

# Secret Agent

Dr Vahid Majidi, Assistant Director of the FBI's WMD Directorate, tells Gwyn Winfield about uncovering the agents that would do us harm

It is no surprise to say that the events of 9/11 and the anthrax letters that followed them caught the world napping. A cosy view of what was "accepted and likely" was quickly shattered and a new world order was let in. One of the intelligence agencies that found itself cast as scapegoat was the Federal Bureau of Investigation (FBI), one of America's bastions of national defence. A lot has happened since then. One of the most obvious changes has been the creation and evolution of the FBI's WMD Directorate, which was a direct result of the failure to anticipate and interdict the terrorist forces.

Now the FBI is far stronger, in terms of both intelligence and response, than it was five-and-a-half years ago; prepared to use all the weapons in its arsenal to stop the terrorist – either home grown or international. The emphasis on the terrorist is important as, in terms of CBRN defence, it is its *raison d'être*. If there is a CBRN alert in the US the FBI is the lead agency if it is a terrorist attack, whereas the police lead if it is criminal and the Environmental Protection Agency (EPA) if it is environmental.

This breakdown ensures that if it is a major event – and terrorist attacks by their very nature are major events (psychological if not physical) – then the response can be nationwide, rather than regional or local. "The FBI's overriding priority is to protect America from terrorism attacks," said Dr Majidi. "Our mission is to identify and disrupt potential terrorist plots by individuals or terror cells, freezing terrorist finances, sharing information with law enforcement and intelligence partners worldwide, and providing strategic and operational threat analysis to the wider intelligence community.

"The FBI has primary jurisdiction and has been the lead investigative agency in terrorism matters since an

Executive Order in 1983, as evident in various U.S. federal statutes and executive orders. Recent Presidential Decision Directives (PDD) 39, 62, and 63 highlighted the growing threat of WMD; PDD-39 reaffirmed the FBI's mission as being the lead law enforcement and crisis management agency in response to terrorist acts, while PDDs-62 and 63 detailed a program management approach to counter-terrorist investigations and call for a national effort to secure US integrated infrastructures."

## Lead agency

The FBI's jurisdiction is not limited to just national matters, however; they have a legal remit for federal jurisdiction in foreign countries, once the host country has agreed, and can use FBI resources to conduct investigations in the host country where the crime was committed. That provides the grand strategic framework, but what about the tactical? Dr Majidi explained: "One of our big roles at the CBRN scene is to co-ordinate. Our main objective, however, is to prevent. If we get to a point that we need to respond to an attack, our role shifts and we co-ordinate with other government agencies, as well as local law enforcement, while also deploying all our assets to deal with the scenario. We are not into consequence management – we are not into setting up a perimeter for example – but we have to respond to an attack. We want to make sure we provide assistance to whoever needs help, then gather evidence and follow it. We have a significant amount of co-ordination with first responders and law enforcement, as well as internally, so we can deploy the right team at the right time."

The FBI's teams clearly sprang from the same primordial alphabet soup that the military use; there is the WMDOU, HMRU, BAU, CMU, CRU, HRDU and EU

to name a few (or, to those outside the pale, the Weapons of Mass Destruction Operations Unit (WMDOU), Hazardous Materials Response Unit (HMRU), Behavioral Analysis Unit (BAU), Crisis Management Unit (CMU), Crisis Response Unit (CRU), Hazardous Devices Response Unit (HDRU) and the Explosives Unit (EU)) To the casual observer it may seem odd that an agency that claims it has nothing to do with consequence management has a Crisis Management Unit and a Crisis Response Unit. Dr Majidi explained the confusion: "The two units reside in the same group and work towards the same goal. The CMU is the unit that puts together a command post and is responsible for the technical guys that bring the computers and hi-tech gadgets; their job is to enable communication and make sure that the FBI can co-ordinate with the other agencies."

