CBRNE-Terrorism Newsletter

Summer Issue – Part 1

Moscow subway attack

Backpack-Wearing Cockroaches to Detect Radiation

Non-toxic cleaners for terrorist attacks

Biosensors in briefs

www.RIEAS.gr

CBRNE-Terrorism Newsletter

Summer Issue – Part 1

Athens, May 20th, 2010

Dear Colleagues and Friends,

Current issue of CBRNE-Terrorism Newsletter is aiming to cover the gap of knowledge for those actively involved in CBRNE and Anti-Terrorism operations as First Responders or military personnel.

Newsletter is a gathering of interesting articles from open sources on latest developments in this specialized area of operations. Since knowledge is power, it is obvious that people involved in this area should always be well informed about what is happening worldwide in order to adjust and improve their skills and abilities.

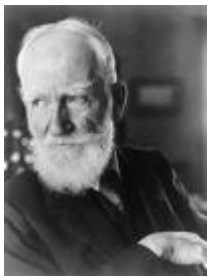
In certain articles there are some comments in Greek – you can easily translate them by using online translation engines (i.e. Google) because certain news are of local interest. These comments and observation represent the opinion of the Editor and not necessarily that of RIEAS that accommodates the Newsletter. Also a few articles are in Greek.

From the next issue, the inner structure of the Newsletter will be modified and there will be separate areas for Chemical, Biological, Radiological/Nuclear and Terrorism threats. Also, in every article there will be the source included below the title. It is always appropriate to recognize the effort of those who initially collected the information presented in this edition.

Newsletter welcomes any comment or suggestion relevant to the title issue and the content provided. If a colleague is interested in participating in the collection and set-up of this Newsletter, he/she can contact me by e-mail and discuss possibilities of further cooperation. There is tons of info out there and a second hand is always a blessing!

I am sure that this Newsletter can improve further and I will keep in working towards this direction for the years to come. People must realize that the threat is real and it can happen to us as well! So be prepared and keep on the good work!

Brig General (ret) Ioannis Galatas, MD, MSc
Consultant in Allergy & Clinical Immunology
CBRN Planner
Senior Terrorism/WMD Analyst
igalatas@yahoo.com



"Αυτό που μαθαίνουμε από την ιστορία είναι ότι δυστυχώς δεν μαθαίνουμε τίποτα από την ιστορία"

GEORGE BERNARD SHAW
(Ιρλανδός θεατρικός συγγραφέας)

15 Απριλίου 2010

Έσωσαν 23 ανθρώπους από βέβαιο πνιγμό

Σμήναρχος (Ι) ΛΕΩΝΙΔΑΣ ΤΣΑΪΡΗΣ – Κυβερνήτης
Επγος (Ι) Σταύρος Κριμιζάς – Συγκυβερνήτης
Ανθυπασπιστής (Μηχανικός) ΙΩΑΝΝΗΣ ΖΩΤΟΣ
Υποπλοίαρχος ΑΠΟΣΤΟΛΟΣ ΚΑΤΡΙΒΑΝΟΣ
Επικελευστής (Δύτης-Διασώστης) ΣΩΤΗΡΙΟΣ ΠΑΓΚΡΑΤΙΩΤΗΣ
Επικελευστής (Δύτης-Διασώστης) ΓΙΩΡΓΟΣ ΤΣΟΥΒΕΛΑΣ

Ανοιχτά της Κρήτης

Πρωί Τρίτης, Μάρτιος του 2010, στην 112 πτέρυγα μάχης του Πολεμικού Ναυτικού, στη βάση της Ελευσίνας, οι τέσσερις άντρες μιλούν με μάτια βουρκωμένα για την επιχείρηση διάσωσης που τους ανέδειξε σε ήρωες, που τους έδωσε το βρετανικό βραβείο για τη δυσκολότερη επιχείρηση διάσωσης παγκοσμίως και ενέπνευσε χιλιάδες ανθρώπους να πιστέψουν στη δύναμη της ανθρώπινης θέλησης.

Ήταν Τρίτη πάλι, Πρωτοχρονιά του 2002, 18.13, όταν στο Εθνικό Κέντρο Συντονισμού Έρευνας και Διάσωσης έφτασε σήμα από την Άγκυρα ότι σε σκάφος μήκους 40 μέτρων που πλέει με βλάβη ανοιχτά της Κρήτης υπάρχουν περίπου 250 άτομα που κινδυνεύουν να πνιγούν. Στο πλοίο μπαίνουν νερά και οι καιρικές συνθήκες στην περιοχή είναι πάρα πολύ κακές. Εάν βυθιστεί το σκάφος, οι πιθανότητες να σωθούν έστω και οι άντρες ναυαγοί είναι μηδαμινές. Για τις γυναίκες και τα παιδιά ούτε λόγος. Ο πνιγμός θα είναι βέβαιος μέσα στα θηριώδη κύματα.

«Από την αρχή φάνηκε ότι η κατάσταση θα ήταν πολύ δύσκολη. Όταν πλησίασα όμως στα δέκα μέτρα, διέκρινα τα πρόσωπα των παιδιών. Τότε νόμιζα πως έβλεπα τα δικά μου παιδιά να κινδυνεύουν» θυμάται ο σμήναρχος Λεωνίδας Τσαΐρης, 47 ετών σήμερα, κυβερνήτης του ελικοπτέρου Super Puma Φαέθων 509 που έφτασε πρώτο στην περιοχή. «Κανονικά έπρεπε να ρίξω το δύτη στη θάλασσα και να καλέσω εκείνον που κινδυνεύει να πέσει στη θάλασσα ώστε να τον μαζέψει στη συνέχεια ο δύτης. Όμως σ' αυτή την περίπτωση υπήρχαν παιδιά πάνω στο πλοίο, τα οποία δεν θα μπορούσαν ποτέ να πέσουν στη θάλασσα. Ο δύτης έπρεπε να κρεμαστεί από συρματόσκοινο και να πλησιάσει στο κατάστρωμα θέτοντας σε κίνδυνο τη ζωή του» λέει ο κυβερνήτης, ενώ ο δύτης, επικελευστής Γεώργιος Τσουβέλας, 37, συγκινείται καθώς θυμάται τον εαυτό του να αιωρείται πάνω από το εγκαταλελειμμένο από τον κυβερνήτη του πλοίο: «Υπήρχε φόβος στην αρχή, που ήμασταν κρεμασμένοι για 25 λεπτά από το συρματόσκοινο σ' αυτά τα μποφόρ και δεν μπορούσαμε να βρούμε τρόπο να κατέβουμε. Φανταστείτε την ταλάντωση του συρματόσκοινου στα 30 μέτρα. Κάποια στιγμή φοβήθηκα ότι μπορεί να μην τα καταφέρω».

«Δεν υπήρχε τίποτα θετικό στην όλη κατάσταση. Όλα ήταν εναντίον των ανθρώπων και των μηχανών. Όμως ήταν μονόδρομος: Η διάσωση έπρεπε να γίνει επιτυχώς» λέει ο υποπλοίαρχος Απόστολος Κατριβάνος, 44, και παραδέχεται πως «Πολλές φορές δεν είναι καλό να έχεις πολύ χρόνο να σκεφτείς. Αυτό μπορεί να σου προσθέσει άγχος. Καμιά φορά ακόμα κι ένας να αγχωθεί μπορεί να δημιουργήσει πρόβλημα».

Επί 25 λεπτά, οι απελπισμένοι λαθρομετανάστες που επέβαιναν στο πλοίο έβλεπαν το τεράστιο ελικόπτερο να πετάει από πάνω τους δίχως να μπορεί να τους βοηθήσει. Ο κυβερνήτης προσπαθούσε να βρει τρόπο να τους σώσει έχοντας κρεμασμένο στο κενό το δύτη. «Η τελική απόφαση ήταν πολύ δύσκολη. Έπρεπε να κατέβω πολύ χαμηλά, ανάμεσα στα δύο κατάρτια, και να συντονιστώ με την κίνηση του πλοίου. Έπρεπε να κρατάω συνέχεια σταθερό ύψος ανάμεσα στο ελικόπτερο και στο πλοίο. Να συντονιστώ με τον κυματισμό, σε σταθερή απόσταση από το πλοίο, χωρίς τη χρήση αυτόματων μέσων αλλά πλήρως χειροκίνητα» λέει ο σμήναρχος Τσαΐρης.

Η πιθανότητα να χτυπήσει ο δύτης πάνω στο πλοίο ήταν μεγάλη. Το ελικόπτερο ανεβοκατέβαινε μαζί με το πλοίο στα 12 μποφόρ. Ανάμεσα τους ο δύτης προσπαθούσε να πατήσει τα πόδια του στο κατάστρωμα του δουλεμπορικού για να σώσει όσους περισσότερους προλάβει. «Κατεβαίνοντας στο πλοίο είδα ένα λαό ολόκληρο να περιμένει από μένα να τον ανεβάσω στο ελικόπτερο. Το πρώτο άτομο που ανέβασα ήταν ένα μωράκι τριών μηνών. Η συγκίνηση μου ήταν μεγάλη. Ήμουν άπειρος εντελώς, ήταν η πρώτη μου σοβαρή αποστολή. Η πρώτη φορά που κράτησα παιδί στην αγκαλιά μου ήταν αυτό τα παιδάκι» λέει ο δύτης και ο υποπλοίαρχος Κατριβάνος δεν προσπαθεί πια να κρύψει τη συγκίνηση του: «Μόλις είχε γεννηθεί η πρώτη μου κόρη και ο δύτης ανεβάζει σ' ένα καλαθάκι ένα βρέφος τριών μηνών! Όταν το έφερε επάνω, ήταν μούσκεμα. Το πήρα στα χέρια μου και κάποια στιγμή λέω στον κυβερνήτη "κε Τσαΐρη, δώστε μου λίγο χρόνο γιατί έχω αποσυντονιστεί. Τι να το κάνω το παιδί; Έχει παγώσει. Να βρω πετσέτες, να το φέρω 'βόλτα', να το ασφαλίσω…". Παράλληλα έχω να κοιτάω το δύτη. Έβγαλα τα σκεπάσματα του βρέφους, το τύλιξα με πετσέτες και το σφήνωσα σ' ένα κάθισμα, γιατί η πόρτα του ελικοπτέρου ήταν συνέχεια ανοιχτή. Ήταν, ίσως, η ωραιότερη στιγμή της ζωής μου. Ένιωθα πως έχω κάνει κάτι στη ζωή μου, πως θα γυρίσω σπίτι και θα πω στη γυναίκα μου και στην κόρη μου ότι έχω κάνει κι εγώ ένα καλό…». Όλοι συγκινούνται.

«Στην αρχή όλα σε φοβίζουν, ειδικά όταν υπάρχουν τέτοιες καιρικές συνθήκες και παιδιά. Σκέφτεσαι πάντα αρνητικά, μετά αλλάζεις» λέει ο μηχανικός, ανθυπασπιστής Ιωάννης Ζώτος, 40, και δεν κρύβει πως, όσο κι αν έχει εκπαιδευτεί ένας άνθρωπος, ο φόβος δεν ξορκίζεται εύκολα.

Η διάσωση ολοκληρώθηκε σε μία ώρα και δεκαπέντε λεπτά αφού ανέβηκαν στο ελικόπτερο 16 παιδιά, 2 γυναίκες και ένας άντρας. Πάνω στο κατάστρωμα όμως είχαν απομείνει αβοήθητοι άλλοι 227 άνθρωποι (το δουλεμπορικό μετέφερε συνολικά 188 άντρες, 36 γυναίκες, 33 παιδιά) να εκλιπαρούν για σωτηρία Τα καύσιμα

του ελικοπτέρου όμως είχαν πια φτάσει κοντά στο μηδέν. «Ζήτησα να προσγειωθούμε σε ένα ισπανικό πολεμικό πλοίο που βρισκόταν κοντά, για ανεφοδιασμό, αλλά επειδή δεν ήμουν εκπαιδευμένος, δεν μου το επέτρεψαν. Οπότε γυρίσαμε στην Κάρπαθο. Το καύσιμο μας έφτασε οριακά» θυμάται ο Λεωνίδας Τσαΐρης και χαμογελάει. Ο καιρός αγρίευε όλο και περισσότερο και ο κίνδυνος για το δουλεμπορικό γινόταν μεγαλύτερος. Κανένα εμπορικό, αλιευτικό ή πολεμικό πλοίο δεν μπορούσε να προσεγγίσει και η πιθανότητα να παραμείνουν γυναικόπαιδα πάνω στο πλοίο αντιστοιχούσε με βέβαιο πνιγμό. Το πλοίο αργά ή γρήγορα θα βυθιζόταν.

«Μας καλέσανε και πάλι να επιχειρήσουμε διάσωση. Το βράδυ ήμασταν οι μόνοι που καταφέραμε να μαζέψουμε ανθρώπους. Οι συνθήκες είχαν χειροτερέψει τόσο πολύ που, αν δεν επρόκειτο για γυναικόπαιδα, πιθανόν να ματαίωνα την αποστολή. Είχα φτάσει πλέον στα ανθρώπινα όριά μου» επισημαίνει ο Λεωνίδας Τσαΐρης. Η επιχείρηση διήρκεσε 24 ώρες και 7 λεπτά. **Το πλήρωμα του Super Puma βρα¬βεύτηκε στο Brighton της Βρετανίας στις 12/3/2002 καθώς έφερε εις πέρας τη δυσκολότερη επιχείρηση μαζικής διάσωσης παγκοσμίως για το έτος 2002 (επιλέχτηκε ανάμεσα σε 10 ηρωικές διασώσεις).**

«Πάντα ο άνθρωπος δοκιμάζει τα όριά του. Δεν μπορεί και δεν πρέπει να γίνεται διαφορετικά. Δεν έχει καμιά σημασία που οι περισσότεροι διασωθέντες ξεχνούν ποιοι τους έσωσαν. Ξέρουν, όμως ότι κάποιοι ήταν εκεί γι' αυτούς όταν χρειάστηκε» λέει ο σμήναρχος Λεωνίδας Τσαΐρης και η ομάδα φεύγει για την επόμενη πτήση της.

Συγχαρητήρια και πάντα ψηλά μαζί με τους αϊτούς !

IDF holds simulation of biological warfare attack

The Israel Defense Forces' Medical Corps held a drill Wednesday to simulate a mass casualty

biological weapons' attack in Tel Aviv metropolitan area. As part of the drill, which involved the IDF, Health Ministry, infirmaries and hospitals, soldiers and citizens were asked to report mock symptoms of fever, rashes and lesions in the mouth cavity. The scenario involved a few cases of "contamination" among soldiers in the Sde Dov Airbase. The air force commander, who was allegedly present and came in contact with soldiers – was also classified as a potential casualty. Medical teams from several infirmaries treated casualties and collected lab samples that later on confirmed that the patients contracted the smallpox virus. "There is a

low awareness to the framework of biological warfare and this drill is meant to raise awareness," said Chief Medical Officer Brigadier-General Dr. Nachman Esh. "We are simulating a number of scenarios. The current drill is part of a perennial exercise, although we don't have a concrete threat at the moment," he added. The medical teams, who were equipped with protective gear and masks, classified certain areas as "sterile zones". Sde Dov Airbase imposed a curfew on departures, in order to prevent "infected" and healthy soldiers from traveling in and out of the base.

Casualties put in isolation

This year for the first time casualties were evacuated to isolated rooms in Sheba Medical Center at Tel Hashomer. "We transferred the hopital patients to other hospital wards along with careful medical supervision," said Sheba's Deputy Director Arnon Afek. "They were all very cooperative. Patients on respirators were kept in the ward because of the health risk involved in moving them."

