do counter IED operations and training naturally lead to CBRN forensics? Is that the best way for people to start?

GP: We are very much involved in counter-improved explosive devices (IED) work and we try to include CBRN related issues on a regular basis within this. We hosted a CBRN search course for the European Defence Agency last year and are working on the implementation in the Austrian armed forces, looking at military search operations carried out under a CBRN environment, or searching for CBRN hidden weapons caches.

We are also now writing up a concept paper on CBRN search as we want to define and develop this very specific capability a lot further. It crosses over with intelligence, CBRN, EOD, laboratory and technical intelligence. It’s very important here to have a solid chain of evidence in place for the forensics side so that we can go out and support in other countries. The first military police special investigators have received basic CBRN training and recently they took part in a live agent training exercise with us.

CW: How do you put together a training programme for CBRN forensics? Can you go to civilian authorities and ask them to teach you, or do you need to start from scratch but to a known (although legally justifiable) goal?

GP: The military police already get training from the civilian police in Austria. They do a couple of months of training and are also invited to spend time with the civilian forensics teams to shadow them in real life while working out in the field.

They get full training with the civilians. We need to get training and accreditation so that we can go out and support in other countries. The first military police special investigators have received basic CBRN training and recently they took part in a live agent training exercise with us.

CW: What experience have you had with forensics?

GP: A few years ago we had several potential anthrax cases, which involved our unit. That was before we had the current CBRN forensics capability and looking back, the way we handled that case really helped to shape how we are working now. The incidents actually turned out to be hoaxes, except in one case, but the experience of handling and working on them was invaluable for getting to where we are now.

In Austria, forensics is mostly the responsibility of the police – the military only have a supporting role but if it is a CBRN incident then they would largely rely on us (i.e CBRN specialists of the CBRN defence school and the CBRN companies) so that’s where we would support them. A couple of weeks ago we were called out to help with a suspicious container found in some woods. It was very similar to one found in Germany which contained sarin, so there was genuine concern.

We worked with the police to assess if it was part of a crime - had it been hidden there by someone for use later, had it been dumped, or was it an old container left over from the war? None of this was apparent. But our team had to think about all the options and possibilities and deal with the container accordingly.

This incident was a good example of cooperation between EOD, CBRN specialists and civil authorities: The police called the CBRN specialists who checked the container and the environment for any contamination, the EOD assessed it regarding explosive threat and took x-rays. We clearly could see that there was some liquid inside and after the container was secured, the civilian police escorted it to a specialist laboratory where the CBRN experts took a sample with specialist drilling equipment.

So police and military worked together. It worked well as cooperation between our EOD people, the police explosives people and our CBRN expertise.

CW: What do you see as the major challenges for Austrian CBRN forensics specifically and CBRN forensics generally?

GP: In Austria we don’t have a lab accredited to the Organization for the Prohibition of Chemical Weapons (OPCW), but our military lab is capable of confirming the identity of chemical warfare agents. We also have a very good military bio lab, it is a biosafety level 3 plus lab. The challenge is getting information updated. Classical chemical agents are not the problem, the challenge is new substances coming through which we have never seen before and identification of all the toxins may be challenging. Things which affect the body, like nano-materials may appear in future. We always rely on database information to help us identify agents so we need to keep it constantly updated and share information.

In general, the challenge is that most nations are not open in sharing information on forensics. More information sharing and cooperation across different countries is needed. Information should be shared more quickly and more openly, but national procedures often restrict that between countries.

The other key challenge for CBRN forensics for the future is when evidence is really heavily decontaminated – at the moment you sometimes have to accept that the evidence is gone and that’s that. Being able to decontaminate items without losing the evidence is really challenging, but is an essential focus for the future of CBRN forensics.
Work is now well under way on the development of three training exercises for the Generic Integrated Forensic Toolbox (GIFT) programme, whereby the protocols, procedures and some of the technologies, will be put to use for the first time under field conditions, to assess and provide proof of principle.

The first exercise, to be held in the UK in December 2016, will involve a radiological/nuclear scenario, while the second one in the Netherlands will focus on a salmonella poisoning to explore the bio aspects of the project. Defence Laboratories (DLD) in Belgium, is currently planning the third and final exercise for early 2017, which will test the chemical aspects of the CBRN forensics toolkit, using the discovery of an improvised chemical warfare laboratory as the setting.

Belgium was one of the first European countries to develop a CBRN sampling and identification of biological, chemical, radiological agents (SIBCRA) team, an expertise that has since spread to its Gallic neighbour and the rest of Europe. Historically, while the US adopted CBRNE, the division between explosive ordnance disposal (EOD) and CBRN remained strong in Europe. Belgium, however, was among the first countries to start knocking that door down, and was a constant feature of NATO Response Force (NRF) CBRN rotations with its EOD unit. Now it is increasing its effort in forensics, a logical next step after providing SIBCRA and CBRN EOD teams.

Belgium is currently looking to roll its two full time SIBCRA units into SIBCRA/forensic units. DLD is an active member of the GIFT consortium (www.giftforensics.eu), which is researching, and in some cases delivering, the next generation of CBRN forensics in Europe. Engagement with this project is allowing DLD to look at the various elements involved, and see what can be utilised for its own needs. Once you have a SIBCRA capability you have a great deal of the CBRN element covered, but DLD views this as a chance to learn how to deal with traditional forensic traces (DNA, data and dactyloscopic elements) in a CBRN environment.

