

Admiral Jay Cohen, Under Secretary of the US Department of Homeland Security Science and Technology Directorate, explains to Gwyn Winfield how they are making the future possible



Dr Futurity

The Department of Homeland Security (DHS) is an enormous entity. Stretching from sea to shining sea, from Coast Guard to Transport Security Agency and from here to eternity, DHS is a beast amongst government departments. The element of it that keeps it strong and ready for future fights is the DHS's Science and Technology Directorate (S&T). This has a billion-dollar budget of which the vast majority is devoted to research (approximately 20% overhead, 60% transition research, 20% basic research and 10% innovative research) and the vast majority of that research budget goes into Chem, Bio and counter IED - DHS S&T is a major supporter of CBRNE research.

Yet DHS S&T is not the only supporter of CBRNE research, there are other labs covering many of the same topics, from USAMRIID and Center for Disease Control (CDC), to Natick and the National Institute of Health. What is the *raison d'être* of DHS S&T and why was the budget of other institutions not increased and given the same task?

Admiral Cohen explained, "America, like the UK and other democracies, is an incredibly optimistic society. We believe that technology can just about do anything. President Kennedy said we are going to put a man on the moon, we didn't know how to do it at first, but we achieved it - that is who we are. After the tragic events of 9/11/2001, the DHS was established with 183 pages of enabling

legislation; of which 17 pages describe the role and mission of the S&T directorate. What is the DHS and why do we have it? It is composed of 22 disparate agencies and directorates - it is an incredible experiment in nuclear fusion - and as a submariner I spent all my life with nuclear fission - a mega merger and acquisition of 22 different agencies. Why did we do that? We did it because criminals and terrorists will always take advantage of seams, so anything that can minimise or eliminate seams is good for security, but it is a work in progress and S&T is a unifying component of those 22. The enabling legislation says clearly that I will have a university component, where you make knowledge discoveries, where you enable the next generation of the workforce - especially the technological workforce; I have a transition portfolio, near term, 3-5-year spiral development, based on the capability gaps of my customers (the 22 components, but also the first responders); the enabling legislation was wise enough to put a component in there to invest in revolutionary technology, for leap ahead and we call that innovation (about 10% of my budget). What the enabling legislation also says is that I am not to recreate the National Institute of Health, CDC, Dept of Energy or DoD labs, but in exchange I get to leverage them. I can't tell them where to invest, they have their own requirements process, but to the extent

Book Now! CBRNe Singapore Workshop, 12-13 November, Singapore

Genencor® enzymes are changing the way the world combats toxic threats

Learn more at...

Dr Futurity

that they invest I get to add my dollars to try and meet the needs of my 22 components and the first responders for homeland security.”

Yet the same problem faces DHS S&T as it does JIEDDO (Joint IED Defeat Organization, see CBRNe World Autumn 2007), that the enemy is short of resources, so needs to become creative in what he can attain. Blue-force science, however, is less short of resources and tends – because of the way people’s learning and careers are staged – to move in iterative steps, that sometimes there might be a leap ahead in capability, but that has come from an iterative improvement elsewhere. To counter Under Secretary Cohen’s analogy is the (apocryphal) story that NASA spent millions solving the problem of a pen that would work in space, Russian cosmonauts took a pencil. Both solved the problem using the best of their resources. The same technology that might be laboriously developed to stop a device may be rendered inoperable by a change in delivery mechanism – and the terrorist delivery mechanisms are generally low tech. “I think that is an excellent analogy,” said Admiral Cohen, “the terrorists don’t create anything, they just destroy, and they use our technology asymmetrically against us. So you would think that if all the terrorist does is give up their children to be suicide bombers then that would be a self-correcting problem, eventually they run out of children, but we are not prepared to wait that long. This is a war of ideas and ideals, and it is not new. History tells us that, every 500 years, forces of repression fight the forces of enlightenment and in the end history tells us that enlightenment wins, but it is long, not pretty and non-linear. The issue here is one of agility, it is measure, counter measure, counter-counter measure. We are looking at countering IEDs (C-IED) and the Pentagon has said publicly that the cycle of measure, counter measure, counter-counter measure, in Iraq is about 10 days, so you start out with a car door opener as the trigger, then there is a counter, a long range 900mhz home phone, counter measure, garage door opener, shift to a cell phone, and so on. At the end of the day in C-IED because we are on the defensive and, as Goethe said, if you defend against everything you defend against nothing. We have got to have the ability to predict, detect, defeat and destroy IEDs ... at range, which is what I have defined as 50 yards. That is something that in the end we will

be able to do and the terrorist will not.”