Tel-Aviv Sourasky Medical Center and Wolfson Medical Center in Holon also participated in the drill. The mock casualties were brought into the empty wards by medical staff equipped with white protective suits and masks. Following conclusions drawn from last years' drill, police officers also participated in the drill and questioned patients in order to determine whether there was suspicion of a biological terror attack. "The biggest challenge is for the community infirmaries that had to detect the unusual case and teach its medical teams how to treat such incidents," said Esh.

Getting ready for Haiti

While holding the drill, Medical Corps personal had to react to a real scenario – they were asked to prepare a rescue team that would depart to Haiti within hours to help with the rescue effort following the massive earthquake that shook the country Wednesday morning. "We are sending a relatively small team of 30-40 members serving compulsory and reserve duty. You can call it an intensive care unit with enhanced abilities – but not quite a field hospital," said

Brigadier-General Esh. The Chief Medical officer explained that the team received an approval from the Chief of Staff and was now waiting for additional permits. "We are accustomed to conducting more than one missions at a time," he said.

Ben-Gurion Airport revolutionizes security with Unipass biometric system

As international aviation officials look to Israel for techniques to safeguard air travel after the failed Christmas Day bombing, Ben-Gurion airport on Tuesday launched a biometric security system for outbound passengers, heralding a new era of hi-tech passenger screening. The Unipass Airport Management System, developed by the Israel Airports Authority, is initially being tested on El Al Matmid Frequent Flyer Club members, before being gradually expanded to include, within two years, all departing passengers who voluntarily register, the IAA said. The IAA said the timing of the biometric security program's launch, amid heightened international air travel security following the Al-Qaeda terrorist plot to blow up a US airliner over Detroit last month, was purely coincidental. The IAA refused to address the issue of passenger profiling, saying instead that the Unipass system will offer improved

service and security, and an identical screening process for all passengers. "This is the first system of its kind in the world. Interest has been expressed by other international airports," an IAA spokeswoman said. It was too soon say how much time the new arrangement will save, the spokeswoman added, but once it becomes fully operational, the system is expected to significantly speed up the security and check-in processes. In the first stage, passengers will arrive at a registration desk, where a machine will scan their passports, and take fingerprint and facial imaging samples to create a biometric signature. The information will then be stored on personal smart card that will be issued to each passenger. The registration is a one-time process. Equipped with their smart cards,passengers can then proceed to the first security stand, where they will be asked to swipe their cards and passports through the machine. As the computer confirms a biometric match, a touch screen panel will present thepassengers with a series of security questions that until now were asked by airport personnel. Guards will stand next to the stands to help anyone who runs into difficulties, the IAA said. "We're not giving up on human interaction," the spokeswoman said. "If any of the questions receive incorrect answers, or the system reports a problem, passengers will be taken aside by a guard for an in-depth check, before being allowed to proceed." The luggage X-ray machine is the next stop, and passengers will once again swipe their Unipass cards through a scanner to inform the system that they have passed the first stage of security. After the luggage is scanned, passengers will go to the airline's check-in desk, where the smart card will again be swiped, prompting a message to appear on the clerk's computer screen that the passenger has passed through all security stages. Once check-in is completed, the hand luggage scanning stage takes place, where travelers once again swipe their cards before continuing on to border control, the duty free stores and boarding. The IAA already allows passengers to circumvent Border Control passport checks with a biometric fingerprint scanner, and says it plans to soon replace Border Control with the Unipass system for

registered passengers. Additionally, the IAA said passengers would soon be able to forgo sending their suitcases through the X-ray machine in the departure hall prior to checking in, thanks to a new system called Hold Baggage Screening. "Passengers registered on the Unipass system will take their luggage directly to check-in, and from there the suitcases will be passed through comprehensive security before being loaded on the plane," the IAA spokeswoman said. "I have no doubt that this system will significantly decrease waiting time for the various security checks," IAA director-general Kobi Mor said. The IAA said the biometric information stored on Unipass computers would be fully secure and could not be accessed by outsiders.

The Escalating Ties between Middle Eastern Terrorist Groups and Criminal Activity

David T. Johnson
Assistant Secretary, Bureau of International Narcotics and Law Enforcement Affairs
Remarks at the Washington Institute for Peace
Washington, DC
January 19, 2010

Good afternoon. I want to thank Dr. Robert Satloff, for his invitation to speak to you today.

It is a pleasure to be here with this distinguished group, and to contribute to the Washington Institute series on these important issues. I would also like to applaud the Stein Program on Counter-terrorism and Intelligence for advancing our understanding of the links between crime and terrorism and the risks those links can pose to America's national security interests.

Dangerous Alliances in the Crime-Terror Continuum
While our discussion today will focus on Middle Eastern terrorist groups' links to criminal activity, it is important to bear in mind that the threat of terror and the origins of terrorist groups spans beyond any single region. Moreover, terrorist groups' links to criminal activity is not a new phenomenon. In the 70s and 80s, for example, groups like the Red Army Faction, the Red Brigades and the domestic Symbionese Liberation Army financed violent terrorism with violent crimes like bank robbery.

In recent years, many of these groups have focused almost exclusively on using narcotics as a means to finance their activities. As the international community clamped down on state-sponsored terrorism and pressured governments from financially supporting terrorist organizations, many groups resorted to drug trafficking and other illicit activities as sources of revenue. According to the U.S. Drug Enforcement Administration, 19 of the 44 groups that the U.S. Government has designated as Foreign Terrorist Organizations (FTOs) participate in the illegal drug trade and many also engage in financial and other forms of crime.

Today, we look at organizations as diverse as Hizballah, Al-Qaeda, the Revolutionary Armed Forces of Colombia (FARC), the Taliban in Afghanistan, the Kurdistan Worker's Party (PKK), the Liberation Tigers of Tamil Eelam (Sri Lanka), all of which engage or have engaged in criminal activities as a vehicle to finance their terrorist (or violent political) activities.

In places like West Africa, we now see how increased drug flows from Latin America, kidnappings, and other crimes produce opportunities for criminal groups that might sympathize with Al Qaeda to tap into the wealth generated by narcotics trafficking and other illicit activities to fund their operations. Last month, for example, US prosecutors in the Southern District of New York charged three men who claimed to be Al Qaeda associates with conspiracy to smuggle cocaine through Africa. In Afghanistan, we have long known that among the Taliban's funding sources were informal taxes on heroin traffickers. Two years

ago, U.S. and Colombian investigators were able to dismantle an international cocaine-smuggling and money-laundering gang that funneled some of its profits to Hizballah, a U.S. designated Foreign Terrorist Organization. In the Horn of Africa, we are seeing illicit routes established by criminal groups to smuggle immigrants, arms, narcotics and other contraband, and know these illicit activities will create opportunities for terrorist groups to exploit.

We also remain concerned about the crime-terror links in an increasing number of ungoverned or insufficiently governed spaces, such as Yemen and the Sahel belt, where insecurity and other destabilizing factors provide opportunities for illicit networks to thrive and find safe haven – and as possible staging platforms to project their terror campaigns abroad. For example, in the tri-border area, along the loosely controlled region that borders Paraguay, Brazil and Argentina, individuals with apparent connections to radical Islamic groups have been active in drug trafficking, money laundering, intellectual property rights piracy, alien smuggling and arms trafficking.

These are very serious issues, but you may ask why these issues are becoming national security priorities for the United States now.

Threats to U.S. National Security

Violent criminal and terrorist networks threaten the security, economic health and social fabric of all nations. These transnational threat networks imperil public trust, and core democratic and market values, especially in the midst of the most serious global economic and financial crisis in decades. Criminal entrepreneurs who smuggle billions of dollars of illegal goods across borders – drugs, arms, humans, natural resources and endangered wildlife parts, counterfeit medicines and pirated software, as well as embezzled public funds – create insecurity, cost our economies jobs and tax revenue, endanger the welfare and safety of our families and communities, and overwhelm law enforcement countermeasures. Similarly, terrorist groups create great insecurity by the acts of cowardice and the killing of thousands of innocent people to advance their political and ideological objectives. They do not respect traditional borders or nation-states, and they exploit ungoverned and under-governed areas as places for safe haven, as places to rest, to recruit, to train, and to plan their operations. In many places, these networks become the de facto government.

Corruption, Crime and Terrorism: The Unholy Trinity

Poor governance and corrupt officials in many parts of the world enable criminals, insurgents, and terrorists to operate with impunity. Criminal syndicates have long supported terrorist groups – for both ideological and economic reasons – by facilitating their trans-border movements, weapons smuggling, and providing forged documents. At the same time, terrorist groups also resort to organized crime to finance their activitites, including through drug dealing.

Such terrorist-criminal cooperation is of particular concern, especially because some of these criminal syndicates have the organizational and financial wherewithal that could potentially allow them to acquire and sell radioactive materials, chemical and biological weapons, or technologies used for weapons of mass destruction. This financial strength makes it much more difficult for governments to shut off the spigot used to finance terrorism, at least through traditional means that focus on deterring exploitation of the formal banking system. As terrorist groups move toward mimicking the tactics of organized crime, our international response will need to incorporate more creative law enforcement tools that go well beyond effective regulation of financial transactions.

The question is frequently raised as to why criminals would want to assist terrorist groups. While it is possible that criminals may not want the extra attention from states' national security institutions that will come from associating with terrorists, some may nevertheless find the financial temptation too great. Others may not care with whom they conspire, as long

as they are paid for the increased risk of detection they assume when cooperating with known terrorist groups. For example, reports indicate that some charge extra for dealing with certain nationalities and others more for "special services". And some criminals may have no idea who their clients really are. These people are undoubtedly clever, but they may nevertheless be more greedy than smart.

A convergence of crime and corruption can also pave the road for terrorist organizations to finance their terror, as was the case in Bali, Madrid and Mumbai. In particular, terrorist financiers are not only concealing their financing assets through complex transactions in the formal banking system, but also harnessing centuries-old money laundering tactics. They exploit informal value transfer mechanisms such as hawala or hundi and trade-based money laundering, and use illegal cash couriers as bulk cash smugglers, particularly in countries with non-existent or weak anti-money laundering enforcement practices.

Winning the Peace: Smart Power and International Cooperation

So what is the U.S. Department of State doing to combat these transnational threat networks? The State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL), which I lead, is responsible for international counter narcotics and counter crime issues. We lead diplomatic efforts to raise awareness of the destabilizing impact of transnational organized crime and illicit activities and we strengthen global efforts to combat these threats, including through enhanced law enforcement cooperation, where organized crime and terrorism intersect. We are enhancing international cooperation to dismantle criminal networks and combat the threats that they pose -- not only through law enforcement efforts, but also by building up governance capacity, supporting committed reformers, and strengthening the ability of citizens to monitor public functions and hold leaders accountable for providing safety, effective public services, and efficient use of public resources.

In the Middle East, and other parts of the world, the United States is working with partner governments to develop effective, democratic, civilian-led and skilled law enforcement and justice sector institutions. Hamas and Hizballah continue to finance their terrorist activities mostly through the state sponsors of terrorism, Iran and Syria, and through various fundraising networks in Europe, the United States, and the Middle East. The funds channeled to these organizations frequently pass through major international financial capitals, such as Dubai, Bahrain, Hong Kong, Zurich, London, or New York. Hizballah also continues to profit from the drug trafficking groups in the Bekaa Valley of Lebanon.

In response, the United States is helping to strengthen the anti-money laundering and counter-terrorist finance programs of partner countries that aim to detect, disrupt, and dismantle these illicit activities. In Palestine and Gaza, besides being responsible for hundreds of rocket, mortar, and small arms attacks into Israel, Hamas and other armed groups in Gaza engaged in tunneling activity, and smuggle weapons, cash, and other contraband into the Gaza. In the West Bank, the United States helps to support the PA security forces (PASF) to establish law and order and fight terrorist cells by helping to build capacity to administer criminal justice institutions. The United States has also helped train thousands of Palestinian security forces at Jordan's International Police Training Center (JIPTC), who can then be deployed by the Palestinian Authority to protect peace and stability in the West Bank. In Lebanon, a place I visited last week, we are partnering with the Lebanese Government, and specifically with its Ministry of Interior, in an initiative to train the next generation of Internal Security Forces officers. Our objective is clear: to support the development of professional institutions under the Ministry of Interior which can provide security and vital services to the Lebanese people.

In Iraq, criminal insurgencies have profited from the illicit trade of siphoned oil. The United States is working to target and dismantle these illicit networks as part of our broader counter-insurgency effort. We continue to support reconstruction and stabilization by helping to develop an Iraqi criminal justice system that is sufficiently fair and effective that the Iraqi

people have confidence in that system and turn to it rather than extra-judicial groups and militias to resolve disputes and seek justice. We also support rule of law programs that focus on judicial security, capacity building for judges, prosecutors, investigators, and court administrators, and integration of the various components of the justice system. We are also working with Iraq on legislation to reform their criminal codes, and continue to support the FBI-led Major Crimes Task Force.

In Afghanistan, where we have long focused on combating narcotics trafficking and the revenue stream that creates for the Taliban, we are also working with our military colleagues to develop criminal justice institutions by giving Afghans the necessary training, equipment, infrastructure, institutional capacity and organizational structure to provide the rule of law and combat crime.

In Yemen, we recently completed a judicial and law enforcement assessment. Based on that, we aim to undertake targeted assistance to the Government of Yemen to strengthen its capacity to control the movement of people and goods through and across Yemen's borders.

In West Africa, over the next three years, INL aims to strengthen criminal justice institutions such as the police, prosecutors and the courts to successfully investigate, prosecute and incarcerate transnational criminals, networks and organizations. Right now, we are considering how best to support Kenya and other partner nations in the Horn of Africa to prosecute and incarcerate those apprehended for piracy. At the same time, though, we and others at the State Department are focused on the longer term solution to the piracy question – political stability, restoring the rule of law, and supporting economic opportunity in the Horn of Africa.

In Indonesia, INL has worked closely and successfully with the National Police for many years, and our investment is paying off. The first Police units that responded to the July 2009 attacks on the Marriot and Ritz Carlton Hotels in Jakarta were trained through INL programs. The unit that ultimately brought down the mastermind behind those bombings, Noordin Top, was also trained and worked closely with us for many years. Noordin had ties to Jemaah Islamiyah as well as to Al Qaeda.

The United States is also committed to working with others to strengthen law enforcement cooperation in combating transnational threats including dismantling illicit networks, and prosecuting high-level corrupt officials, to disrupt the convergence of various threat networks. On numerous occasions, President Barack Obama and Secretary of State Hillary Clinton have highlighted the threat of high-level corruption, and we are working to strengthen the tools we have to combat and deter corruption and to use those tools more effectively.

International legal and political cooperation is essential to prevent, investigate, prosecute and punish serious crimes as well as to break up terrorist networks, to eliminate safe havens, and to disrupt those activities that support terrorist organizations. Our efforts are aimed not only at the murderous acts terrorists perpetrate, but also their funding, their travel, their communications, their recruitment, and their intelligence and information collection.

With our international partners, we encourage others to implement the United Nations Convention against Transnational Organized Crime (and its Protocols) and the United Nations Convention against Corruption (UNCAC). These international instruments, built on the foundation of the three United Nations counter-drug conventions, create a broad legal framework for mutual legal assistance, extradition and law enforcement cooperation. Additionally, the United States supports implementation of UN Security Council (UNSC) Resolution 1373, and other UNSC resolutions and UN legal instruments, to combat terrorism.