Mrs Katleen De Meulenaere, CBRN technical manager at the lab, and lead for GIFT, explained: “The forensics part will be an extra task for our current SIBCRA teams. They have already done CBRN sampling and there is a current need for sampling of traditional forensics as well; it’s a great opportunity but a lot of work. This operational capability gap is one of the reasons we are in the GIFT project, it is an excellent chance to work with specialists and people in forensics.” It means that we can work on a European level as well as a
national level, as we can collaborate closely with other GIFT partners such as the NICC (the Belgian forensic research lab). It is a win-win situation," she said.

Direct linkage of research to operational army units is not unusual for DLD, as it views itself as an operational unit. The SIBCRA units in the army have DLD scientists incorporated, while DLD itself comprises full time scientists and military personnel with scientific backgrounds. The split is about 50/50, which allows a great deal of understanding and knowledge to build up in the team, and provides a greater understanding of operational matters when it comes to offering CBRN advice to commanders.

Lt Col Martel, DLD’s commander, explained the make-up of the organisation. “We have three technical departments. Katleen is head of the CBRN department which has five labs. There is the protection lab focusing on personal protective equipment (PPE), Colpro and decontamination. The detection and sampling preparation lab is deployable; its people can take samples, mainly in the area of environment and health and safety but they also do the sample preparation for Organization for the Prohibition of Chemical Weapons (OPCW) proficiency testing, for example.

“We have the rad and nuke lab, which provides logistical support for all the dosimeters of the military staff, operational and medical services. They have a lot of sources and we can test detectors, so we will test the GIFT detectors. Then there’s the chemical analytical lab which is focused on unambiguous detection of CWA compounds but also experienced in the identification of things like heavy metals and environmental issues.

“Finally we have the federal orientation lab which receives suspect samples for screening and dispatch. We do a lot of testing but also give a lot of advice to the military and sometimes to first responder departments.”

Katleen de Meulenaere sees the collaboration between national and international agencies as a massive benefit from the GIFT project and that these links will be maintained and even increased in the near future. “In terms of the CBRN lab it is important to have enough flexibility to see how we can help build new capabilities since we live in a changing world with changing threats. We have to try and collaborate more intensively with civil departments; it is becoming specialised, complicated and detailed so we will need to actively inform each other to foster sharing. This is also true in a Nato context, the development of a network is very important. We should go on participating with Nato, OPCW and in other international contexts, as it is necessary to work together to provide answers to tomorrow’s threats.”
CSI2: CBRN Crime Scene Investigation

©OPCW

38 CBRN Forensics
Dr Randall Murch,* professor at Virginia Polytechnic Institute and State University, on considerations for success in preparing for and initiating CBRN forensics programmes

Twenty years ago, the FBI created the world’s first forensics investigation programme for weapons of mass destruction (WMD) founded on the following principles, realities and vision:

- Forensics and attribution had not yet been recognised as a critical component of the national counter-WMD programme, but in time it would be. While not all threats and illicit plans and actions can be prepared for, anticipated, prevented, thwarted or mitigated, a robust investigative capability leading to attribution, including through forensic support, should be implemented.
- Law enforcement had neither fully recognised nor assumed a broader role in WMD investigations and prosecutions, nor assumed its rightful place as the leader and national integrator for the desired investigative, operational and forensic programmes, even though existing laws would have permitted it.
- Major special events, such as the 1996 Olympic Games and national political conventions, presented WMD targeting opportunities for adversaries. The US had a woefully inadequate forensic response capability. While certain smaller scale nuclear and chemical threats and events could be dealt with in limited ways, larger scale threats and events could not, and events involving biological threats would not have been at all.
- National-level capabilities in various agencies existed for nuclear pre and post-blast analysis, chemical weapons analysis for military and nonproliferation purposes, and legacy bioweapons programmes but none of these were organised, staged, purpose or resourced to robustly support forensic investigation which informed legal, policy, operational and other processes, decisions, actions and outcomes. Vertical integration (federal, state and local) was nonexistent.
- The capabilities that existed then, could not and would not have withstood rigorous adversarial review of the science, interpretations and conclusions as would be expected in a US court of law or on the world stage if forensic investigation and analysis supported US allegations or actions against a suspected perpetrator.
- The US required programmes for C, B, R and N that drew on existing programmes and assets in various agencies, which were assigned to related missions that could be leveraged quickly and well for forensic support. Duplication of programmes and effort would not be supported or acceptable. Relationships, shared missions and responsibilities had not been recognised.
- WMD forensic investigative programmes would have to integrate appropriate traditional forensic disciplines, to maximise the gain for WMD investigations, operations and intelligence gathering. Traditional forensic collection and analysis involving evidence potentially contaminated with very hazardous materials would require specially trained personnel, specialised equipment and methods, and facilities that could accommodate it.
- There were narrow and disjointed interagency constructs for cooperation, many barriers existed to the creation of an effective national WMD forensic enterprise, certain required agencies were not involved, and no one was clearly in charge.
- Significant gaps and shortfalls existed across the board, from the tactical to the strategic levels.
- At the time, forensic investigation was generally thought to be an after-the-fact endeavour, but the vision was materialising that, in reality, the value of forensic investigation is much broader in scope across investigative process and the ‘business cycle’ of perpetrators and persons of interest.
- The threat of C, B, R and N terrorism and proliferation had increased, particularly through what was being projected as loss or redirection from unsecured WMD weapons programmes and what was being learned from the pursuit and use of WMD by sub-state and apocalyptic groups.