Ever since gunpowder made the first “bullet” fly we have used innovative ways to produce projectiles, or blast, at speed and it is difficult to see how that ingenuity can be turned off. Perhaps the best result is that ingenuity only becomes turned off at the lowest level, once the counter-counter measure becomes too expensive it becomes the domain of states and not garages. “It is all about innovation and agility,” said Under Secretary Cohen. “If the mother of the enemy realises that no matter how many children they sacrifice that free and enlightened societies will develop technology that they cannot defeat then you know have a deterrent and the mothers have to ask themselves ‘Why are we sacrificing our children in a cause that cannot prevail?’ That is the end result of deterrence in a free society, but it is messy getting there.”

With the S&T Directorate there are 12 Capstone Integrated Product Teams (IPTs), border security, cargo security, CB defense, cyber security, transportation security, C-IED, incident management, information sharing, infrastructure protection, interoperability, maritime security and people screening. At first sight it becomes apparent that this is a threat-driven list rather than a cold, clean research programme – mixing vertical product lines with horizontal capabilities. For example, counter IED would feature in border, cargo, transportation and maritime security as well as people screening. This relationship is further complicated by six technical divisions – Explosives, CB, C2 and Interoperability, Borders and Maritime Security, Human Factors and Infrastructure.

Yet there is no neat relationship between the 12 IPTs and the six divisions, as Admiral Cohen explained. “We do not have a one-to-one correspondence – divisions to IPTs. One division has three IPTs, one might have one IPT, it varies. What we have found as the Department matures, as it sets capability gaps, is that we may be over-invested in one IPT, which, from a Department viewpoint, is lower priority than another capstone IPT where I am underinvested. What we do is take that information to the Technology Oversight Group and they then decide if there are going to be IPT-IPT lateral moves of resources and investment and the affected components are there to argue their case. It is not my place to set requirements, it is my place to fill with advanced technology

the shortcomings and needs of my customers.”

The IPTs have set themselves some fierce technological targets, within The High Priority Technology Needs of June 2008 (http://www.dhs.gov/xlibrary/assets/High_Priority_Technology_Needs.pdf). In Cargo Security, for example, is the need for the “Capability to screen 100 percent of air cargo.” That’s your lot, that is the entire description of that need – seven words and a number to encapsulate a massive technological and commercial problem. While it might leave a lot of opportunities to solve the problem, it doesn’t really provide any guidance – how long does the screening take, is this all airports, just selected cargos, what is being screened for?

Adm. Cohen suggested that it was back to the three lines of research, “We have the three investment portfolios: basic research labs, you don’t know what you don’t know, you go up a lot of blind alleys, and that can have an eight-year horizon; transition, zero to three years, spiral development; innovation which is one to five years and prototypical. On container screening, let’s take the high end: we don’t know how to do it holistically... yet. We are talking about chem, bio, nuclear, radiological, explosives, stowaways and contraband detection – if technology will support it you may as well look at everything that is illegal and untoward. In innovation we established a Homeland Innovation Prototypical Solution (HIPS) called Safe Con – Safe Container. So at the port from the time that the claw comes down onto the ship and lifts the container and swings it to a waiting trailer there are 45 seconds, and in that 45 seconds we would be able to do a complete CBRNE, contraband, human scan. If the operator gets a green light it goes onto the trailer, commerce is not affected, and off it goes. If the operator gets a yellow light it means the scan is either incomplete or inconclusive, it goes the other way and goes to a holding yard where it gets a visual inspection. A red light means that something nefarious or dangerous was discovered – now I am not an operator but I would put it back on the ship and have them set sail, but that might not be the solution!

“Now, can we do any of those in 45 seconds today? No. But I am building a facility under the idea of ‘build it and they will come.’ There are a lot of incredible ideas out there and I don’t know whether they will work or not, but we might not

Book Now! CBRNe Singapore Workshop, 12-13 November, Singapore – More Information on www.cbrneworld.com

get 45 seconds but I might get 90 seconds – that is the high end, shooting for the moon. At the lower end, the transition end, my customer tells me what has priority – nuclear vs. bio vs. explosives etc – what level of fidelity they want to look at, what kind of false alarms can they live with and other considerations and we do incremental improvements, test it out at airports with DHL and UPS, we test it out in partner countries like Singapore, or Long Beach or Port Elizabeth. If I don't have it in innovation or transition it defines the investment I need to make in phenomenology in the universities and laboratories to give me the detectors to do what we have just talked about.”