The role of the FBI is one, primarily, of terrorism but, as is often the case, this may not be announced until hours after the event. The last thing that anyone needs is a jurisdiction issue over whether that burning tanker is an environmental issue, a criminal act or a terrorist attack. Equally, there may not be the smoking tanker that provides clues to the time and agent involved; covert releases are by their nature clandestine and may not provide clues to their origin. "In the example of a covert release of a biological agent, an invocation of a different type of response would be seen, typically driven by the public health community," said Dr Majidi. "By its nature, a covert release may not be accompanied by any articulated and/or known threat and the presence of the biological agent may be discovered through the presentation of unusual signs and symptoms, in individuals who self-report to local hospitals. In this case, there is initially no crime scene for law enforcement



*"I told you not to park it here!" The FBI WMD directorate investigates any potential terrorist CBRN activity ©FBI*

personnel to respond to. The criminal act may not be revealed until days have elapsed, following the identification of the agent, coupled with preliminary results obtained from the epidemiological inquiry conducted by the public health sector. In the example of a covert release, the public health sector is responsible for making the necessary notifications to the law enforcement community. In a public health investigation, the FBI will concurrently conduct a parallel investigation, until an act of terrorism can be definitively ruled out. If something smells or tastes like terrorism, then the FBI will start the process. We will come up with an immediate resolution and the moment we believe this is not a terrorist attack and is an environmental disaster, for instance, then we turn everything we have collected, such as the evidence and the scene management, to the right agency."

Yet the lines between terrorism and criminality are blurred. Often terrorist groups are heavily involved in narcotics, kidnapping, money laundering or other forms of criminal activity that will help them fund their activities. This stops both groups fitting into a neat pigeonhole, and the information that might be needed to interdict these groups could fit across agencies like the FDA, FBI and law enforcement. "Absolutely right," agreed Dr Majidi. "We recognised this early on and every

fielded office has a link into an entity called JTTF – Joint Terrorism Task Force. The JTTF gives you membership into a range of local organisations – including local law enforcement – where we do come and talk. While there might not be a direct terrorist nexus, it can provide us with intelligent information that might lead us into a terrorist or WMD nexus. We work this at a local level where they are co-ordinated through a national HQ entity and our job at the WMD directorate is to constantly be in touch with our 56 field offices and through them the JTTF, and our folks are involved throughout the whole process. Any of the cases that might lead to someone who is a terrorist interested in WMD might not start because we thought they were a terrorist; we look at ancillary issues that might ultimately lead to terrorism or WMD."

Dr Majidi went into more detail: "The FBI created the National Joint Terrorism Task Force (NJTTF) to enhance communications, co-ordination, and co-operation between federal, state, and local government agencies. The NJTTF provides a point of fusion for terrorism intelligence and further provides support to the FBI field office JTTFs located throughout the United States. One of the critical operations of the NJTTF, is to hold a daily counter-terrorism intelligence briefing for all NJTTF members and both NJTTF and JTTF members have

access to FBI database information systems including the FBI's Automated Case File and the Guardian tracking system. In addition, the FBI participates in the National Counter-terrorism Center (NCTC), the National Virtual Translation Center (NVTC) and the National Counter Proliferation Center (NCPC). NCPC was established to co-ordinate and oversee the intelligence community's efforts against the proliferation of weapons of mass destruction. The NCTC serves as the primary organisation in the United States Government for integrating and analysing raw terrorism intelligence; intelligence either acquired by and/or possessed by the United States Government while the NVTC serves as a clearinghouse to facilitate both the timely and accurate translation of foreign intelligence for all elements of the US Intelligence Community.

"Another example of the FBI's continued commitment to sharing information with members of the greater US Intelligence Community is the creation of the Weapons of Mass Destruction Integration and Targeting Unit (WMDITU)," he continued. "WMDITU is a specialised unit whose mission is to integrate US Intelligence Community operations and FBI counter-terrorism investigations to identify, assess, target, and defeat international WMD terrorism threats to the United States. WMDITU has

# Secret Agent

established itself as the foundation and formulated strategic partnerships between the FBI National Security Branch (NSB), the Central Intelligence Agency (CIA), the National Security Agency (NSA) and select members of the US Intelligence Community which target terrorists attempting to create, access, purchase and ultimately utilise a WMD. Exercising a unique functionality as it is embedded in the CIA/CTC/WMD component, WMDITU serves as the designated conduit between the CIA and FBI on all WMD terrorism matters. Within the FBI WMDD, WMDITU is specifically responsible for operational liaison activities between the FBI's International Terrorism Operations Sections (ITOS I) and (ITOS II), CIA/CTC/WMD, the Laboratory Division, and other FBI WMD-related components, to co-ordinate active international WMD terrorism investigations and WMD terrorist targeting initiatives."