These are still instructive today, whether prospectively or retrospectively.

Since 1996, much has changed. For example, the US has and continues to invest in a fully integrated multiagency and multidimensional programme. This continues to evolve to address emerging threats, technical opportunities, mission areas, and existing and new requirements, how response and coordination will manifest and what is needed for decision support. The US government has prioritised that holding adversaries at risk and accountable through attribution is a critical component of national counter-WMD capabilities; national strategies, policies and authorities are in place. Nuclear, chemical and weapons forensics have been firmly established and recognised as legitimate disciplines. Developers and practitioners are committed to incorporating forensic requirements and expectations into research, development, validation, transition, practice, communication and quality management to ensure effectiveness, robustness and confidence for customers and stakeholders at all levels.

Nuclear (radiological) and chemical forensics are well established through long-standing nonproliferation programmes while biological (microbial) forensics is maturing as a discipline. It is well realised that the three are not the same for many legitimate reasons and have to be treated differently. Actual case evidence has been subjected to respective analyses and legal, policy and command decisions have been made and actions taken as a result. There has been much collaboration between the US and certain other nations on WMD forensics in areas such as programme development and preparedness (training), evidence collection and analysis technologies and methods, exercises and decision support.

Peer reviewed papers are published in the open literature when possible, which strengthens acceptance of and confidence in the underlying science and its applications. Other nations have realised the value and need for such capabilities and established their own programmes which are tailored for their own purposes, while still more are considering such. While, forensic analysis and attribution is recognised, accepted and used to support nuclear and chemical weapons nonproliferation investigations and outcomes, the discussion has been elevated to the appropriate international fora to similarly incorporate biological weapons forensics and attribution.

Based on his own and colleagues’ experience and many ‘lessons learned’ over the past 20 years at national and international levels, the author offers some thoughts for those who are just beginning to consider or have begun instituting a CBRN forensic programme.
- First, ‘ready, aim, shoot’ as modus operandi is vastly superior to ‘shoot, ready, aim’, for both short term and sustainable success. Two good starting points are understanding, validating and aligning requirements of customers and stakeholders and conducting a systems analysis to understand: where are you are, where you need to be by when, and how are you going to get there?
Understanding requirements should include how forensic science does or would contribute to decision making in pertinent government agencies and processes. CBRN forensic programmes require substantial investment in personnel, science and technology, consumables, equipment, infrastructure, transportation and logistics, training and exercises and unexpected expenses. Unless resources are unlimited, a carefully thought through and executed strategy and plan with risk management options is helpful. Further, it should be accepted that there will be a substantial up front and continuing resource investment for a capability that is fundamentally for rare events.

Second, forensic capabilities must effectively inform questions that customers and stakeholders pose or need answers to, even if situational awareness changes and the fidelity of the answer which can be offered increases with time, otherwise the value is suspect or, and even if provided, will be discounted. Forensic science can contribute to answering most of these questions. Investigators, prosecutors and operational commanders’ questions can include: Did a crime/event of interest occur? What happened? How did it occur? When did it occur? Where did it occur? Why did it occur? Who was involved or is responsible? What evidence exists? What does it tell us? How strong are the links? How reliable and credible is the evidence? What alternative explanations are there for the evidence? Can we defend our conclusions and actions?

Forensic science contributes to answering all these questions and can provide essential, independent information that strengthens the quality and confidence in the answers. For planned or new programmes, objective assessments should be conducted to determine how well existing CBRN forensic capabilities can, or planned capabilities could, address these sorts of questions, including strengths, weaknesses, gaps and opportunities.

Third, one should not assume that existing forensic laboratories have the infrastructure, resources and personnel with the formal training, knowledge and expertise to properly and safely conduct and effectively communicate CBRN forensic analyses, results and interpretations. Dealing with very hazardous materials and associated evidence requires special expertise, certifications, equipment and laboratory configurations, safety considerations, evidence logistics and preservation and storage.

Further, it should not be assumed that just because someone understands nuclear weapons materials, design and effects, or chemical weapons decontamination, transport or analysis, or the diagnosis and effect, or the genomics and bioinformatics of highly pathogenic microbes they necessarily understand forensic requirements, processes and expectations. Exploiting CBRN contaminated physical evidence for traditional forensic results of investigative or intelligence value (eg, latent fingerprints, human DNA, documents, digital media, trace evidence and materials) requires CBRN/hazmat trained forensic personnel, and specialised instrumentation or equipment, methods, safety programmes and facilities.

Fourth, evidence collection should seek only that of probative value and maintain integrity and accountability. Analyses
performed on CBRN evidence should be properly validated, accurate, reliable, repeatable and defensible. The science and practice being performed should match the outcomes being sought, and stay within the bounds of what the science is capable of. Validation of methods and protocols should meet forensic requirements, which incorporate legal and other priorities. The attributes and limitations should be understood by the performers and communicated so that consumers of forensic information will factor these in as part of their decision calculi.