Yet it is not just the equipment that will end up being judged, but also the methods of using it. Biowatch (not originally an S&T project though iterations two and three will be), the system of biological detection in a handful of US cities, worked fine... technically. The system utilised air samplers drawing air in and having these samples pulled at regular intervals, these samples would then be taken to a lab and tested. The whole process took about a week, but this was seen to be a workable period to get a gold standard confirmation and to swing into action. Where the system cracked was when the human in the loop was introduced, samples were handled incorrectly, cracked, labelled wrongly, all of which could have led to incorrect chain of custody, potential spread of agent or compromising of the sample. The GAO has hammered Biowatch as much as it can, and this has been one of the driving forces in getting the improvements down range as quickly as possible. Yet it is not the technology that has been an issue, but the tactics, techniques and procedures (TTPs), and it is the introduction of human fallacy that needs to be examined in any system as much as the technology itself. What sort of impact does the MiTL (man in the loop) have on the choice of technology? Is that down to the user to sort out, or does it have to be analysed before the technology is released?

“We have technological capabilities which, for a wide variety of reasons, we don't have the TTPs to fully utilise. One of the things that we have established is a Community Acceptance Panel, made up of average citizens outside of DHS, and we asked them to come in and see what is culturally – not legally, because we always work within that – acceptable. In

Biowatch, over five years ago, there was a strong desire to get background sampling to see, whether annually or seasonally, what is occurring in our major population areas relevant to bio-threat. The goal was, should that limit be exceeded, to be able to inform local personnel, make the necessary evacuation. We have now come up with Biowatch two. It is analogue, we have 30 fairly large sensors in thirty cities: but they only sense one point and they draw air over a filter and it is not real-time monitoring. We collect the filters at great expense, analyse them, we have close to four million samples in the last four years, no false positives but about two dozen real positives. It turned out that those real positives were environmentally caused, they really existed, they were low-threat pathogens, but they were validated. So City A, when it gets this time-late information, they go to battle stations, they send out teams, validate it, etc. In another city they say, that was a week ago, they check the pharmacies – the Tylenol is still on the shelf – they call emergency rooms and morgues – business as usual – and they go, ‘Ok, dodged that bullet!’ and they don't take action. That is the cultural side of it.

“We are now working on Biowatch three, this is lab on a chip, digital, lower power, about 25% of the cost of Biowatch 2 so we can get it into four times as many cities, it is wireless and near real-time transmission that an event may have occurred. But that is not good enough for me: in my innovation portfolio we have something that is called Cell-All. Today your cell phone is not a phone, it is a mini super-computer. It has voice, digital, messaging, video, GPS, it does all of this on a small lithium battery and there are 2.8 billion in use. So what if we can have a sensor on one for Cobalt 60, a sensor on one for anthrax, they would send an alert, a time and GPS, all of a sudden we would have ubiquitous sampling on people who are in harm's way.”

This would appear to be one of those ideas that works well on paper, but as anyone who has been involved in detectors knows they all – under the right circumstances – false alarm, and 2.8 billion is a large factorial for “right” circumstances. What experience again suggests is that after enough false alarms responders stop paying much attention to signals and will – if possible – turn the

The new military frontier – enzymes for biodefense

Learn more at...

www.biosafetyenzymes.com

Book Now! CBRNe Singapore Workshop, 12-13 November, Singapore

Dr Futurity

sensitivity down, so it takes a far larger spike before it sends an alarm. Sensor fusion can deal with some of the technical problems, but in reality it is another problem with the man-machine interface.

"Technology is only an enabler," agreed Admiral Cohen, "the rest of it is integration, training, TTPs etc. In Cell-All we would expect false alarms, it would go to 911 and they would say, 'Oh, it is happening in Picadilly, just one, it is a false alarm.' Two minutes later you get another one, cobalt 60, two minutes later you get a third and a fourth, all of a sudden you have a cluster, maybe it is time to look into it, and you know, because of the technology in the cells, that you can send a forced message to a cell area, so the police can send a forced text message all around the area saying 'There is a radiological event occurring. Please evacuate to the south because the plume is blowing to the north.'"

If the 100% cargo screening was a big "ask" then it is nothing compared to the technology needs for Counter IED: to non-intrusively detect domestic VBIEDs (Vehicle borne IEDs), detect person-borne IEDs at a stand-off range, inerting common explosives, and capability to predict the threat of an IED attack. These are massive projects, under study in one form or another at many agencies, organisations and universities – how much of this is just blue-sky research, the running down of blind alleys?