## Death by committee?

Yet what is to stop this being "death by committee"? The world is full of people who gain their sense of worth from being on these committees and withdrawing information without putting everything in. This is especially true at the local level where hardworking members of local law enforcement may be suspicious of losing cases to the FBI if they release information – and with those cases go the kudos and promotions. Assistant Director Majidi agreed that this could be a problem and that they had gone to great lengths to ensure that every one was 100 per cent honest. "We make sure that there is a net benefit that goes to the locals to make sure they get something from the JTTF. We allow them access to first tier intelligence from the JTTF – the sort of stuff they wouldn't otherwise have access to. This means that working with JTTF allows them to stop things that would otherwise come to fruition if they were working with just their own state assets and resources; it's a win-win. We get full participation from all agencies, big and small, and this is a reason for their success and there is a great deal of enthusiasm. I see your concern – that

this could be seen as a way of sidelining them and ensuring that the FBI get something out of it, but at our briefings we always stress this case was only solved with the help of locals and there is always a local sheriff, or law enforcement official, at any JTTF briefing to provide information – everyone gets credit."

The FBI faces the same quandary that other law enforcement organisations face: whether saving lives is more important than catching the perpetrator. Unlike explosives, a CBRN attack is an ongoing event, and the source of the contamination might need to be contained to stop further individuals being affected by the plume. The most common way to mitigate it would be to spray it with gallons of decontamination solution, neutralising and/or containing the agent – yet this has the side effect of destroying evidence such as fingerprints. Does the FBI have a silver bullet to defeat this bugbear? "Unfortunately that [the destruction of evidence] could be the case," agreed Dr Majidi. "First we must make sure that anyone who could be in harm's way is taken to a safer location. Even if life is threatened we will move people from the hazard; the next step is worrying about the sample and having scene control. If the plume could be putting a lot of people in danger, our concern is to make sure we get them out and don't worry about the sample till we have a better control. Sometimes as we secure the scene at an event; if it is plume or a release, then we may lose some evidence, but evidence is secondary to the safety. I know it is not the 'answer', but we have to look after people first."

Perhaps the second biggest whodunit case in history, after Jack the Ripper, is the 2001 anthrax letters. The perpetrator of these has still not been brought to justice and, from the outside at least, it looks as if the case has gone cold. Are the anthrax letters a failure that needs to have lessons-learned drawn from them? Or are they symptomatic of the sort of CBRN cases that law enforcement agencies face? There are parallels with the Litvenienko Polonium poisoning case in the UK, where the murder weapon trail can only

be followed so far before it goes cold. Or is it just the fact that this was so unexpected that procedures, now second nature, were so unknown then that it was purely ignorance of the threat that got the case of to a cold start? What positives does the FBI take from the anthrax letters? "One of the outcomes of the anthrax letters was a clear understanding that we did not have all the tools necessary to deal with a problem of this magnitude," said Dr Majidi. "These events, as unfortunate as they were, have been used to develop a new programme – a Chem/bio unit within the lab – and this Directorate has been created directly because of the kind of stuff that the anthrax promoted and we are now organised to respond to these issues. It has to be remembered, though, that in some instances law enforcement cases can go a long time before a reasonable conclusion is made; the Attorney General recently announced a civil rights case that occurred many years ago and the individual was indicted, four decades later. So, as much as we might like to have a quick and speedy resolution, we have to be patient and make sure that we do this the right way."

While the anthrax letters have been the largest biological attack on US soil, the FBI has not been short of analogous cases. Despite not being its core concern, it took a lot of lessons from the Katrina disaster – specifically those that looked at how organisations dealt with mass-casualty catastrophes – and the Bureau has now set up a Principal Federal Office concept to try and ensure the flow of aid and assistance is well managed and co-ordinated. This emphasis on co-ordination will be the saving grace if there ever is a major CBRN incident; the paucity of cases and variety of threats make it difficult to plan for every eventuality, meaning a great deal of the response to the event will have to be done "on the hoof." It is only when you have a firm understanding of your fellow agencies and their capability does this ad-hoc response become a major advantage rather than disadvantage and a major attack will show the strengths, or weaknesses, of the JTTF and co-ordination work that the FBI has been doing.