The expectations of customers and stakeholders, most of whom are not scientists or otherwise experts in these fields, should be integrated with the components of forensic investigation, from scene investigation through reporting. It is prudent to ensure that this in place before evidence is collected, processed, analysed and reported on - and not afterwards - though some situations can be accommodated if the use of the science is limited. In the US and elsewhere, the capacity of forensic science to withstand withering external scrutiny, such as in a court of law or a high stakes policy forum is extremely important. If these requirements are not met, the entire system is at risk for loss of value and impact, independence, confidence and utility.

• Fifth, for best value, CBRN forensic capabilities should be scalable and adaptable to the types, range, dynamics and uncertainties of the scenarios that the performers and beneficiaries expect to encounter. One effective approach towards a desired end state is to use a set of realistic scenarios in tabletop and field exercises. These scenarios might bracket very small scale and focused events and a large scale, massive impact event or one for which a combination of CBRN threats has been presented or the adversary has used creative scenarios in tabletop and field exercises.

Alternatively, scenarios could accommodate situations which support intelligence gathering on a group suspected of CBRN development, acquisition and use, hoax situations or post event considerations. This methodology can inform programme planning, implementation, investment strategies, resource and risk management. One set of key issues that would be illuminated from this analysis is the partitioning and positioning of field-deployable and fixed assets. Concomitantly, this would inform thinking on the need for rapid, partial answers that can be delivered from the field versus deeper, more informative answers that require more time and sophisticated laboratories.

• Sixth, unless one agency has or can acquire everything necessary, an interagency CBRN forensic construct for planning, preparedness, response, resource leveraging and command, control and communication should be carefully considered. If one rolls up everything that would be required or needs to be accommodated from what the author has communicated thus far, for most if not all countries, more than one agency has the necessary expertise, resources and facilities. Thus, to maximise return on investment and minimise duplication of effort, the best of various agencies can be fitted together under the command and control of a single agency or interagency leadership council. Further, if any one nation cannot afford everything it has decided it needs, bilateral or multilateral partnerships could be considered. This might require creative and patient negotiation on several levels but could be worthwhile the investment of time and energy.

In any case, engaging with countries that have successful programmes and have been down this road already, would be valuable at the start or at specific points along the way. This will save time and manage resources, maximise performance and increase the likelihood of a successful and sustainable outcome as desired. For many reasons and realities, CBRN forensic programmes are more complex in a number of dimensions than they initially appear to be.

Finally, here are some considerations, which new starters might contemplate for early design and implementation and which will help define how choices and investments might be made:

• A competent CBRN forensic programme is a major up front and enduring investment. It encompasses personnel (specialised credentials, knowledge, skills, abilities and possibly incentivisation), specialised training and exercising (unit, sector and enterprise), equipment, consumables, logistics, field, laboratory and staging infrastructure and operations, safety, and knowledge management, and decision support to name a few. Need, affordability, required readiness and expectations for responsiveness will drive investment and implementation decisions.

Programmes will have to be maintained, and likely evolve. Appropriate resource planning and investment, as well as change management, are necessary. Decision makers should accept the fact going in that CBRN forensics is an expensive proposition.

• At least initially, a CBRN forensic programme may not warrant a full time presence. It is also possible that even when a programme is at the desired equilibrium, full and part time elements could be needed. Part time elements will need to stay focused on their principal missions while being available and focused on demand. These situations can be accommodated by aligning the part time duties, responsibilities, expectations and outcomes with forensic support as closely as possible with full time assignments. Closely parallel capabilities are often present in civilian forensics, public health, agricultural and environmental agencies, specialised national laboratories, and military medical and CBRN programmes that can be leveraged and knitted together, then staged, prepared and maintained or called up as required.

• Adversaries, the nature of threats, possible scenarios and threat presentations, and access to advancing technology and technical knowledge changes all impart required evolution, adaptability and agility to CBRN forensics programmes if currency and effectiveness is to be expected. As a framework for thinking about managing change, one should contemplate the potential, which is not a bridge too far, with respect to bioterror and dual use technology and knowledge. Today and looking ahead, not only will bioforensics programmes have to address current threats and challenges, but those potentially created or influenced by the realities of rapidly advancing and universally available, legitimate life sciences capabilities that can be redirected for illicit purposes.

Nefarious uses could derive from powerful genetic engineering technologies (eg CRISPR genome editing), improved bioprospecting and exploitation of natural diversity, very small footprint biodice and production systems (eg DIY), creative denial and deception, and synthetic biology. Biodefense programmes are becoming aware that they will have to become more agile and adaptive to develop and make available measures to prevent, thwart, protect and recover from new threats. The same is true for the bioforensics component.

The future presents many challenges indeed, and may, perhaps, seem overwhelming. Proper prior planning and thoughtful, step-wise, ‘lean-forward’ implementation to the desired end is a prudent approach, however. Fully understanding and modelling the problem-capability space up front is advantageous. Maximising preparation and collaboration and system integration should occur. Instituting regular, critical reviews and adjustments will assist with change management. Taken together these will reduce the chances that a suboptimal programme is established, which cannot keep pace and meet expectations when it matters most.