Dynamic Threat Mitigation: Fighting Networks with Networks
Beyond the United Nations, my colleagues and I in the Bureau of International Narcotics and Law Enforcement Affairs also work, through the G-8, the European Union, INTERPOL, the Financial Action Task Force (FATF) and its regional sub-groups, APEC as well as other regional forums. Through these groups, we set international counterdrug and anti-crime standards, take steps that close off safe-havens to criminal and terrorist groups, pool skills and resources, and improve cross-border cooperation. For example, at last year's G8 summit in L'Aquila, Italy, leaders expressed concern about the converging threats of terrorism, drugs and organized crime, and agreed to strengthen international cooperation and capacities to prevent international criminal networks, kleptocrats and terrorists from corrupting public institutions to advance their goals. Additionally, the United States is working with INTERPOL and other multilateral partners to strengthen inter-regional law enforcement efforts to combat transnational threats in a coordinated manner across the Pacific and Atlantic.

As the world witnessed this past Christmas day when a terrorist attempted to blow up a commercial airliner, Al Qaeda remains keen to harm Americans and others around the world. Our enemies will continue to use all available means to sustain their agenda. As already noted, places in Afghanistan, Southeast Asia, West Africa, Somalia, and Yemen, illicit networks, trafficking in everything from weapons to drugs are making it easier for Al Qaeda and other terrorist groups to fund their campaigns. As a recently captured Taliban underscored: "Whether it is by opium or by shooting, this is our common goal [to harm all infidels as part of jihad]".

Faced with these challenges, we must continue to take more effective steps to understand our adversaries and to strengthen our capabilities to deter, disrupt and dismantle transnational threat networks, not only at the end of their efforts, when they carry out acts of violence, but at every step along the way.

Ray Guns Real

Boeing is developing a mobile laser weapon for the U.S. Army. Mounted in an Osh Kosh armored vehicle, the weapon will will enable the military to fight at the speed of light. The ray gun is real ... or at least it will be soon. The U.S. Army is betting big on laser warfare -- designing, testing and perfecting ultra-precise weapons based on devastatingly powerful beams of light. And given recent developments, it's only a matter of time until the military has

in its arsenal a weapon that until now has been the staple of science fiction -- the ray gun. Set your phasers to kill. Boeing, one of the Pentagon's top contractors, already has a laser weapon that will improve the military's ability to counter artillery, mortar, drone aircraft and even rockets, a spokesman tells FoxNews.com. Boeing's is the highest-profile program of all of the projects under development for the Department of Defense, and last week it took a step closer to reality. At its facility in Huntsville, Ala., Boeing accepted a military truck built by Oshkosh Defense that will carry its laser beam control system into battle. The device is the cornerstone of a high-priority U.S. Army project, called the High Energy Laser Technology Demonstrator (HEL-TD), touted as the future of American war, which will enable the military to fight at the speed of light. "The system is technically not in production right now," says Marc Selinger, a spokesman for Boeing's missile defense systems unit in suburban Washington, near the Pentagon. "Boeing is building only a demonstrator now ... in this case, a test unit." That means the project is moving out of the design phase and, with the Oshkosh Heavy Expanded Military Tactical Truck, into production. The eight-wheel, 500-horsepower HEMTT A4, a widely used military tactical vehicle, is being tightly integrated with the Boeing rugged beam control system. Suppliers are already shipping related components to Boeing for assembly. The weapon will eventually include high-speed processors, optical sensors, and an array of mirrors. Testing of the device's lethal capacity will begin next fiscal year at the White Sands Missile Range in New Mexico. In addition to the U.S. Army, Boeing is developing its laser technologies for the Air Force and Navy. A number of new materials enhance the weapon as well, including sapphire substrates for LEDs, semiconductors, and optics. One Chicago-based supplier, Rubicon Technology, provides components made of sapphire for military lasers and sensors. Lasers are sensitive devices, yet in combat, they will be used in harsh conditions, including sand and wind storms. Sapphire is the second-hardest material on earth, next to diamonds, "yet they can be free of imperfections and perfectly flat," says Beth Hespe, a spokeswoman for Rubicon. The material helps keep the laser stable -- key to its effectiveness as a weapon.

A Brief History of Laser Guns

For decades, the Army has tried -- and essentially failed -- to develop alternative weapons that target threats before they can reach ground troops. One earlier technology was called the Trophy Active Protection System, which in concept would have fired a shotgun-like blast of pellets at incoming rocket-propelled grenades and antitank missiles. Scientists now hope that lasers can do what flying metal cannot. Dissipating the heat laser beams generate is one problem the military has faced in its efforts to weaponize lasers, which new, proprietary technology is overcoming. The technology consists of a laser, a power source and a command and control element. Development of an effective power source -- something that could generate enough energy to destroy incoming projectiles -- has been another key advancement. At the most fundamental level, laser weapons are based on the concept of delivering a large amount of stored energy from the weapon to the target, thus producing structural and incendiary damage effects. A directed energy weapon delivers its effect at the speed of light, rather than supersonic or subsonic speeds typical of projectile weapons. The lasers basically obliterate their targets. Many scientific, military, medical and commercial applications have incorporated lasers since their invention in 1958. When the Apollo astronauts landed on the moon, they planted retroreflector arrays to make possible the Lunar Laser Ranging Experiment. Laser beams focused through large telescopes on Earth aimed at the arrays, and scientists measured the time the beam took to reflect to determined distances with high accuracy. Military uses of lasers include applications such as targeting and ranging, defensive countermeasures, communications and directed energy weapons. The military's tech at present is focused on larger, truck-mounted laser guns. But as the technology is honed and miniaturized, its easy to imagine a future with handheld versions of the ray guns -- just like in the movies.

Uses for Laser Beams

Last March, Northrop Grumman announced that its engineers in Redondo Beach, Calif., had successfully built and tested an electric laser capable of producing a 100-kilowatt ray of light, powerful enough to destroy cruise missiles. An electric laser requires much less space for its supporting equipment than a chemical laser, which is powered by a chemical reaction rather than an electrical power source. Lasers are also being used in radar and radio applications by the military. "They are also playing a leading role in the development of wideband communications -- wideband essentially being a synonym for delivering broadband capability to the battlefield," said Jon Alhart, a spokesman for military contractor Harris Corp. Using lasers and other technologies, the military can set up broadband networks anywhere radios are conventionally out of range. This is accomplished wirelessly, over-the-air, without the assistance of gateways or other ad-hoc networking technologies. But America's enemies are also exploring laser technology, and the U.S. military is preparing for that too. Last week, U.S. Sen. Patrick Leahy (D-Vt.) disclosed $2.4 million in new funding for Revision Eyewear in Essex Junction, Vt., to make new lenses to protect soldiers against lasers on the battlefield, according to Jonathan Blansay, CEO of Revision. And last year, Leahy secured another $3 million contract for laser protective eyewear -- more than $10 million since 2005, said Blansay. It's only a matter of time until lasers form the backbone of many different aspects of military life, not just warfare.

Israeli Robots Remake Battlefield

Israel is developing an army of robotic fighting machines that offers a window onto the potential future of warfare. Sixty years of near-constant war, a low tolerance for enduring casualties in conflict, and its high-tech industry have long made Israel one of the world's leading innovators of military robotics. "We're trying to get to unmanned vehicles everywhere on the battlefield for each platoon in the field," says Lt. Col. Oren Berebbi, head of the Israel Defense Forces' technology branch. "We can do more and more missions without putting a soldier at risk." In 10 to 15 years, one-third of Israel's military machines will be unmanned, predicts Giora Katz, vice president of Rafael Advanced Defense Systems Ltd., one of Israel's leading weapons manufacturers. "We are moving into the robotic era," says Mr. Katz. Over 40 countries have military-robotics programs today. The U.S. and much of the rest of the world is betting big on the role of aerial drones: Even Hezbollah, the Iranian-backed Shiite guerrilla force in Lebanon, flew four Iranian-made drones against Israel during the 2006 Lebanon War. When the U.S. invaded Iraq in 2003, it had just a handful of drones. Today, U.S. forces have around 7,000 unmanned vehicles in the air and an additional 12,000 on the

ground, used for tasks including reconnaissance, airstrikes and bomb disposal. In 2009, for the first time, the U.S. Air Force trained more "pilots" for unmanned aircraft than for manned fighters and bombers.

Terrorism: Al-Qaeda warns of 'dozens' of in-flight bombs

Al-Qaeda has prepared "dozens" more bombs like the one used by the young Nigerian accused of trying to blow up an airliner in the United States on 25 December last year. The

claim was allegedly made by the Yemen-based Al-Qaeda in the Arabian Peninsula terror cell in a message posted in its online magazine 'al-Malamih'. "We have dozens of sophisticated explosive devices which are similar to that used by the Nigerian,Umar Farouk Abdulmutallab on the Christmas Day flight from Amsterdam to Detroit," said the message in 'al-Malamih'. Al-Qaeda in the Arabian Peninsula said in December it had provided Abdulmutallab with the explosive device he allegedly used to try to blow up Northwest Airlines Flight 253 with nearly 300 people aboard. "The plan was to blow up the plane as it approached Detroit, so that it would fall onto buildings below and kill the maximum number of Americans," the message said. Had it succeeded, it would have been the worst attack on the United States since Al-Qaeda's September 11 2001 assault. "Four years ago, we began producing similar devices to that used by Umar Farouk," the 'al-Malamih' message said. AQAP was officially formed in January 2009 from a merger of Al-Qaeda's Yemeni and Saudi branches. The message claimed that Abdulmutallab trained at camps in Yemen in the second half of last year and was eager to "go into action". Abdulmutallab was "always quiet and thought a lot," kept to himself, read the Koran and fasted every Monday and Thursday, the message said. The explosive material used in the device concealed in the Nigerian's underwear was 'Pent', it stated. Just four grammes of the substance are needed to produce a major blast, it claimed. "The reason we chose a flight that left from (the Dutch capital) Amsterdam, is that the Netherlands is a country that has offended the Koran and Islam," the message stated. This may be a reference to late Dutch director Theo Van Gogh's film 'Submission' which was aired on Dutch TV in 2004. Somali-born feminist AyaanHirsi Ali wrote the screenplay for the film, which sharply criticised domestic violence against Muslim women. A fatwa was issued against Hirsi Ali and Van Gogh, who was murdered by Dutch-Moroccan extremist Mohammed Bouyeri on 2 November, 2004.

RISING IED ATTACKS

The number of "effective attacks," in which improvised explosive devices kill or wound coalition troops, is increasing in Afghanistan. Attacks in January of each year:

Year	Effective Attacks	Killed	Wounded
2007	5	0	13
2008	14	6	29
2009	28	14	64
2010	67	32	137

Source: Joint IED Defeat Organization

A death threat against Hirsi Ali was pinned to his body with a knife.

Winter weather failed to deter insurgents from stepping up roadside bomb attacks in Afghanistan, as both blasts and casualties among U.S. and allied troops in January more than doubled from a year earlier, Pentagon data show. Coalition troops found 727 bombs in January compared with 276 in the same month of 2009. Blasts killed 32 U.S. and allied troops

and wounded 137 others, compared with 14 deaths and 64 injuries in January 2009, according to the data. These bombs are the top killer of U.S. troops in Afghanistan. In previous years, winter was a slow season for Taliban and insurgent attacks in Afghanistan. Over the weekend, U.S.-led forces launched the largest offensive in the eight-year war to oust the Taliban from their southern stronghold of Marjah. Coalition and Afghan troops encountered only sporadic resistance from insurgents Sunday. The biggest threat to them: hundreds of mines and roadside bombs planted by the Taliban before the offensive."

Taliban use modern anti-detective IEDs

According to icasualties.org, in the past two months, more than half of the battlefield deaths suffered by U.S.-led troops in Afghanistan were caused by IEDs. The Taliban in Afghanistan have built a new generation of improvised explosive devices which is not detectable, a Taliban statement has said. The new IEDs, called "Omar", have been made by the Taliban technical experts inside Afghanistan and cost only $85 each, the statement, released on Friday, said. According to the Taliban statement the new IEDs are not detectable by special mine-detector machines used by foreign forces based in the country. Taliban said they have made the new remote-controlled IEDs after the US and NATO forces entered into Afghanistan special modern devices that are able to detect and neutralize ordinary IEDs made by the Taliban. The Taliban say the new-generation IEDs have proved to be effective. The report comes as the United States promised on Friday to provide armored vehicles, ground penetrating radar and other equipment to NATO allies to help protect their troops in Afghanistan from increasingly deadly roadside bombs. "Today I told our allies that the United States will be able to offer them more intelligence, training and equipment including jammers, route clearance robots, surveillance systems and ground-penetrating radar," U.S. Defense Secretary Robert Gates told a news conference after a gathering of NATO countries in Istanbul. IEDs are the main killers of foreign soldiers in Afghanistan. More than 500 U.S.-led troops have been killed in the war-torn country in 2009, including more than 310 Americans. Another report released on February 2, 2010 suggests that for British soldiers serving in Afghanistan expensive hi-tech weapons are not the problem, but it is the Taliban's IEDs that are costing British lives. The IEDs have become the deadliest of enemies to British troops in Afghanistan. Last summer British forces were dealing with a thousand incidents a month. "Although the Taliban still fights with small-arms, rocket-propelled grenades and improvised explosive devices, they have increasingly focused the role of IEDs as antipersonnel devices," the report said.