Admiral Cohen stated that time was short, "I cannot wait for the blue-sky answer. IEDs are the preferred weapon of terrorists, it is not a question of if, but when and by what means. When you are at war and not on domestic soil, with all the protection that our Constitution gives, we have the ability to actively jam, persistent surveillance, work our way up the kill chain, etc., and you see the positive effects that that approach is having, even with the measure/counter measure, in Iraq and Afghanistan. Because we are a cyber-enabled society, if I was to jam – and I am not allowed to because of the Federal Communication Commission – downtown Washington DC, I would effectively turn off every automated teller machine, every Blackberry and shut down the electronic commerce that enables our society. I work with first responders rather than soldiers and marines – we are here to protect and serve – so in 50 yards I want to be able to detect remotely and non-invasively that there is an IED on a person under his clothing or in a car. Today we do well at

checkpoints with Terra-hertz, millimeter wave, dogs, swipes etc. We do well detecting explosives at checkpoints, but you are proximate to the bomb and the bomber, and he might set it off at the checkpoint – that is not good enough. So we are looking at ultraviolet lasers, we are looking at system of systems that will allow us to put our first responders on the offensive at a Superbowl or at the Olympics, New Year's Eve, so that they can be detected. Now the bomber might still explode, but they explode when we want them to, not when they want. If their mothers understand that their children will not get to their target, there might be death and destruction but they did not get to their target, it means that we are putting the problem on the suicide bombers: they have the recruitment problem, not us. In the war of ideas and ideals technology is the enabler."

The ability to remotely detect and specifically jam/disrupt an explosive on a person or vehicle is the Holy Grail of C-IED, but, like that chalice, would presumably be closer to fiction than fact. The amount of clutter, the signal to noise, in picking out a suspicious cargo in one out of a few hundred vehicles moving at speed past a specific point...

Admiral Cohen admitted that it was not going to be easy, but that technology would get there eventually, "The difficulty is enormous, but it is not just vehicles but we are also looking at human behaviour. This is a whole new science of hostile intent. When there was concern in the Pacific about SARS, when you went into an airport as you landed there were IR cameras looking at your forehead; they didn't care whether you were Asian, Caucasian, black or whatever, male, female, just foreheads. If your forehead in IR was hotter than anyone else's walking down that passageway you most likely had a fever and they would take you for secondary screening to prevent the spread of SARS, so there is a mass-transit scenario. So we are asking if there are attributes to suicide bombers that you can detect, such as nervous perspiring, are they flashing their eyes, gait, heart rate and on and on; all of them can be explained by other reasons, you had a parent die, you ran to the airport... We are looking to narrow the field that we need to take to secondary screening, this is enormously complex and will take decades to get us to a point where we have thoroughly effective deterrents towards IEDs, but we will get there."

While a great deal of the work that the S&T Directorate is directly related to the efforts of the staff working on it, it has to also be noted that Admiral Cohen came into S&T and turned around what had been a rather confused agency (the Editor had done previous interviews with the agency in 2005) into something that has become more outward facing and results driven. The outreach programme that can be seen at various regional and national exhibitions (the next opportunity will be Global Security Asia:

www.globalsecasia.com) have seen the whole team presenting mini papers at their stand and working the exhibitions to try and get new technology and new leads.

Undersecretary Cohen is also keen to point out the results that are flowing out of the directorate: "In explosives we have demonstrated the ability to detect and defeat Manpads against civilian aircraft – large and small. In C2 there has been enormous progress made with first responders on governance and interoperability, voice, data and streaming video is not a tech problem anymore. In Borders and Maritime there are numerous devices in things like non-lethal weapons, like the dazzler – one of Time magazines top 100 innovations. It is a sea-sick machine, instead of tazing. What we are really excited about is new, the all-composite, shipping container, the 20/40 ft PCUs that go on shipping. We are putting anti-tamper devices on the walls and floor so we know if anyone has tried to get in there, we have tracking devices and all these have been done with small industry and universities. In infrastructure protection, the work that we are doing there to provide real-time levee repair devices to stop them giving way, so in every division we have had exciting stuff. This weekend I was at Huntington station on the DC metro and 85 ft below the ground – and this is a Welsh idea, coming from the Channel tunnel – and we have a large inflatable plug, 18ft in diameter, so if there was flooding or CB hazardous material in our Metro or underground tunnels, we can block it off, limit the damage in those tunnels, and it was a roaring success."

The DHS S&T directorate is actively pursuing many opportunities to work with companies, agencies, universities and laboratories throughout the world. Interested parties should go to http://www.dhs.gov/xopnbiz/opportunities/editorial_0617.shtm

Book Now! CBRNe Singapore Workshop, 12-13 November, Singapore – More Information on www.cbrneworld.com