*Since leaving the FBI, Dr Murch has been involved in developing new capabilities, extending the CBRN forensic mission to additional agencies, participating in national level reviews, improving capabilities at the interfaces of science/operations/law/intelligence and policy, publishing peer reviewed scientific papers, making presentations (microbial forensics) and conducting international outreach.
The generic integrated forensic toolbox (GIFT) project has now completed its research and data gathering phase, having engaged with first responders and forensic specialists from across Europe. End user workshops have been held in The Hague, Netherlands; Bristol, UK; Rome, Italy; and Riga, Latvia; with first responders attending from 12 member states. These responders provided invaluable feedback on their current national capability, gaps in their response procedures and the GIFT consortium’s approach.

Certainly these workshops demonstrated one fundamental truth about CBRN forensic science − in Europe at least − and that is that very few first responders have specialist CBRN forensic knowledge or experience. Attendees included individuals with specialist forensic knowledge and others with impressive CBRN backgrounds but apparently the twain never meet where front line responders are concerned.

The project’s research work package (WP2) is now complete. As a result the outcomes of this work package are tangible and the R&D is well under way as the next phase gets going, incorporating the feedback from the research. In essence WP2 focussed on two main objectives supported by a number of subtasks. The first of these was to set the incident scene by capturing a number of credible and feasible CBRN scenarios that could require forensic investigation. The second objective tried to identify current best practice in CBRN forensic science within EU member states, and future solutions for operational capabilities. This process of identification for European CBRN forensics has now led to the development of a set of road maps, which can be used by both high and low capability member states to develop an adequate CBRN forensic response capability based on their available resources and threat spectrums.

To meet the first objective − creating a set of CBRN scenarios that could be used by the forensic community − the GIFT consortium collected existing threat scenarios rather than reinventing the wheel. In total 15 scenario sets were amassed, primarily from within the EU with some national planning scenarios included. Once gathered, these scenario sets were critiqued to assess their suitability for GIFT’s purposes. Those deemed suitable for the project delivered a substantial cross section of the CBRN threat spectrum for European member states.

The scenarios quite logically tended to focus on the actual release of CBRN material into the environment, which would then require a
Very few first responders across Europe have specialist CBRN forensic knowledge or experience

response to save lives and mitigate the consequences. Such incidents would certainly involve a forensic response, which was not factored in when these scenarios were originally developed. Other types of CBRN incidents that might require forensic investigation, were missing from the scenario sets however, for example the discovery of an improvised chemical or biological laboratory. In order to provide an inclusive set of scenarios for the forensic community such incidents were developed and incorporated into the scenario sets.

The GIFT consortium needed to ensure it had a comprehensive cross section of the threat spectrum, covering most if not all conceivable challenges likely to be encountered during a CBRN forensic investigation, so that these scenarios would support the future development of CBRN forensics. Not only did this involved filling incomplete capability or knowledge gaps but in some cases it meant writing entirely new scenarios to include preparation of CBRN agents and/or weapons, deployed weapons and released weapons. The end result was a dedicated and comprehensive template with a total of 20 scenarios, comprising six each of chemical, biological and radiological and two nuclear scenarios.

These scenario sets were then used to satisfy the second main objective of this work package; namely the development of CBRN forensic roadmaps (as well as making them available to the forensic/CBRN community). In developing these roadmaps it was important to identify and understand the current capability gaps in various nations across Europe.

The GIFT consortium held a gap analysis workshop in June 2015 at the Netherlands Forensic Institute (NFI), utilising the developed CBRN scenario sets. A broad spectrum of organisations from all over Europe attended including the International Committee of the Red Cross; Czechoslovakia’s National Institute for NBC Protection; the UK’s Defence Science and Technology Laboratory (Dstl); Bundeskriminalamt from Germany and the Dutch Ministerie van Defensie.

For obvious reasons identification of gaps is essential in developing a capability, but simply identifying the gaps doesn’t necessarily lead to a set of roadmaps showing the way from the current to the desired capability levels. It was therefore important to work on a number of subtasks to build these roadmaps.

To follow a map you need a starting point. So firstly GIFT had to establish the current capability levels of various nations across Europe, no easy task given the disparity in wealth, economics and public services across the EU. The current state of the art for CBRN forensics was initially determined through the workshops mentioned earlier, and through questionnaires that covered a broad range of regional differences and approaches to CBRN forensic science. This approach provided keen insight into the member states’ current CBRN forensic capabilities and the differently implemented operational models. The disparities in capability and operating models were eventually subdivided into three levels, namely low, average and high capability. Once the point of departure was set, GIFT needed a clear line of sight to the possible destinations for both low and high capability countries. These destinations were established by analysing both near and far future developments in forensic science and technology, and the needed/required solutions as indicated by the European end user community.

The culmination of 12 months’ research is the generation of four different roadmaps that describe the forensic tasks for both high and low capability nations (medium being an extrapolation from the two extremes), and the required actions needed to reach an improved CBRN forensic response capability. These roadmaps are primarily intended for the EU member states and their forensic communities, but will also serve the GIFT CBRN project by validating the technological and procedural developments over the lifespan of the project.
Dangerous clues

This article explores the ways in which the military has been using forensic science and the forensic capabilities of sampling and identification of biological, chemical and radiological agents (SIBCRA) teams. There is a lesson to be learnt from analysis of the way in which silos within the military may mean that the potential for SIBCRA teams has not been as well used as perhaps it could have been. For reasons of operational sensitivity, no single country’s SIBCRA capability will be looked at in detail but rather discussion will be generalised or drawn from the Nato guidance.