FARC rebels' missile purchase raises concerns

Colombia's FARC guerrillas have allegedly purchased at least seven anti-aircraft missiles that experts say could threaten U.S.-provided helicopters essential to the South American country's fight against the rebels. Peruvian prosecutors detailed the purchases when they charged a dozen people in December with buying hundreds of weapons from crooked Peruvian security force officials and delivering them to an arms buyer for the Revolutionary Armed Forces of Colombia, or FARC. The missiles could complicate Colombia's decades-old civil war, where the military has made strong gains in recent years by deploying a fleet of

U.S.-provided transport and attack helicopters for swift raids on FARC targets. Colombian military analyst Alfredo Rangel said that if the Peruvian allegations are true, the handful of missiles ``could be used to shoot down a couple of helicopters," but ``their impact would not be very significant." The weapons likely would be devoted to the defense of the FARC's top leaders but ``would not allow the FARC to shift to the offensive or alter the balance of power against the government forces," he told El Nuevo Herald in a telephone interview. The Peruvian prosecutors' records detail the sale of at least four Russian-made Strela and Igla ground-to-air missiles between May and October 2008 and another three in 2009, ``each one for the sum of 45,000 US dollars." They were sold by Jorge Aurelio Cerpa, a Peruvian air force official, and were delivered to Freddy Torres, an Ecuadorean who had been buying weapons for the FARC since 2007, according to the records. They and nine others were arrested and charged with collaboration with terrorism, and several have confessed. Peruvian army and police officers also sold Torres hundreds of hand grenades for up to $60 apiece, 40-50 heavy machine guns for $19,000 each and tens of thousands of rounds of ammunition, according to the records, first published by the La República newspaper in Lima. Torres, who was arrested Dec. 19 on Peru's northern border with Ecuador, was paying $150,000 to $200,000 for arms deliveries ``every 15 or 20 days," a copy of the records provided to El Nuevo Herald showed. But the most significant purchases were the heat-seeking Strela and Igla missiles, which can be carried by one person and fired from the shoulder. U.S. officials have been particularly concerned that such weapons could fall into the hands of terrorists. The Strela and older Igla missiles have a maximum range of about three miles and are highly effective against slow-flying aircraft not equipped with electronic countermeasures. It's not clear whether Colombia's U.S.-made UH-1H and Blackhawk helicopters have the appropriate countermeasures. Hoping to reverse its recent setbacks, the leftist FARC, has made it a priority to obtain the man-portable missiles. Such missiles would allow the rebels to deal ``forceful blows to the enemy's air power," the FARC leader known as Alfonso Cano wrote in an Aug. 16, 2009 e-mail intercepted by Colombian military intelligence and published in that country's media. The e-mail, a 14-point plan to improve the FARC's fighting abilities, said the rebels should set aside $5 million to $6 million to buy weapons for its estimated 9,000 fighters, who finance their war largely through cocaine trafficking and kidnappings. The FARC's need for missiles was also mentioned in an e-mail found in computers captured when the Colombian military raided a rebel camp in neighboring Ecuador in 2008 and killed the top FARC commander known as Raúl Reyes. ``The anti-aircraft weapons are already, for us, an urgent necessity," said the e-mail between two rebel commanders, also published in the Colombian media. While Colombian and U.S. officials have long been concerned about the possibility that the FARC could obtain the ground-to-air missiles, most of the unease to date had focused on Venezuela, where leftist President Hugo Chávez has long expressed sympathy for the guerrillas. Chávez has been on an arms-purchasing spree since 2006, buying $6 billion worth of Russian jets, helicopters, tanks and Igla-S missiles -- also known as SA-24, the latest and most sophisticated version of the weapons -- for what he calls the defense of his country from planned U.S. attacks. The U.S. Treasury Department accused a former Chávez cabinet minister and two generals in 2008 of helping the FARC with weapons, finances and drug-trafficking, and ordered the seizure of any of their assets found in the United States. But the Peruvian case focused new attention on that country, which bought 633 IGLA-1 missiles, also known as SA-16s, from 1992 to 1996,

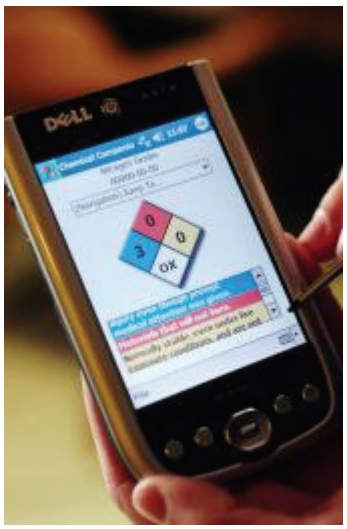
and 500 older Strela 2 missiles, also known as SA-7s, from 1978 to 1981, according to the Stockholm International Peace Research Institute, which tracks weapons purchases around the world. The prosecution documents make no mention of any ideological affinity between the FARC and the Peruvian military officers who sold the weapons -- after writing them off the books as spent in training exercises or junked because of old age -- indicating that they were doing so purely for money. Nicaragua voluntarily destroyed about 1,400 Strela 2 missiles after the war between the Soviet-backed Sandinista government and U.S.-backed contra guerrillas, but U.S. officials are still offering the current government $5 million to destroy its remaining 600.

Cultivating Emergency Managers

As I survey the nation's emergency management landscape, I see an aging population of emergency managers in leadership positions at all levels of government and industry. It's time to begin cultivating the next generation of emergency managers who will be taking your places. It isn't unique that Washington state's current leaders in key positions have been there for almost 20 years. About a generation ago there was a transition in leadership and an expansion of the discipline due to an increased recognition of hazards. The 9/11 terrorist attacks created another surge in emergency management with the creation of homeland security and another expansion of emergency management and homeland security jobs. The impact of 9/11 also created a network of colleges and universities that now offer undergraduate and graduate degrees in emergency management and homeland security. The challenge is getting these newly minted graduates into the governmental system so they can get experience before the old guard retires. I've heard from numerous graduates from these programs who are frustrated about not being able to get hired in government positions, especially at the state and local levels. Individually there aren't a huge number of emergency management jobs in single jurisdictions, but on a national scale we collectively number in the tens of thousands of people serving in one capacity or another as emergency managers. For us to grow the next generation of emergency managers we will need to have entry-level positions that allow these younger people to successfully compete for and have a career path within the discipline. Larger private-sector consulting firms are much better at this than government. It's common to have a series of progressive positions in emergency management consulting. It may start with research analyst and then progress with associate, senior associate, program manager, senior program manager, principal, vice president and end with senior vice president of a division. Here are some steps that you might take to help develop the next generation of emergency managers: If you have multiple positions within your emergency management organization, when one becomes vacant, reallocate it to a more junior-level position. As the economy picks up, revenues improve and you have the opportunity to hire someone new, don't make the position an "expert" in emergency management. Create an entry-level position that perhaps requires a degree in emergency management. Use a homeland security grant to hire at the junior level. With a little bit of supervision and mentoring, you can take enthusiastic hires and make them into the positive program people you would like them to be. Leave a legacy by mentoring a junior emergency manager. This doesn't have to be someone in your organization. If you know junior emergency managers who have potential, offer to be available to them to talk about their ongoing projects and the challenges they face. Also be approachable and available to people doing informational interviews on an emergency management career. If we're going to be really successful in our careers, we must prepare the next generation for theirs.

Free, Handheld Reference Adds Situational Awareness at HAZMAT Incidents

When a call for service comes into the Douglas County, Ga., Fire Department that may involve hazardous materials, Deputy Chief Kim Ransom or another senior member of the department's HAZMAT team grabs his or her tools and hustles to the scene, along with the initial fire crew. Once the crew arrives with on-board chemical sensors activated, they plug the information into several tools including: the Wireless Information System for Emergency Responders, the Computer-Aided Management of Emergency Operations chemical database, the 2008 Emergency Response Guide and the Chemical Companion deci sion support tool. The Chemical Companion is a Windows-based reference of 130 of the most common chemicals involved in hazardous materials incidents including their properties, signs of exposure and possible antidotes. When the HAZMAT team arrives on scene, the first thing they do is consult the Emergency Response Guide for basic response information, including initial isolation distance and the initial first aid measures that should be administered to those who have been exposed. Then the data picked up from the sensors aboard the fire apparatus is plugged into the various databases. This gives the initial responders information such as whether the unknown substance has a low explosive limit or if the chemical can be identified. In the summer 2009, the Douglas County Fire Department responded to the scene of an overturned tanker truck involving an unknown mixture of chemicals for which a single material safety data sheet (MSDS) was not available and a chemist wasn't immediately available on scene. Responders entered how the substance was reacting and its temperature into the Chemical Companion. "We narrowed [it] down to where we had an idea that it was more closely related to one of the MSDS sheets than the other," Ransom said. "The Chemical Companion is great about being able to measure symptomology and help you kind of narrow down your potential hazard."

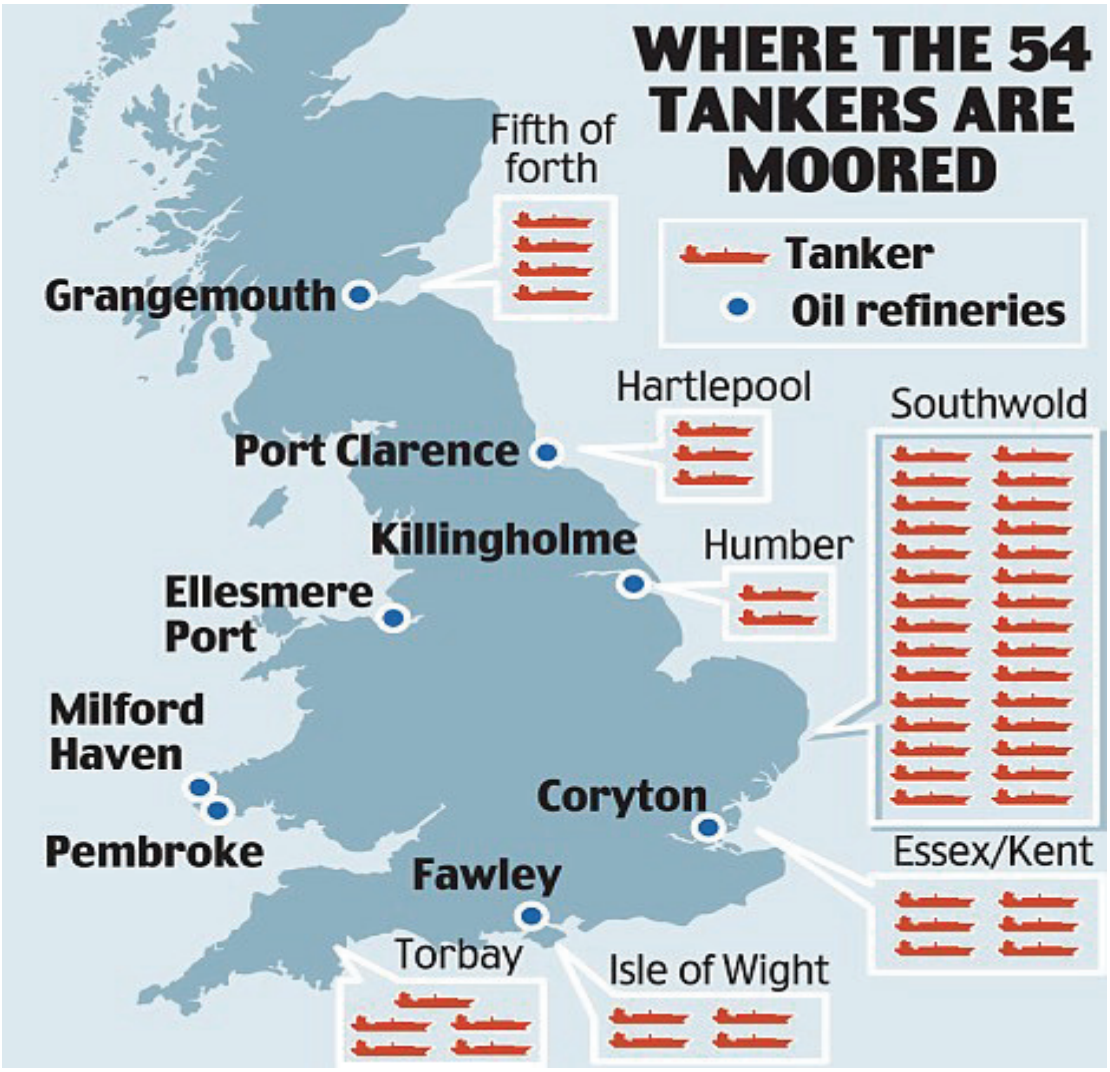


Smart Companion

Ease of use and an interface that's mostly driven by menu choices helps minimize mistakes, Ransom said. "When you're dealing with intricate chemical names — one misspelling can change the whole chemical compound — it's really nice to be able to have your text in there," she said. The Chemical Companion also can help first responders choose the appropriate suit for a spill and determine estimated time a responder can work in contact with a chemical at a particular rate before it permeates the suit. "It is nice to know that you have time in a certain type of suit or with boots or with different types of gloves that you can work in the product before it has the potential to permeate the material and become contaminated," she said. The tool was developed by researchers at the Georgia Tech Research Institute with input from first responders and HAZMAT teams. It operates on Windows CE-based personal digital assistants. The Chemical Companion is available as a free download for emergency responders. Private-sector personnel involved with hazardous materials response may download the software with an approved application.

Terrorism risk posed by tankers off the East Anglian coast

Since the 9/11 attacks in 2001 and more specifically since the London 7/7 attacks in 2005, the UK has been slowly coming to terms with being a major terrorist target. However, whilst 'climate change' is a theme being taken up across virtually all government departments, the same is not yet true of counter terrorism. Yet the threat of terrorism potentially affects almost every sphere of government. Major international sporting events now have specific terrorist threats against them. For example, the Hockey World Cup and Commonwealth Games both due to take place in India in March and October respectively have each received very specific threats from an affiliate of al-Qaeda. In short, we cannot assume that anything will be immune from the threat of Islamist terrorism. It is therefore somewhat odd to say the least that the government have not made preventing terrorism a cross departmental responsibility in the way that they have made tackling 'climate change'. One illustration of the present government's lack of joined up thinking on preventing terrorism is the large number of oil tankers that for the last year have been anchoring off the East Anglian coast as a result of a



series of government decisions or more recently lack of decisions about them. This fleet of tankers numbering 30-40 at any given time and including some of the world's largest supertankers has in the last 12 months become one of the highest concentrations of oil tankers in the western world (research by the Daily Mail last year showed that even UK oil ports normally have only 4-6 tankers anchored offshore - see map). The issue only came to light last summer when Suffolk Coastal MP John Gummer asked the government why so many

tankers were anchoring off the North Suffolk coast in his constituency. It subsequently transpired that the government had, without any local consultation, secretly made an agreement with oil companies that this would be the one place in UK waters where ship to ship oil transfers would be allowed offshore. This has led to it becoming the international location for tankers from accross the world to transfer Russian oil to supertankers that are too large to enter the Baltic. In response, Mr Gummer very rightly raised serious concerns - the Suffolk coast happens to be an area of outstanding natural beauty (AONB) as well as being home to internationally important nature sites and is heavily dependent on tourism, all of which were potentially threatened by any oil spillage. There has followed a series of government ministers saying that they were moving 'quickly' to ban the practice. These included Transport Secretary Lord Adonis, who 'hoped' it might be banned before Christmas 2009 and Deputy Minister for the East of England Bob Blizzard MP, off whose Waveney constituency some of the tankers are anchored. Mr Blizzard recently announced that legislation would be laid before parliament 'as early as May', which for anyone with the slightest knowledge of the electoral process means 'not in the lifetime of this parliament'. This week the government finally started a six week 'consultation' on banning these offshore oil transfers…before it drafts a statutory order which on current timescales is unlikely to come into force until 1st October… However, as well as the environmental concerns that John Gummer has so rightly highlighted, there is also a significant security issue raised by having the largest concentration of tankers in the western world anchored just off our shores. Since 9/11 al-Qaeda and its ideological associates have made very specific threats against the oil industry. This is partly because Islamists tend to regard western use of Middle Eastern oil reserves as a particular grievance. For example, Bin Laden's 'Message to the Americans' of 6th October 2002 stated: "You steal our wealth and oil at paltry prices because of your international influence and military threats. This theft is indeed the biggest theft ever witnessed by mankind in the history of the world." However, more importantly the economic impact of the 9/11 attacks led a number of Islamists to focus part of their strategy on causing maximum economic damage to the West. Bin Laden in particular realised that oil has an immense potential as a weapon of economic warfare. In a December 2004 speech he urged his followers to engage in suicide attacks against oil targets: "Mujahidin be patient and think of the hereafter, for this path in life requires sacrifices, maybe with your life…Remember too that the biggest reason for our enemies' control over our lands is to steal our oil, so give everything you can to stop the greatest theft of oil in history from the current and future generations in collusion with the agents and the foreigners, oil,…which is the basis of all industry, has gone down in price many times. After it was going for $40 a barrel two decades ago, in the last decade it went for as little as $9, while its price today should be at least $100 at the very least. So keep on struggling, do not make it easy for them, and focus your operations on it…" Whilst oil installations particularly in Saudi Arabia and Yemen have been a focus of Islamist attacks, the ships which carry 60% of the world's oil supply have also been specifically targeted. A number of planned terrorist attacks on tankers have been thwarted by US and other forces. However, in October 2002 the French supertanker Limburg carrying almost 400,000 barrels of oil was attacked off the coast of Aden (Yemen) by a suicide boat, similar to the one that had attacked the USS Cole in Aden almost exactly two years earlier. Significantly there have also been specific threats against British tankers close to European waters. In June 2002 the Moroccan government arrested a group of al-Qaeda operatives suspected of plotting attacks on US and British tankers in the Straits of Gibraltar. The intention of such attacks is not primarily physical damage, but economic impact. A few months before the planned attacks on British and US tankers off Gibraltar an online jihadist article appeared about the advantages of bombing tankers which stated: "it is well known that the American economy will not be able to endure whatsoever the rise in oil prices." A fundamental principle of security planning is to make oneself less of a target, or at least a more difficult target to hit, than others. Terrorists always look for weak spots. Allowing the greatest concentration of oil tankers in the western world, including some of the world's largest supertankers, to anchor off our coast doesn't quite seem to qualify as making us less of a target… Astonishingly, it is our own government that has actually caused this concentration

of tankers from around the world to anchor off the Suffolk coast by specifically designating this as the one place in the UK where offshore ship to ship oil transfers would be allowed. Both this and the government's continued dragging of its heels over when it will finally ban this practice does not simply indicate a degree of incompetence. Perhaps more significantly, it also indicates the government's real state of thinking about preventing terrorism. Whilst tackling climate change is now a cross departmental responsibility, it would appear that the same degree of priority has yet be given to preventing terrorism. What this situation illustrates is that the UK needs a government with a whole new paradigm in the way it thinks about preventing terrorism.