All contacts leave a trace, according to the great forensic scientist Locard. As a result, there is often information that can be extracted from evidence that links traces (DNA, finger marks etc), trace carriers (phones, clothing, surfaces etc) and trace sources (people, locations etc). You don’t need to have watched CSI New York or NCIS to know that this has been a source of great investigative capability for modern police forces across the globe. TV generally shows it being used in a basic comparative method, in a sadly true reflection of the way in which some forensic services have declined. This is where a sample is compared with another sample to demonstrate they are of the same provenance. More advanced scientists venture into the more controversial but also highly valuable area of investigative forensic science, where you have no comparative sample but try to elicit information from unknown samples and traces. The Sherlock Holmes version of this would be finding a trace of soil on an explosive device and analysing it to try and determine where it might have originated [Dr Lorna Dawson at James Hutton Inst rocks at this! Ed.].

Forensic science has been applied to explosive devices since 1800 at the latest, with the French development of a weapons intelligence capability under the supervision of the polymath Citizen Monge. But the capability has generally been civilian and its military equivalents, such as weapon or technical intelligence teams, were more focused on the effectiveness of captured weapon systems. The increasing occurrence of asymmetric tactics in the complex, congested and contested military environment forced a reconsideration of this. If you can’t get the opponent to face you on a battlefield, then you need to pursue and find them by other means. When they are hiding among a civilian population it is only natural that forensic investigative techniques come to the fore. Usually considered to be material and personnel exploitation (MPE) forensic science in the military has grown to a stage where many countries have deployable forensic labs, teams to recover evidence and develop doctrine. An MPE or forensic capability includes an evidential recovery component which may be accredited to the civilian ISO 17020 standard. Analysis of the evidence is conducted in the second part of the capability, the forensic exploitation lab. This may be accredited to ISO 17025. These two ISO standards are subject to a little controversy as they are really test house standards, and require interpretation and guidance to apply them to forensic science.

While MPE might be unfamiliar to some readers, SIBCRA teams should be more comfortable territory. As SIBCRA is reviewed keep in mind MPE. SIBCRA is a fascinating capability that has evolved over the years from a starting position of realising that the use of strategic weapons needs to be verified in order to justify the resulting actions of the party that has suffered the insult. If a country decides that its response to a chemical attack is to launch nuclear weapons, then it needs some pretty strong evidence both for its own purposes but also to validate its actions in the eyes of the world and the UN in particular. So SIBCRA teams have often been seen as strategic assets, held back, behind the areas where the materials might be used, and then deployed in response to allegations of use. This can feel inefficient, especially if they are held back in another country, but the purpose is generally to prevent the teams becoming victims or contaminated themselves.

SIBCRA teams can vary from country to country although Nato through allied equipment publications (AEP) establishes some commonly accepted standards for key components of the capability. The SIBCRA team focuses on the recovery of samples and the lab to process the samples. While traditionally samples would be taken back to
a national lab, recent years have seen some countries produce deployable labs to speed up the exploitation of the sample and to avoid the risks of taking samples long distances and to the homeland. The strategic nature and manner of their operation means that they may not give any intelligence to the local commander, and so they do not remove the requirement for CBRN recce teams, although it isn’t unheard of for some SIBCRA teams to have been cross trained with CBRN recce teams.

Perhaps ghostly wisps of déjà vu are teasing you as you read. Both of these capabilities have sampling teams, a recovery and transportation component and an analytical lab. They both input their intelligence at a high level rather than the tactical level. SIBCRA teams follow a painstaking process of sampling and documenting their samples because of the impact of their intelligence – or perhaps we could say evidence. So you would probably assume that when the MPE capability was developing and trying to address challenges like the transportation of potentially hazardous samples (eg explosives) one of the best starting points might have been SIBCRA teams – not least because some were specifically called military sampling teams or military specialist couriers.

The older and more cynical of you will be less surprised that many in MPE have been unaware of SIBCRA due to it being structurally outside their areas of responsibility. But there have been exceptions and there has been an interesting development with the increased attention on CBRN forensics, as a component of MPE.
CBRN forensics has been given a real platform by Nato and institutions like the Netherlands Forensic Institute, DSTL, AWE and LLNL which have really provided thought leadership. There has been exploration of both the forensic analysis of the CBR materials themselves, which can be considered a classic SIBCRA function, and the processing of evidence which may be CBR contaminated. This latter task is effectively MPE but in contaminated conditions. At this nexus between MPE and SIBCRA the obvious question arises, who should carry out this work? Potentially there is also a question of whether there is utility in this capability being used both domestically as well as for expeditionary military situations.

Briefly the lab processing component is necessarily dominated by the SIBCRA supporting labs. This is because once a piece of evidence is contaminated with a CBR material then very few labs can legally store and handle it. For most countries there is just a single CB facility and a single RN facility. Many more have no real capability at all and would need to rely on allies to support them. So where CBRN forensics lab capability has been explored it has tended to have a civil driving force and to be based in existing CBRN facilities. Unfortunately, that means that there is an initial separation of MPE facilities, which tended to be based out of explosive research units – of which there are plenty – and CBRN forensic labs, even though both may be administered by the same research organisation. Strangely economic pressures are currently tending to make sure that the civil developed CBRN forensic capabilities would be the natural support to CBRN MPE.