Anti-terror buggy

A mini armoured car, designed for use in confined spaces such as airports and hotels targeted in terror attacks, has gone on display at an Indian arms fair. The battery operated, two million rupee ($45,000) Anti-Terrorist Assault Cart (Atac) is said to resemble a bullet-proof golf buggy with firing ports. It has been specially designed to transport two armed security personnel during or after terror attacks. It was created in the wake of the Mumbai (Bombay) hotel attacks of 2008. The attacks in November 2008 took place in two luxury hotels with gunmen surrounded by security forces for about 60 hours. One hundred and sixty-five people were killed in the attacks, including nine gunmen. The company behind the cart, Metaltech Motor Bodies Pvt Ltd, said the Atac had been designed in the aftermath of the attacks.

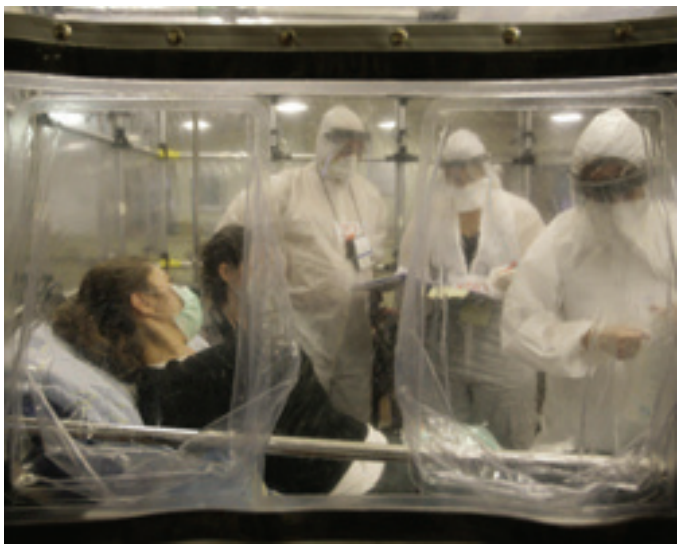
'Helplessness'

"It can extract civilians or engage terrorists," Metaltech managing director JB Sehrawat told the AFP news agency. "It's a product of our sense of helplessness over the casualties we took in the attacks. We put our heads and hearts together and came up with the Atac." It weighs just under half a tonne, has bullet-proof windows and contains numerous firing ports. Furthermore it is able to negotiate corridors and lifts. Metaltech says the squat and heavily armoured vehicle can also withstand grenade blasts and last for six hours on a single charge - with a top speed of 25km/h (15mph). The company said it was offering a prototype of the vehicle, which drew applause from visitors and military scientists attending the arms fair in Delhi, for trials with the sponsors of the Commonwealth Games, due to be held in the city in

November. India has had to reassure foreign countries that those games and next month's hockey World Cup in Delhi will be safe and free of terror attacks. "Given the growing threats, we need nano-engineering such as the Atac," Metaltech Vice President SW Thatte said.

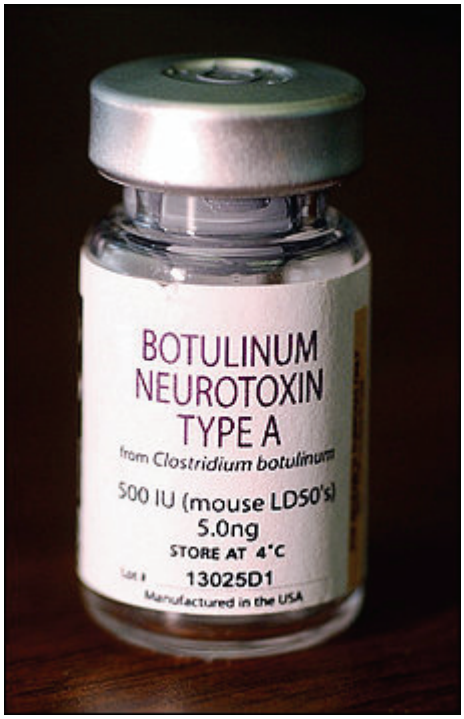
30 countries joined Israel in mass bio-terror drill

The security and health systems conducted a mass drill against a smallpox terror attack last week, involving a scenario whereby terrorists infected with a virus entered Tel Aviv posing as tourists from a European country. It was the largest drill of its kind ever held in Israel. Among other things, the drill, which was conducted in the Dan region over a two-day period, involved the simulated purchase of tens of thousands of courses of medication against the disease. Dubbed "Operation Orange Flame 4," the biological defense drill was conducted by the Defense Ministry and the Health Ministry, along with the Israel Defense Forces Home Front Command. Also involved in the drill were representatives from 30 other countries, in Israel to participate in a conference on emergency and disaster management. The drill included a response to a smallpox outbreak affecting about 1,000 people. The teams in the drill that were to investigate the identity of the biological contaminant as well as the medical teams were not told what material they were meant to be dealing with and how it would be spread. Among the participants was the CEO of SIGA Technologies Dr. Erik Rose, whose company produces anti-viral pharmaceutical agents, and which is developing a smallpox anti-viral medicine, known as ST-246 for the U.S. Department of Health. A statement released by the company in the United States said SIGA Technologies had contracted with the defense and health ministries to immediately sell Israel tens of thousands of anti-viral medications against smallpox. The exercise simulated a scenario whereby two infected terrorists spread the disease by going to a sports stadium and a hotel and infecting as many passersby as possible. In addition to the 1,000 mock-infected persons, the drill also simulated treatment and isolation of 20,000 others with the disease, and initiated a national inoculation operation against smallpox. According to researchers, smallpox has killed more people than any other disease in history - between 300 and 500 million people in the 20th century alone. In the 1960s, a world campaign began to eradicate the disease, with the last death from smallpox occuring in the mid-1970s. Medical experts say that for all intents and purposes, the disease has been completely wiped out, with samples of the virus remaining only in a small number of guarded World Health Organization labs. However, intelligence and medical officials fear that terror groups could get hold of the virus and use it for mass biological warfare. Israel is said to have enough vaccines to inoculate the entire population against smallpox. However, it is believed that terror groups could use the virus to infect a large number of people before the vaccination campaign could reach the whole population. Such a campaign could be expected to take a few weeks. The Health Ministry spokeswoman confirmed that a mock-purchase of medication against smallpox was made during last week's operation.



Officials fear toxic ingredient in Botox could become terrorist tool

In early 2006, a mysterious cosmetics trader named Rakhman began showing up at salons in St. Petersburg, Russia, hawking a popular anti-aging drug at suspiciously low prices. He flashed a briefcase filled with vials and promised he could deliver more -- "as many as you want," he told buyers -- from a supplier somewhere in Chechnya.
Rakhman's "Botox" was found to be a potent clone of the real thing, but investigators soon turned to a far bigger worry: the prospect of an illegal factory in Chechnya churning out raw botulinum toxin, the key ingredient in the beauty drug and one of world's deadliest poisons. A speck of toxin smaller than a grain of sand can kill a 150-pound adult. No Chechen factory has been found, but a search for the maker of the highly lethal toxin in Rakhman's vials continues across a widening swath of Eastern Europe, the Middle East and Asia. U.S. officials and security experts say they know the lab exists, and probably dozens of other such labs, judging from the surging black market for the drug. Al-Qaeda is known to have sought botulinum toxin. The Lebanese Hezbollah movement, which the United States has designated a terrorist organization, and other groups have bought and sold counterfeit drugs to raise cash. Now, with the emergence of a global black market for fake Botox, terrorism experts see an opportunity for a deadly convergence. "It is the only profit-making venture for terrorists that can also potentially yield a weapon of mass destruction," said Kenneth Coleman, a physician and biodefense expert. Last year, Coleman and fellow researcher Raymond Zilinskas set out to test whether militant groups could easily exploit the counterfeit Botox network to obtain materials for a bioterrorism attack. In a project sponsored by the James Martin Center for Nonproliferation Studies, two scientists found that a biologist with a master's degree and $2,000 worth of equipment could easily make a gram of pure toxin, an amount equal to the weight of a small paper clip but enough, in theory, to kill thousands of people. Obtaining the most lethal strain of the bacterium might have posed a significant hurdle for would-be terrorists in the recent past. But today, the prospect of tapping into the multibillion-dollar market for anti-wrinkle drugs has spawned an underground network of suppliers and distributors who do most of their transactions online, the researchers found. Customers don't need prescriptions or identification, other than a shipping address. "We assume that illicit producers are willing to sell their products to anyone with cash," Zilinskas said.



Lethal weapon

Botox -- the trade name for the most common commercial formulation of the drug botulinum toxin Type A -- is not a weapon. It has been used for decades to cure medical ailments including migraine headaches and facial tics, and more recently as a wildly popular treatment for the wrinkles of aging. Eight companies worldwide are licensed to make variations of the drug, and in the United States it is sold only by prescription, under the oversight of the Food and Drug Administration. Each vial contains a minuscule amount of the actual toxin, a naturally occurring nerve agent secreted by a kind of bacterium called Clostridium botulinum. The amount of poison in a prescribed dose is so small that a determined terrorist would have to obtain hundreds of vials at $400 each to kill even a single person, bioterrorism experts say.
Pure toxin is another matter. At full strength, it is the most toxic substance known to exist. So lethal is the undiluted toxin that at least three countries -- the United States, the then-intact

Soviet Union and Iraq -- explored its possible use as a possible biological or chemical weapon. All three gave up on the idea, partly because botulinum toxin degrades quickly when exposed to heat, making it poorly suited for delivery by missile or bomb. Terrorists, on the other hand, have long been drawn to the toxin as a way to inflict widespread casualties through contamination of food or water supplies. The Japanese doomsday cult Aum Shinrikyo experimented with a botulinum weapon in the early 1990s. An al-Qaeda training manual discovered in 2001 advocated the use of botulinum toxin in terrorist attacks. None of the previous efforts succeeded. Aum Shinrikyo managed to cultivate a lethal strain of the toxin-producing bacterium, but stumbled when it tried to convert the poison into an aerosol form. Al-Qaeda's known bioweapons efforts were hampered by rudimentary lab equipment and limited access to lethal strains. All of those problems can now be bypassed at a time when illicit networks are making the toxin for profit, said Coleman, the co-author of the study. "There are no major obstacles," he said. "It's not that hard to acquire the bacterial strains. But you don't even have to make it. You can buy it from existing manufacturers. And you can buy it in sufficient quantity to cause widespread harm."

Tracking the sources

The case of the Russian counterfeiter offers a glimpse into an illegal network of fake Botox suppliers that operates largely in the shadows. Anti-wrinkle drugs are exceptionally popular in Russia and Eastern Europe, where less stringent consumer laws allow their distribution by non-physicians, including operators of beauty salons. But commercial botulinum toxin is costly, and many users have flocked to vendors who offer cheaper substitutes, said Marina Voronova, until recently a Russia-based bioweapons expert who has investigated counterfeit networks in the former Soviet Union. Voronova, who now works for the nonprofit environmental group Global Green, said the Rakhman case came to light because of the man's success in undercutting licensed suppliers in St. Petersburg's salon circuit -- and also because he was among a very few vendors to make personal sales calls in an industry that mostly operates in cyberspace. Rakhman built up a brisk trade simply by walking into upscale shops and offering to sell Botox at a deep discount, she said. "He was coming to St. Petersburg with a suitcase full of vials," said Voronova, who learned details of Rakhman's sales pitch in interviews with local officials. Rakhman took regular flights from Chechnya and seemed to have unlimited supply. When an undercover investigator asked how many doses he could deliver, he replied: "As many as you want," Voronova said, citing an account given to her by a Russian investigator. Rakhman abruptly halted his St. Petersburg trips when local authorities began closing in, and Russian investigators were never able to determine where his counterfeit Botox was manufactured. Zilinskas and Coleman, in their study, concluded that much of the fake Botox sold over the Internet originated in China, a country with a history of producing knockoff versions of drugs and cosmetic products sold under patent in the West. But they noted that the toxin could be made in a garage-size laboratory almost anywhere, including Chechnya, notorious for black-market smuggling and a home-grown Islamic insurgency. China recently acknowledged the seriousness of Botox counterfeiting domestically when it announced it was shutting down a factory in Shanxi province accused of making a copycat version of the drug. That crackdown came several months after Allergan, the chief U.S. manufacturer of commercial Botox, formally complained to Beijing that Chinese manufacturers were violating Allergan's patent protections. Allergan officials say they are continuing to work with China to identify bogus manufacturers, but they also acknowledge that some producers are outlaws who hide from Chinese authorities by frequently changing their names and business addresses. "There are organized criminal networks, and they act as registered agents for one another," said Allergan spokeswoman Caroline Van Hove. Indeed, Internet hawkers of discount Botox -- sold under names such as Beauteous -- often list legitimate-sounding Chinese addresses that turn out to be fictional. The Washington Post recently sought to locate three Chinese firms that offered cut-rate Botox over the Web, only to find empty lots and dead ends. The manufacturer of Beauteous gave a manufacturing address that turned out to be an upscale corner of Beijing where many foreign embassies are located. The street number listed on the Web site does not exist.

Home-grown threats?

No laboratories for fake Botox have turned up in the United States, but there have been prominent examples of doctors and vendors who obtained cheap, unlicensed botulinum toxin to sell to unsuspecting patients and customers, sometimes with lethal results. In 2004, U.S. Justice Department officials raided a string of clinics in five states after uncovering a supply network that substituted industrial-grade botulinum toxin for commercial Botox. The inferior toxin, which was made legally for laboratory research and not licensed for human use, paralyzed four patients. But U.S. investigators acknowledge that they know less about the volume of trade in Botox-like drugs over the Internet. The counterfeits are part of a booming trade in fake pharmaceuticals ranging from cancer-treating medicines to knockoff Viagra. One U.S. investigator called the problem "out of control." "We don't know how much is getting through," said the investigator, who insisted on anonymity because of his involvement in ongoing criminal probes. The fact that one of the hottest commodities happens to be a lethal poison elevates the risk to whole new level, he said. "We know al-Qaeda has talked about going after food supplies in the United States," the official said. "There are new reasons to be concerned about what they're going to target next."

'Chemical Ali' executed in Iraq after Halabja ruling

Majid, an enforcer in Saddam Hussein's regime and his cousin, had earlier been sentenced to death four times for genocide and crimes against humanity. Earlier this month, he was sentenced to death for ordering the gas attack on the Kurdish town of Halabja in 1988. It is believed that about 5,000 people died in the attack. Iraqi jets swooped over Halabja and for five hours sprayed it with a lethal cocktail of mustard gas and the nerve agents Tabun, Sarin and VX.

Brutality

Majid was "executed by hanging until death", Iraqi government spokesman Ali al-Dabbagh said in a statement "The execution happened without any violations, shouting or cries of joy," he added, in sharp contrast to Saddam's death on the gallows in 2006.

Iraqi state television, al-Iraqiya, broadcast pictures of what it said was the execution of Majid, although the BBC has not yet confirmed the authenticity of the images. News of the hanging came shortly after three suicide car bombs struck in central Baghdad. It was not immediately clear whether the attacks were linked to his execution. Majid was first sentenced to hang in June 2007 for his role in a military campaign against ethnic Kurds, codenamed Anfal, that lasted from February to August of 1988. In December 2008 he also received a death sentence for his role in crushing a Shia revolt after the 1991 Gulf War. In March 2009 he was sentenced to death, along with others, for the 1999 killings of Shia Muslims in the Sadr City district of Baghdad. The BBC's Jim Muir in Baghdad says Majid could have been hanged earlier - after his first death sentence for the Anfal campaign. But it was important to Iraqi Kurds to see him convicted of the Halabja attack, seen as one of the worst atrocities of Saddam Hussein's regime.

FOUR DEATH SENTENCES

- Jan 2010: For ordering gas attack on Kurdish town of Halabja in 1988 in which 5,000 people died
- March 2009: For the 1999 killings of Shia Muslims in the Sadr City district of Baghdad
- Dec 2008: For his role in crushing a Shia revolt after 1991 Gulf War
- June 2007: For role in six-month military campaign against ethnic Kurds, codenamed Anfal, in 1988

No remorse

Our correspondent says there will be great rejoicing or, at the very least, quiet relief among both Iraq's Shia and Kurdish communities, which have suffered greatly at his hands. There was a mixed reaction from ordinary Iraqis to news of the execution. "I give my condolences to the Iraqi people on the death of Ali Hassan al-Majid, who was killed by traitors and hooligans," said a resident of Majid's home town, Tikrit. But Baghdad resident Ali Suhail said the execution was just: "He had executed so many people. So he deserves to be executed." A resident of Halabja also said he was pleased: "We, the families of those killed in the attack on Halabja, are very pleased to hear that Ali Hassan al-Majid was executed. "Once again we call upon the Iraqi people and government to be united and serve the Iraqi people and families of those killed in poison gas attack." Majid - the King of Spades in the US military's pack of cards of most-wanted Iraqis - was arrested in August 2003. He has refused to express remorse at any of his trials, insisting that he was acting in the interests of Iraqi security. The Iraqi High Tribunal was set up to try former members of Saddam Hussein's mainly Sunni government and was the same one that sentenced the former president to death. Footage of Saddam's execution in December 2006 was posted on the internet. It showed the dictator being confronted by opponents who jeered and clapped as he was being hanged.

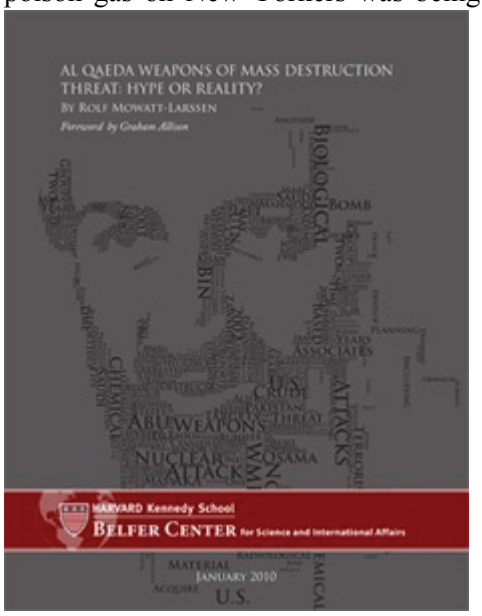
Terror group Lashkar-e-Taiba 'planning paraglider attacks' in India

Indian intelligence officials suspect that the terrorist group behind the 2008 Mumbai attacks is planning another audacious strike on the country — this time from the air, using suicide bombers flying paragliders. U. K. Bansal, an Indian Home Ministry official, told reporters that the Pakistan-based Lashkar-e-Taiba faction was thought to have acquired a number of the gliding parachutes. "We have intelligence reports that LeT has purchased 50 paragliding kits from Europe with an intention to launch attacks on India," he said. No other details were given, but security levels have been hiked across the country ahead of tomorrow's Republic Day celebrations, one of India's biggest holidays. If accurate, the intelligence would mark a radical new tactic. Experts said the potential threat posed by jihadist paragliders would have to be considered seriously as LeT — which murdered 166 people in Mumbai in a sophisticated commando-style raid — has already proven itself highly innovative. "The Mumbai attack [where ten LeT gunmen sailed to Mumbai from Karachi, murdering the crew of a fishing boat en route], was the group's first act of sea-borne terrorism," said B. Raman, a former counter-terrorism chief in the Indian foreign intelligence service, the Research and Analysis Wing. "It would be natural for them to plan another spectacular attack from the air. The warning has to be taken seriously." Paragliders usually do not have an engine but can — in skilled hands and in the right conditions — cover large distances. The world record for flying a paraglider is more than 460km (285 miles). However, they usually need to be launched from a high point, or towed by a boat or car, which could

limit their effectiveness. The latest alert came after the US Defence Secretary Robert Gates warned last Wednesday that a syndicate of terrorist groups could trigger a war between Pakistan and India through a “provocative act”. Relations between India and Pakistan, nuclear armed neighbours which have gone to war three times, deteriorated sharply in the wake of the Mumbai attacks. LeT has been active since the early 1990s and is said to have been created with the help of Pakistan’s powerful spy agency, the Directorate of Inter-Service Intelligence. It was founded to try and free Kashmir from Indian control, and came to specialise in the type of suicidal raid that shocked the world over a 60-hour period when Mumbai was attacked in November 2008. The organisation was banned in Pakistan in 2002. Indian officials also warned last week that a terrorist group — possibly LeT or al-Qaida — was poised to hijack an Indian passenger plane. On Friday, an Indian Home Ministry official confirmed that security had been tightened at all airports. Officials said that sky marshals would be deployed on flights around the region. Indian officials have feared the possibility of an air attack for some time. Eight days after the Mumbai attacks, the Defence Ministry ordered the nation’s armed forces to be on guard against “terror strikes from the air”. At that time, the India Bureau for Civil Aviation is thought to have been given warning of plans to capture one or more planes at Delhi, Mumbai, Bangalore or Chennai airports, the country’s main transport hubs. Officials said that credible intelligence indicated a plan to attack a major population centre using an airliner in an assault that would resemble those made on New York in 2001. There were also fears that one of India’s nuclear facilities could be targeted. The last time an Indian passenger plane was targeted was Christmas Eve 1999, when an Indian Airlines flight was hijacked by Pakistani nationals as it flew from Kathmandu to Delhi. That plane landed in Afghanistan, where the hostages were released in exchange for three Islamist extremists.

Al-Qaeda still aims to use weapons of mass destruction against U.S.

When al-Qaeda's No. 2 leader, Ayman al-Zawahiri, called off a planned chemical attack on New York's subway system in 2003, he offered a chilling explanation: The plot to unleash poison gas on New Yorkers was being dropped for "something better," Zawahiri said in a message intercepted by U.S. eavesdroppers. The meaning of Zawahiri's cryptic threat remains unclear more than six years later, but a new report warns that al-Qaeda has not abandoned its goal of attacking the United States with a chemical, biological or even nuclear weapon. The report, by a former senior CIA official who led the agency's hunt for weapons of mass destruction, portrays al-Qaeda's leaders as determined and patient, willing to wait for years to acquire the kind of weapons that could inflict widespread casualties. The former official, Rolf Mowatt-Larssen, draws on his knowledge of classified case files to argue that al-Qaeda has been far more sophisticated in its pursuit of weapons of mass destruction than is commonly believed, pursuing parallel paths to acquiring weapons and forging alliances with groups that can offer resources and expertise. "If Osama bin Laden and his lieutenants had been interested in . . . small-scale attacks, there is little doubt they could have done so now," Mowatt-Larssen writes in a report released Monday by the Harvard Kennedy School of Government's Belfer Center for Science and International Affairs. The report comes as a panel on weapons of mass destruction appointed by Congress prepares to release a new assessment of the federal government's preparedness for such an attack. The review by the bipartisan Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism is particularly critical of the Obama administration's actions so far

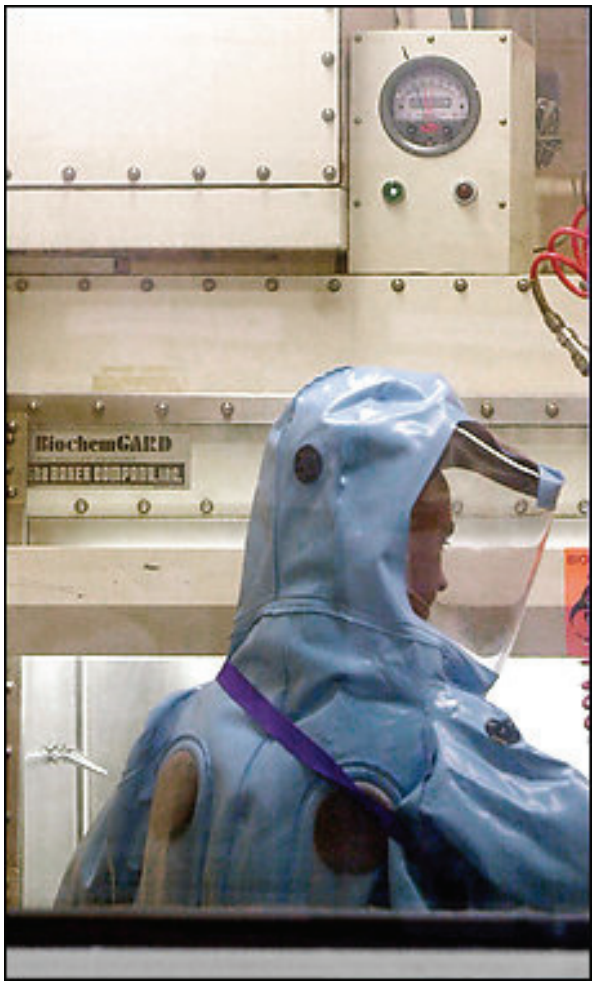


in hardening the country's defenses against bioterrorism, according to two former government officials who have seen drafts of the report. The commission's initial report in December 2008 warned that a terrorist attack using weapons of mass destruction was likely by 2013. Mowatt-Larssen, a 23-year CIA veteran, led the agency's internal task force on al-Qaeda and weapons of mass destruction after the Sept. 11, 2001, terrorist attacks and later was named director of intelligence and counterintelligence for the Energy Department. His report warns that bin Laden's threat to attack the West with weapons of mass destruction is not "empty rhetoric" but a top strategic goal for an organization that seeks the economic ruin of the United States and its allies to hasten the overthrow of pro-Western governments in the Islamic world. He cites patterns in al-Qaeda's 15-year pursuit of weapons of mass destruction that reflect a deliberateness and sophistication in assembling the needed expertise and equipment. He describes how Zawahiri hired two scientists -- a Pakistani microbiologist sympathetic to al-Qaeda and a Malaysian army captain trained in the United States -- to work separately on efforts to build a biological weapons lab and acquire deadly strains of anthrax bacteria. Al-Qaeda achieved both goals before September 2001 but apparently had not successfully weaponized the anthrax spores when the U.S.-led invasion of Afghanistan forced the scientists to flee, Mowatt-Larssen said. "This was far from run-of-the-mill terrorism," he said in an interview. "The program was highly compartmentalized, at the highest level of the organization. It was methodical, and it was professional." Mowatt-Larssen said he has seen no evidence linking al-Qaeda's program with the anthrax attacks on U.S. politicians and news outlets in 2001. Zawahiri's plan was aimed at mass casualties and "not just trying to scare people with a few letters," he said. Evidence from al-Qaeda documents and interrogations suggests that terrorists leaders had settled on anthrax as the weapon of choice and believed that the tools for a major biological attack were within their grasp, the former CIA official said. Al-Qaeda remained interested in nuclear weapons as well but understood that the odds of success were much longer. "They realized they needed a lucky break," Mowatt-Larssen said. "That meant buying or stealing fissile material or acquiring a stolen bomb." Bush administration officials feared that bin Laden was close to obtaining nuclear weapons in 2003 after U.S. spies picked up a cryptic message by a Saudi affiliate of al-Qaeda referring to plans to obtain three stolen Russian nuclear devices. The intercepts prompted the U.S. and Saudi governments to go on alert and later led to an aggressive Saudi crackdown that resulted in the arrest or killing of dozens of suspected al-Qaeda associates. After that, terrorists' chatter about a possible nuclear acquisition halted abruptly, but U.S. officials were never certain whether the plot was dismantled or simply pushed deeper underground. "The crackdown was so successful," Mowatt-Larssen said, "that intelligence about the program basically dried up."

Report Sounds Alarm Over Bioterror

Seven years after the 2001 anthrax attacks, a congressionally ordered study finds a growing threat of biological terrorism and calls for aggressive defenses on par with those used to prevent a terrorist nuclear detonation. Due for release next week, a draft of the study warns that future bioterrorists may use new technology to make synthetic versions of killers such as Ebola, or genetically modified germs designed to resist ordinary vaccines and antibiotics. The bipartisan report faults the Bush administration for devoting insufficient resources to prevent an attack and says U.S. policies have at times impeded international biodefense efforts while promoting the rapid growth of a network of domestic laboratories possessing the world's most dangerous pathogens. The number of such "high-containment" labs in the United States has tripled since 2001, yet U.S. officials have not implemented adequate safeguards to prevent deadly germs from being stolen or accidentally released, it says. "The rapid growth in the number of such labs in recent years has created new safety and security risks which must be managed," the draft report states. The report is the product of a six-month study by the Commission on the Prevention of Weapons of Mass Destruction and Terrorism, which Congress created last spring in keeping with one of the recommendations of the 9/11 Commission. Drafts of chapters pertaining to bioterrorism were obtained by The Washington

Post. The document cites progress in many areas of biodefense since the deadly anthrax attacks of 2001, including major investments in research, stockpiling of drugs and development of a network of sensors designed to detect airborne viruses and bacteria. The Bush administration has spent more than $20 billion on such countermeasures, far more than any of its predecessors. But the report says the next administration must do much more to prevent dangerous pathogens from falling into the wrong hands in the first place. While politicians often warn about the dangers of nuclear terrorism, a serious biological attack would be easier to accomplish and deserves a top priority, it says. "The more probable threat of bioterrorism should be put on equal footing with the more devastating threat of nuclear terrorism," the draft states. It calls on the Obama administration to develop a comprehensive approach to preventing bioterrorism and to "banish the 'too-hard-to-do' mentality that has hobbled previous efforts."