The situation is a little more challenging when looking at evidence recovery in a CBRN environment. Again, we can consider this as occurring in the civil domain for police/court purposes, military MPE or military SIBCRA. Starting with the military space it is hardly a revelation to observe that in an area as underfunded and unvalued as CBRN there isn’t space for duplication of effort. This economic pressure doesn’t wholly remove duplication and it can also introduce political pressures where more reasoned logical decisions would be preferable. So in an effort to inform such an argument, would a SIBCRA team be able to carry out CBRN forensics/MPE?

Traditionally, processing a crime scene is a mixture of documentation and on scene analysis. A SIBCRA team is already very well trained in the documentation of scenes and often receives training from police forces as well. While they may not use police/evidential packaging or markings, their process is very respectful of the chain of evidence. Cross contamination is second nature to them due to the practice of working with hazardous materials. Slightly more problematic is the fact that they are generally concerned about protecting themselves from contamination and some of their protective equipment, such as air purifying respirators, can cause a lot of trace and DNA evidence to be introduced to the scene. Most commonly this results from the expulsion of sweat/spit from exhalation valves. This is a relatively easy problem to address, though. A good SIBCRA team working to Nato guidelines would extract evidence to a reasonable level of forensic integrity.

Scene processing or analysis is more challenging. SIBCRA teams are mainly focused on the recovery of the CBR materials. This is not to the exclusion of other useful evidence, as documents and IT are often identified by SIBCRA teams as important intelligence to remove. They are not necessarily as well trained in processing without bias through a scene. Looking for trace evidence, body fluids, finger marks and DNA are all quite tough skill sets which can appear straightforward. It is true that anyone can learn to lift a mark in minutes – but to find and lift them consistently well takes a lot of experience and training and then doing so in protective equipment is an even greater challenge. SIBCRA teams already have a pretty high training burden and it’s not unreasonable to ask if this is a step too far for them. But would the burden be any lighter for a bespoke CBRN MPE team?

MPE teams have been a bit of a fluid development. Ranging across levels, at the lowest everyone is a collector and small kits have been designed for the conventional collection of evidence. This is the recovery of a trace carrier rather than more detailed processing and is a ‘best of a bad situation’ approach where otherwise evidence might be lost. Levels above that are teams with military police, intelligence and often explosive specialists. Although these have experience, it is fair to say that at this stage they are still some distance off the level of a high end police counter terrorism forensic team. This is partly a problem of training and equipment and partly one of currency – with withdrawal from Afghanistan there are far fewer opportunities to practice. As all military staff in Nato have a basic CBRN proficiency, it is not un-thinkable to see the simplest solution as them just doing their work but in CBRN equipment.

Weighing the two options for CBRN MPE/forensics instinctively a third option arises. With the training burdens faced on either side and the challenge of currency and exercising it is perhaps best that neither SIBCRA or MPE take on the role themselves. Rather taking a modular approach a CBRN forensic capability might best be delivered by a team drawn from MPE, SIBCRA and other relevant units. The challenge this presents is interoperability and exercising enough to make sure such ad hoc arrangements can work efficiently. That is no small effort but worthy of exploration. It would be an extremely interesting topic for war gaming and defence experimentation to see which of the methods would be most appropriate and if a hybrid modular option could be made to work.

Traditional military respirators can make a DNA mess of the scene due to leakage from the exhalation valve ©CBRNe World
RAMEM has been working within GIFT on developing and validating a novel detection technique focused on detecting possible chemical contamination at a crime scene.

The RAMEM DMA (differential mobility analyser) technique is an ion mobility spectrometry technique, and RAMEM has been testing a higher resolution to try to reduce the false positive and negative rates, as well as a new ionisation technique. In the case of the DMA, the ion source is ultraviolet (UV) light. We have been working on methods to analyse the air at a crime scene and identify potential chemical agents present. So far, the results obtained have seen better resolution and increased sensitivity, with lower limits of detection and quantification.

Reproducibility has been improved by shortening the ion pathways and consequently, minimising the probability of ion clustering. Detection of explosive substances using a UV ion source and DMA has shown promising results.

It is important to underline the importance of these results in explosive detection using UV ionisation as an ion source for explosives. It is also important to emphasise that the lower vapour pressure explosives have been detected as well. Just a simple laboratory heating plate raises the temperature sufficiently to allow detection of PETN, TNT, ammonial (ammonium nitrate/TNT or nitrometane/aluminium), ammonium nitrate and RDX.

The project has focused on some of the challenges from the lower vapour pressure explosives, including an appropriate sample introduction system, which is needed due to the special characteristics of the analytes. Several chemical toxic substances, some of them considered as chemical weapon agent simulants have also been detected.

The DMA could be used on site, to analyse air extracted from within the crime scene and detect potential chemical contamination. The information fed back from the toolbox will enable decisions to be made on the usage of personal protection equipment and treatment of casualties, as well as protocols and procedures.
Forensics and Privacy: beyond the right to be forgotten by Iris Huis in 't Veld, researcher at Eticas Research & Consulting

Discussions about privacy are everywhere and there are countless examples of cases where privacy has been unacceptably infringed. Edward Snowden revealed how the US government is engaged in surveillance programmes that undermine the right to privacy. The hacking of the dating website Ashley Madison caused the release of users' personal information including real names, home addresses, search history and credit card transaction records, while the company InBloom, which offered a cloud service for student data, was shut down because it shared data with third parties without parental consent.

What does this have to do with forensics? It might seem counter intuitive to discuss forensics and privacy together because, while the legitimacy of identification is questionable in some of the cases described above, identification is a fundamental goal of forensics. It is easy to disregard the importance of privacy in this context, but this would be based on a misconception of privacy.

What does privacy mean for forensics? The topics of privacy and data protection are almost inseparably linked to data-intensive technology. Technology is data-intensive when the data is fundamental to the functioning of the technology or is generated in the process. When data about people is involved, rights and values should be considered in order to prevent negative consequences for those individuals.

Considering that forensic investigations involve dealing with personal data – including fingerprints and DNA – the requirements for data protection also applies to forensics. Personal data can contain sensitive personal details or lead to assumptions about the individuals involved. In the wrong hands, or when misinterpreted, data can have disastrous consequences. Negative consequences include stigmatisation, discrimination and wrongful convictions which can prevent justice from being served. Privacy is a human right, often framed as the right to be forgotten, as well as a societal value that allows people to maintain a private space in which to be themselves. But above all, what privacy means is context dependent.

Nothing to hide
How can privacy be understood in the context of forensics? A basic question to ask is: do we have the right to be forgotten? The answer depends on the interpretation of the premise. Privacy is often downplayed by the argument that you should not be worried about privacy when you have nothing to hide. The assumption is that privacy is about hiding things – so if you have done nothing wrong, you do not need to fear a privacy infringement.

This definition of privacy as secrecy does not reflect what privacy means in terms of data-intensive technology and certainly not what it should mean within a forensic context. Privacy is not about hiding away from an investigation or being secretive about it. It is more about the right to protect and be protected from the harmful consequences of an infringement of privacy.

The lesson learned here is that values and ethical considerations concerning data protection – such as minimising the data collection where possible - should be taken into account.

This all adds to the responsibilities of the forensic data management chain. Emotional factors, like uncertainty, and time pressure, especially at the crime scene, can cloud judgement and affect decision making. Altogether, this places a heavy burden on the decision making skills and moral judgements of the individual agent. This can be solved with protocols and training, but a solution can also be found in the design of the data technology itself.

Privacy by design
The idea of embedding privacy proactively into the technology itself – making it the default – is the core of the design philosophy of Privacy by Design. When privacy risks and vulnerability points are identified at an early stage of development, the information can be fed back into the development process and solutions can be embedded in the design.

Within the GIFT consortium, technology and protocols are being designed to enable CBRN forensics and support decision making at the crime scene. There is an opportunity to foresee the data management requirements and make responsible design choices at the outset.

When privacy – along with other relevant ethical values – are embedded in the design of the toolbox it will help to minimise risks. The aim is to create a strong socio-technical toolbox to aid the CBRNE forensics teams in ensuring privacy issues are maintained along the chain of custody.
Mobile CBRN Labs at the Point of Need

E-N-G is the U.S. leader in mobile laboratory design and production. We have delivered over 400 Mobile Laboratories worldwide since 1977 — more than any other US manufacturer.

These versatile, easy-to-operate labs allow fast, on-site identification or confirmation of CBRN hazards and threats. E-N-G mobile laboratories are also effective in quickly determining on-site the extent of contaminated areas and in monitoring the progress of remediation efforts.

The MobiLab™ line includes vans, trucks, trailers and containers. Applications range from general-purpose and chemistry to BSL3-ready and CBRNE threat detection and analysis.

Scientists are on staff to assist with workflow design, instrument specification and laboratory practices training. MobiLab systems support procedures ranging from screening to certified testing methods.

Customers include US EPA, DOL, Army, Navy, Homeland Security and other public agencies and private companies.

Fully-engineered base models include electrical and environmental systems, lab support equipment
Lab-grade interior finishes for easy decontamination
Models are instrument ready and turnkey systems are available
Models are easily customized to meet specific requirements
BSL1, 2 and 3-ready models

Applications include:
- CBRNE Threat Detection and Analysis
- Public Health and Research
- Environmental / Air Quality
- Industrial Chem & Bio
- Education, and more

E-N-G is your partner for state-of-the-art mobile solutions. Call us to discuss your unique requirements.

E-N-G is a PositiveID Company
PositiveID develops detection and diagnostics capabilities for Point-of-Need (PON) applications, including its M-BAND autonomous monitoring for biological weapons (licensed to Boeing) and FireflyDx handheld molecular diagnostics.
Introducing... 
Handheld *Through-Barrier* Chemical Identification

- ID through opaque and coloured plastics, dark glass, paper, wrapping, sacks and fabric
- Assess and analyse samples without tampering with packaging
- Seals remain intact - Evidence is preserved
- Accurate ID of chemicals and mixtures in ~1 minute

[www.cobaltlight.com/resolve](http://www.cobaltlight.com/resolve)