Some bioweapons specialists have argued that it is practically impossible to prevent a biological attack, because lethal strains of anthrax bacteria and other deadly microbes can be found in nature. But the report argues that it would be far easier for bioterrorists to obtain the seeds of an attack from laboratories that have ready supplies of "hot" strains. U.S. officials think an Army biodefense lab was the source of the anthrax spores used in the 2001 attacks that killed five people. The biodefense research industry that sprang up after 2001 offers potential solutions to a future attack, but also numerous new opportunities for theft or diversion of deadly germs, the report says. Today, about 400 research facilities and 14,000 people are authorized to work with deadly strains in the United States alone, and several of the new labs have been embroiled in controversies because of security breaches, such as the escape of lab animals. No single government agency has authority to oversee security at these U.S. labs, most of which are run by private companies or universities. Such facilities in the United States "are not regulated" unless they obtain government funding or acquire pathogens from the government's list of known biowarfare agents. Because of this gap, labs can work with "dangerous but unlisted pathogens, such as the SARS virus," which causes severe acute respiratory syndrome, without the government's knowledge. Internationally, the challenges are even greater. While the U.S. government continues to spend billions of dollars to secure Cold-War-era nuclear stockpiles, similar efforts to dismantle Soviet bioweapons facilities have been scaled back because of disagreements with the Russian government, the report notes. The only global treaty that outlaws the development of biological weapons has no mechanism for inspections or enforcement. Efforts to strengthen the 1972 Biological Weapons Convention were dealt a symbolic blow in 2001 when the Bush administration withdrew its support for a new accord that had been under negotiation for six years. Meanwhile, the growth in biodefense research seen in the United States has spread to dozens of countries, including developing nations such as Malaysia and Cuba that are investing heavily to develop world-class biotech industries. One of the fastest-growing technologies is DNA synthesis, which offers new capabilities to

alter the genes of existing pathogens or synthesize them artificially. While governments, trade groups and professional organizations are experimenting with various voluntary controls over such new capabilities, the United States should lead a global effort to strengthen oversight and clamp down on the unregulated export of deadly microbes, the panel said. "Rapid scientific advances and the global spread of biotechnology equipment and know-how are currently outpacing the modest international attempts to promote biosecurity," the report says.

Al Qaeda's Pursuit of Weapons of Mass Destruction

In 1998, al Qaeda leader Osama bin Laden declared that acquiring and using weapons of mass destruction (WMD) was his Islamic duty -- an integral part of his jihad. Systemically, over the course of decades, he dispatched his top lieutenants to attempt to purchase or develop nuclear and biochemical WMD. He has never given up the goal; indeed, in a 2007 video, he repeated his promise to use massive weapons to upend the global status quo, destroy the capitalist hegemony, and help create an Islamic caliphate. Since the mid-1990s, al Qaeda's WMD procurement efforts have been managed at the most senior levels, under rules of strict compartmentalization from lower levels of the organization, and with central control over possible targets and the timing of prospective attacks. The modus operandi has been top-down -- more similar to the 9/11 attacks than to more recent bottom-up efforts, like the attempted bombing of Flight 253. For instance, al Qaeda deputy chief Ayman al-Zawahiri personally shepherded the group's ultimately unsuccessful efforts to set off an anthrax attack in the United States. Al Qaeda concentrated its efforts on nuclear devices in the run-up to the September 11, 2001 attacks. Based on the timing and nature of its WMD-related activity in the 1990s, al Qaeda hoped to use such weapons in the United States during an intensified campaign following the 9/11 attacks. There is no indication that the fundamental objectives that lie behind its WMD intent have changed over time. Al Qaeda seems to have failed in its mission to successfully detonate WMD due to its overpowering interest in such big-casualty, big-impression attacks. The organization has not pursued simpler, cheaper, and easier-to-use technologies, like crude toxins and poisons, with anything like the same fervor. To be sure, experimentation with and training in such agents was standard fare in al Qaeda's camps in Afghanistan before 9/11. But bin Laden and his top associates left the initiative to lower-ranking planners and individual cells. Once, Zawahiri even canceled a planned attack on the

New York City subway in lieu of "something better" that never materialized. But just because "something better" has never materialized, and just because the threat of WMD terrorism has been used to political ends, does not mean that WMD are not a threat. This chronology provides the knowable extent of al Qaeda's interest in, plans to obtain, and efforts to use the world's most deadly weapons.

Timeline

- **1988**: Osama bin Laden founds al Qaeda. Other founding members include Jamal al-Fadl, Abu Ayoub al-Iraqi, Ayman al-Zawahiri, and Dr. Fadhl al-Masry.
- **Winter 1990 - Spring 1991:** Bin Laden and his associates relocate to Khartoum, Sudan.
- **Feb. 26, 1993:** A car bomb is detonated under the World Trade Center in New York City. According to Federal Judge Kevin Duffy, the goal of al Qaeda mastermind Ramzi Youssef was to "engulf the victims trapped in the North Trade Tower in a cloud of cyanide gas." The explosion incinerates the gas, greatly decreasing the number of casualties. Five people die.
- **Late 1993 - early 1994:** Al Qaeda tries to acquire uranium in Sudan to use in a nuclear device. This is the first evidence of bin Laden's plans to purchase nuclear material for an improvised nuclear device.
- Evidence of this attempted transaction comes from Fadl, who defected from al Qaeda in 1996 and became a source for the FBI and CIA. He testifies in court that former Sudanese President Saleh Mobruk attempted to help al Qaeda acquire uranium of South African origin. Fadl says he heard later that the uranium, which al Qaeda acquired for $1.5 million and was tested in Cyprus, was "genuine."
- **1996:** Zawahiri, leader of the Egyptian Islamic Jihad (which later merged into al Qaeda), is detained and released by the state security service in Russia. There is unconfirmed speculation that Zawahiri was seeking nuclear weapons or material there.
- **May 21, 1996:** Abu Ubeida al-Banshiri, a founder of al Qaeda, dies in a ferry accident on Lake Victoria. According to testimony from senior al Qaeda officials, he was seeking nuclear material in southern Africa.
- **May 1996:** Al Qaeda's leadership relocates to Afghanistan.
- **Early 1998:** Zawahiri's Egyptian Islamic Jihad (EIJ) merges with al Qaeda. Zawahiri and EIJ bring technological know-how about chemical, biological, radiological, and nuclear weapons to the more ideological al Qaeda. Zawahiri takes control of nuclear and biological weapons development for the whole organization.
- Before this time, high-ranking al Qaeda members had held internal discussions about the wisdom and efficacy of pursuing chemical, biological, radiological, and nuclear interests. 1998 marked the year when systematic and programmatic efforts began.
- **Feb. 23, 1998:** Bin Laden issues a fatwa against the United States, saying, "The ruling to kill the Americans and their allies -- civilians and military -- is an individual duty for every Muslim who can do it in any country in which it is possible to do it."
- **Aug. 7, 1998:** Al Qaeda initiates simultaneous suicide truck-bomb attacks at the U.S. embassies in Dar-es-Salaam, Tanzania, and Nairobi, Kenya. At least 230 civilians, mostly locals, die. The FBI places bin Laden on its "10 most wanted" list and starts monitoring al Qaeda closely.
- **Aug. 20, 1998:** The United States destroys the Al-Shifa pharmaceutical factory in Khartoum, Sudan, based on suspicions that the plant might be producing the nerve agent VX for the Sudanese government and al Qaeda.
- **Dec. 24, 1998:** Osama bin Laden states in an interview with Time's Rahimullah Yusufzai: "Acquiring [WMD] for the defense of Muslims is a religious duty."
- **1999-2001:** Al Qaeda training camps in Afghanistan conduct basic training courses in chemical, biological, and radiological weapons for hundreds of extremists. Abu

Khabab al-Masri, a chemist and top bomb-maker, and Abu Musab al-Suri (better known as Setmariam), a Spanish citizen born in Syria, conduct the training courses at the Durante and Tarnak farms.

- Setmariam is captured in a raid in Pakistan on Nov. 3, 2005. The outspoken proponent of using chemical, biological, radiological, and nuclear weapons in attacks against the United States tells authorities that al Qaeda had made a mistake by not utilizing WMD on Sept. 11, 2001.
- **Early 1999:** Zawahiri recruits a midlevel Pakistani government biologist with extremist sympathies, Rauf Ahmed, to develop a biological weapons program. He is provided with a laboratory in Kandahar, Afghanistan.
- **Early 1999:** The head of Jemaah Islamiyah (JI), an al Qaeda-associated militant Islamist group based in southwest Asia, introduces an ex-Malaysian Army captain and California Polytechnic State University (better known as CalPoly) graduate, Yazid Sufaat, to Zawahiri.
- Zawahiri starts a second, independent, parallel program to the al Qaeda Afghanistan program, with Sufaat at the helm. Neither program knows of the existence of the other; each reports to Zawahiri independently. This collaboration between al Qaeda and JI is likely the first instance of Islamist terrorist groups jointly developing WMD.
- The Afghanistan program, headed by Ahmed, acquires equipment and sets up labs. Sufaat, a more trusted JI member, focuses on developing the anthrax pathogen. He has been described as the "CEO" of al Qaeda's anthrax program.
- **1999-2001:** Al Qaeda's Abdel Aziz al-Masri conducts nuclear-related explosive experiments in the desert. He is an explosives expert and chemical engineer by training, reportedly self-taught on things nuclear.
- **January 2001:** Pakistani nuclear scientists with extremist sympathies create the humanitarian nongovernmental organization Umma Tameer e Nau (UTN). Bashiruddin Mahmood, the former head of Pakistan's Khushab plutonium reactor, is its chair; the former head of Pakistan's Inter-services Intelligence directorate, Hamid Gul, is on its board.
- Mahmood is later forced into retirement due to concerns about his extremist sympathies and reliability. He pens controversial books predicting an imminent apocalypse, offering a radical interpretation of the Quran.
- **June 2001:** Sufaat hosts a meeting of the 9/11 attackers in Kuala Lumpur. Sufaat provides a false Malaysian address for Zacarias Moussaoui, who was arrested shortly before 9/11, to help him travel to the United States.
- **Before Aug. 2001:** UTN's Mahmood discreetly offers to construct chemical, biological, or nuclear weapons programs for al Qaeda and the Libyan government. The United States gathers intelligence on the offers and passes it to the Libyan intelligence service office in London. The head of the London office later confirms to the United States that Libya will have no dealings with UTN.
- **August 2001:** Zawahiri personally inspects Ahmed's completed laboratory in Kandahar. He separately meets with Sufaat for a weeklong briefing on the reportedly successful efforts to isolate and produce a lethal strain of anthrax.
- **Summer 2001:** Mohammed Atta, an organizer and leader of the Sept. 11 attacks, allegedly meets with WMD figures, including al Qaeda's Adnan Shukrijumah. According to the FBI, Shukrijumah cases targets in New York City for possible attacks; he is later associated with multiple nuclear and "dirty bomb" plots.
- A person fitting Atta's description seeks to apply for a loan to purchase a crop duster in Florida, and is refused. After 9/11, the FBI approaches every U.S. crop duster company, searching for links to terrorists.
- **Summer 2001:** The United States detains Abderraouf Yousef Jdey, who traveled with Moussaoui from Canada into the United States. Moussaoui is detained with crop duster manuals in his possession; Jdey has biology textbooks. They might have been involved in planning a second wave of attacks for immediately after 9/11.

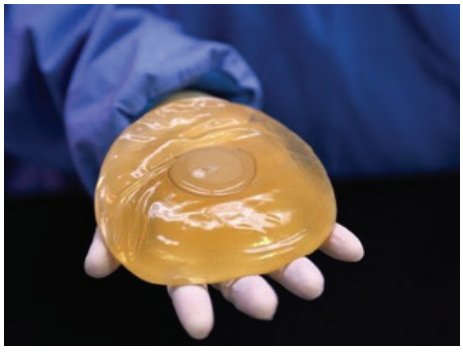
- **Sept. 11, 2001:** Nineteen members of al Qaeda board two passenger planes in the United States, hijacking them and piloting them into the two towers of the World Trade Center in New York. Nearly 3,000 die.
- **September 2001:** Al Qaeda breaks camp. Most senior operatives and their families **flee Afghanistan in anticipation of an imminent U.S. invasion.**
- **Oct. 7, 2001:** The United States launches Operation Enduring Freedom, invading Afghanistan to neutralize and destroy al Qaeda and bin Laden.
- **Oct. 23, 2001:** Pakistani intelligence services detain a long list of UTN members and associates, at the request of the U.S. government.
- Sometime this month, George Tenet, the director of the CIA, meets with President Pervez Musharraf of Pakistan regarding the threat posed by UTN and the evidence that al Qaeda might be building chemical, biological, and nuclear weapons programs. Musharraf reportedly responds, "Men in caves can't do that."
- Still, Musharraf agrees to work with the U.S. government to out and arrest Pakistani scientists cooperating with al Qaeda. Musharraf and Pakistan's intelligence services follow through with the promise.
- **1990s-2001:** A nuclear weapons network run by the father of the Pakistan nuclear weapons program, Abdul Qadeer Khan, supplies Iran, North Korea, and Libya with nuclear technologies and know-how. Nuclear bomb designs are found on the computer of a European supplier working with the Khan network. Al Qaeda reportedly contacts associates of Khan for assistance with their weapons program. The Khan network rejects them, for unknown reasons.
- **Nov. 7, 2001:** Bin Laden states in an interview with Pakistani journalist Hamid Mir, "I wish to declare that if America used chemical or nuclear weapons against us, then we may retort with chemical and nuclear weapons. We have the weapons as a deterrent."
- In the same interview, Zawahiri states, "If you have $30 million, go to the black market in central Asia, contact any disgruntled Soviet scientist, and a lot of dozens of smart briefcase bombs are available. They have contacted us, we sent our people to Moscow to Tashkent to other central Asian states, and they negotiated and we purchased some suitcase bombs."
- **Nov. 14, 2001:** U.S. President George W. Bush meets with Russian President Vladimir Putin in Crawford, Texas. Bush presents a briefing on the proliferation threat posed by UTN. Bush asks Putin if he is certain that all Russian nuclear weapons and materials are secure. Putin responds that he can only vouch for the safety of nuclear materials since he gained power.
- **November 2001:** Pakistan arrests Mahmood and many other members of UTN. Mahmood confesses that he met with bin Laden around a campfire that summer in Pakistan. He says they discussed how al Qaeda could build a nuclear device. He drew a very rough sketch of an improvised nuclear device, but advised bin Laden that it would be too hard to develop weapons-usable materials for it. Bin Laden reportedly said, "What if I already have them?"
- **November 2001:** A search of UTN's Kabul office produces documents containing crude chemical, biological, radiological, and nuclear-related plans, including hand-written notes in Arabic and Internet-related searches.
- **December 2001:** Malaysian authorities arrest Sufaat, the JI leader working with al Qaeda on nuclear weapons. Pakistani authorities arrest Ahmed, his Afghan counterpart, at his home in Islamabad. Ahmed confesses his involvement in the project and provides substantiating evidence.
- **January 2002:** U.S. and Egyptian forces capture al Qaeda senior operative Ibn al-Shaykh al Libi. During interrogation by Egyptians, al Libi claims al Qaeda operatives received chemical, biological, radiological, and nuclear weapons training in Baghdad. He claims several small containers of nuclear material were smuggled into New York City by the Russian mafia. Al Libi later recants this statement.

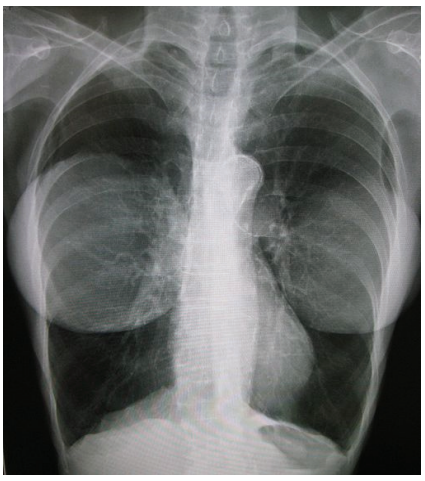
- **March 2002:** Russian special services assassinate Chechen leader Ibn al-Khattab, using poison, the kind of weapon he hoped to use against high-level Russian targets.
- **March 28, 2002:** U.S. and Pakistani forces capture al Qaeda leader Abu Zubaydah in Faisalabad, Pakistan. During interrogation, he reveals a plot by an American associate of al Qaeda, Jose Padilla, to explode a "dirty bomb" in the United States. Padilla is subsequently identified and arrested in Chicago.
- **Spring 2002:** In Khartoum, Sudan, a CIA officer meets with two senior al Qaeda associates, Mubarak al-Duri and Abu Rida Mohammed Bayazid, in a brokered arrangement. The CIA officer attempts to determine whether they were involved in al Qaeda's nuclear and biological weapons programs.
- Bayazid, a founding member of al Qaeda, graduated from the University of Arizona with an advanced degree in physics. He was directly involved in al Qaeda's attempt to purchase uranium in 1993 and 1994. Al-Duri, an agronomist, also received his degree at the University of Arizona. He told the CIA officer, "Killing millions [of you] is justifiable by any means.... It is your doing. You made us what we are."
- **Summer 2002:** Al Qaeda leaders in Saudi Arabia begin planning attacks against the royal family and Saudi oil assets. Nuclear and biological weapons-related references begin to appear in communications between top-level al Qaeda leaders and the Saudi cell.
- **Summer 2002:** With bin Laden's blessing, al Qaeda issues two fatwas to justify an escalation of terrorism. One authorizes attacks on infidels other than Americans, including the Saudi royal family. The other justifies the use of WMD. Al Qaeda-associated extremists start to case Saudi targets, including the city of Ras al-Tanura and facilities belonging to oil giant Aramco.
- **June 2002:** Extremists under Zarqawi's command conduct crude chemical and biological training and experiments in a remote camp, Khurmal, in northeastern Iraq. The commanders include men who served with Zarqawi at the Herat camp. Zarqawi has close ties with al Qaeda, but is an independent operator who never swore loyalty (bayat) to bin Laden.
- **July 10, 2002:** Al Qaeda spokesman Sulayman Abu Ghayth al-Libi, under "house arrest" in Iran, says al Qaeda's fatwa justifies the use of WMD to kill four million Americans.
- **August 2002:** CNN runs an exposé on al Qaeda's late-1990s experiments with crude toxins and poisons. Abu Khabab al-Masri led the gruesome efforts, testing the lethality of cyanide creams, ricin, mustard, sarin, and botulinum. A tape shows al Qaeda associates gassing dogs to death. Al-Masri later laments that his students did not take the training to heart by using the toxic weapons in terrorist attacks.
- **September - December 2002:** Zarqawi associates infiltrate Turkey, Britain, Spain, Italy, France, Sweden, Germany, and other countries. They begin coordinating and planning ricin and cyanide attacks via a loose association of cells.
- Bush and Vice President Dick Cheney receive briefings on the Zarqawi network's activities and plans to attack with poisons and toxins. Over the course of several briefings, U.S. knowledge of the extent of the network grows from a handful of terrorists in one country to dozens of extremists in 30 countries.
- **Jan. 5, 2003:** In a bloody raid on a safehouse, Britain arrests seven extremists plotting to use ricin poison on the London Underground. This represents the first in a wave of arrests of Zarqawi-network terrorists in Britain, continental Europe, and beyond. The arrests confirm intelligence reports, producing forensic evidence of planning for crude-poison and toxin attacks.
- **January - March 2003:** Zarqawi-associated operatives are arrested, disrupting ricin and cyanide attacks, in Britain, Spain, Italy, and France.
- **Feb. 5, 2003:** U.S. Secretary of State Colin Powell gives a speech to the U.N. Security Council, naming the Herat camp leadership, including Zarqawi. He identifies poison-attack cells across Europe.

- **February - March 2003:** Zarqawi returns to Baghdad to prepare for an insurgency to meet the U.S. invasion of Iraq.
- **March 1, 2003:** 9/11 mastermind Khalid Sheikh Mohammed (KSM) is captured in Pakistan. Confronted with the evidence found during the raid, KSM confirms some details of al Qaeda's nuclear and biological weapons programs. He later recants some of his testimony.
- **March 2003:** Zawahiri calls off an attack that had been planned against the New York City subway system, in lieu of "something better." Al Qaeda associates from Bahrain had cased the subway system in December 2002 and planned an attack with a homemade cyanogen gas-releasing device called a "mobtaker."
- **March-May 2003:** Al Qaeda Saudi senior operative Abu Bakr communicates with Iran-based al Qaeda senior members, including the chief of operations. They plan to purchase three "Russian nuclear devices." An unidentified Pakistan specialist is enlisted to verify the goods.
- **May 21, 2003:** Radical Saudi cleric Nasir al-Fahd writes a fatwa justifying the use of WMD. Another radical cleric, Ali al-Khudair, endorses it.
- **May 28, 2003:** The Saudi intelligence agency makes a series of arrests in a campaign to neutralize al Qaeda in Saudi Arabia and eliminate its capacity to mount attacks. Al-Fahd is arrested. Cyanide is found in an al Qaeda safehouse in Riyadh.
- **June 26, 2003:** An Armenian citizen, Garik Dadayan, is caught with 170 grams of highly enriched uranium on the Georgia-Armenia border. This is allegedly a sample of a larger cache, due to be sold to an unknown customer, possibly in the Middle East.
- **Aug. 13, 2003:** Riduan Isamuddin, the head of JI, is arrested. He provides confirmation of his role in the anthrax program.
- After August 2003, it is not possible to extend the chronology without excluding considerable information that is sensitive or classified. Even though the passage of time has enabled more of the story of al Qaeda's WMD efforts to be told, much detail remains too sensitive to reveal, even in the years covered by this chronology. It is not the author's intent to reveal information that might frustrate efforts to identify and neutralize al Qaeda's ongoing efforts to develop weapons of mass destruction. Rather, it is his hope that an accurate portrayal of a compact period in the recent past would enable the reader to develop an understanding of the intensity of al Qaeda's interest in WMD, as well as an appreciation for the U.S. government's response to it.

Breast Implant Bombs Could Be Terrorists New Weapon

Breast implant bombs could be the newest method for terrorists to conceal explosives according to this report. British spy satellites have reportedly intercepted terrorist





communications from Pakistan and Yemen, talking about women suicide bombers getting explosives put inside breast implants. Former Houston FBI Director Don Clark said he believes U.S. Homeland Security is taking this threat very seriously. “Sometimes as

ridiculous as it may sound, it can probably be pulled off…Terrorists and terrorist attack are a reality," Clark said. The British Intel service reports several plastic surgeons who were trained in many of London's hospitals have returned to their countries to perform the surgeries. "I am sure we are gathering all the information, intelligence that the government can" he said. "They are also securing all the ports, airports and main attractions as much as possible. The government takes these types of threats seriously and not relaxed." Houston plastic surgeon Dr. Franklin Rose said that the industry's technology makes the bombs possible and easy. "To have a plastic surgeon put in liquid explosion in an implant and teaching somebody how to detect it-it's unfathomable," Rose said. Travelers at Boston Logan Airport reacted with outrage and anxiety. "I guess it's surprising, but I guess it's not surprising that they're going to go to any lengths," one traveller said. Another person at Logan said it could indicate increased security measures need to be taken. "I think that we need to invest in full-body scan equipment at the airports. I think that would be the only helpful and the right thing to do," one man said.

Dickin Medal awarded to bomb sniffing search dog Treo

A search dog that sniffed out bombs in Afghanistan is to be honoured with the animal version of the Victoria Cross.

Princess Alexandra will award black Labrador Treo the Dickin Medal at the Imperial War Museum in London.

The now retired dog, from 104 Military Working Dog Support Unit, North Luffenham barracks in Rutland, twice found hidden bombs in Helmand province.

Treo will be the 63rd animal to receive the medal created by veterinary charity the PDSA to honour gallantry in war.

'Bravery in duty'

The eight-year-old dog will be joined by his handler, Sgt Dave Heyhoe, at the ceremony on 24 February. The pair have worked together for five years and Treo has now become a family pet. PDSA director general Jan McLoughlin said: "We look forward to honouring Treo with the PDSA Dickin Medal. "The medal is recognised throughout the world as the animals' Victoria Cross and is the highest

award any animal can receive for bravery in the line of duty. Treo is, without doubt, a worthy recipient." A total of 26 other dogs, 32 World War Two messenger pigeons, three horses and one cat have won the award, introduced by PDSA founder Maria Dickin in 1943.

Buried at the newly restored cemetery are some of the recipients of the PDSA Dickin Medal, the charity's animal equivalent of the Victoria Cross.

Beauty, owned by PDSA Supt Bill Barnett of the charity's wartime animal rescue squads, helped to dig out 63 pets during the London Blitz.

Sheila is the only non-military animal to have received the PDSA's Dickin Medal for bravery. She helped save the lives of four US airmen whose bomber crashed in a blizzard in 1944.

Rob the 'para dog' was recruited by the SAS for a series of undercover operations in Italy during the Second World War. He made more than 20 parachute descents.

Awards made between 2000 – to date

Gander – Newfoundland
Date of Award: awarded posthumously on 27 October 2000

"For saving the lives of Canadian infantrymen during the Battle of Lye Mun on Hong Kong Island in December 1941. On three documented occasions Gander, the Newfoundland mascot

of the Royal Rifles of Canada engaged the enemy as his regiment joined the Winnipeg Grenadiers, members of Battalion Headquarters 'C' Force and other Commonwealth troops in their courageous defence of the Island. Twice Gander's attacks halted the enemy's advance and protected groups of wounded soldiers. In a final act of bravery the war dog was killed in action gathering a grenade. Without Gander's intervention many more lives would have been lost in the assault."

Appollo – German Shepherd
Date of Award: 5 March 2002

NYPD dog Appollo received the PDSA Dickin Medal on behalf of all the Search and Rescue dogs at Ground Zero and the Pentagon following the terrorist attack on 11 September 2001. "For tireless courage in the service of humanity during the search and rescue operations in New York and Washington on and after 11 September 2001." Faithful to words of command and undaunted by the task, the dogs' work and unstinting devotion to duty stand as a testament to those lost or injured."

Appollo, an NYPD dog, was one of a number of dogs recognised for their role in the search and rescue operation of the World Trade Center following the September 11 attacks.

Salty and Roselle – Labrador Guide dogs
Date of Award: 5 March 2002

"For remaining loyally at the side of their blind owners, courageously leading them down more than 70 floors of the World Trade Center and to a place of safety following the terrorist attack on New York on 11 September 2001."

Sam – German Shepherd
Royal Army Veterinary Corps
Date of Award: 14 January 2003

"For outstanding gallantry in April 1998 while assigned to the Royal Canadian Regiment in Drvar during the conflict in Bosnia-Hertzegovina. On two documented occasions Sam displayed great courage and devotion to duty. On 18 April Sam successfully brought down an armed man threatening the lives of civilians and Service personnel. On 24 April, while guarding a compound harbouring Serbian refugees, Sam's determined approach held off rioters until reinforcements arrived.

This dog's true valour saved the lives of many servicemen and civilians during this time of human conflict."

Buster - Springer Spaniel
Royal Army Veterinary Corps
Date of Award: 9 December 2003

"For outstanding gallantry in March 2003 while assigned to the Duke of Wellington's Regiment in Safwan, Southern Iraq. Arms and explosives search dog Buster located an arsenal of weapons and explosives hidden behind a false wall in a property linked with an extremist group. Buster is considered responsible for saving the lives of service personnel and civilians. Following the find, all attacks ceased and shortly afterwards and troops replaced their steel helmets with berets."

Lucky: German Shepherd
RAF number 3610 AD: RAF Police anti-terrorist tracker dog – from 1949 to 1952 during the Malaya Campaign
Date of Award: 6 February 2007

"For the outstanding gallantry and devotion to duty of the RAF Police anti-terrorist tracker dog team, comprising Bobbie, Jasper, Lassie and Lucky, while attached to the Civil Police and several British Army regiments including the Coldstream Guards, 2nd Battalion Royal Scots Guards and the Ghurkhas during the Malaya Campaign. Bobbie, Jasper, Lassie and Lucky displayed exceptional determination and life-saving skills during the Malaya Campaign. The dogs and their handlers were an exceptional team, capable of tracking and locating the enemy by scent despite unrelenting heat and an almost impregnable jungle. Sadly, three of the dogs lost their lives in the line of duty: only Lucky survived to the end of the conflict."

Sadie: Labrador
RAVC arms and explosive search dog – Kabul, Afghanistan in November 2005
Date of Award: 6 February 2007

"For outstanding gallantry and devotion to duty while assigned to the Royal Gloucestershire, Berkshire and Wiltshire Light Infantry during conflict in Afghanistan in 2005. On 14 November 2005 military personnel serving with NATO's International Security Assistance Force in Kabul were involved in two separate attacks. Sadie and Lance Corporal Yardley were deployed to search for secondary explosive devices. Sadie gave a positive indication near a concrete blast wall and multinational personnel were moved to a safe distance. Despite the obvious danger Sadie and Lance Corporal Yardley completed their search. At the site of Sadie's indication, bomb disposal operators later made safe an explosive device. The bomb was designed to inflict maximum injury. Sadie's actions undoubtedly saved the lives of many civilians and soldiers."

Bomb sniffing dogs are super stars of anti-terrorism efforts at Super Bowl 44

Darel takes a break to pose for publicity photo Courtesy ATF

All the technology, the intelligence gathering gadgets, the James Bond-like tools, nothing law enforcement will ever develop can compare to the natural crime fighting gifts of a dog. Teams of trained dogs are running interference to prevent any would be terrorists or criminal lunatics from planting explosives in or near the Sun Life Stadium in Miami this Super Bowl Sunday. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) says in a press release the best K-9 explosive detection teams from across the country have been working in Miami for several weeks and will continue working throughout the big game. ATF is just one of 50 law enforcement agencies teamed together for Super Bowl security this year and the dogs the agency has brought in are considered "the best of the best," says Special Agent in Charge, Hugo Barrera. The ATF only uses Labrador Retrievers in its K-9 program. Besides their exceptional sniffing abilities, the labs are not as intimidating when agents bring the animals into large crowds. The Guiding Eyes for the Blind, the Guide Dog Foundation and Canine Companions for Independence supply the dogs to the agency. The dogs and their handlers undergo an initial 10 week training course at a facility in Front Royal, Virginia, according to the ATF. Training is ongoing throughout the dogs' crime-fighting careers. Besides explosive materials, the dogs are also trained to sniff out firearms and ammunition. Below is a photo array and some information on the ATF K-9 teams involved in this year's Super Bowl security effort.

Ethics of medicalized weapons questioned

A new report raises questions as to the ethics of so-called medicalized weapons, which are biological weapons meant to incapacitate rather than kill, and the implications of medical personnel designing, manufacturing and testing such weapons. The latest issue of the Hastings Center Report takes aim at these new battlefield weapons, which could make fighting insurgents an easier proposition. Medicalized weapons are nonlethal and rely on recent advances in neuroscience, physiology and pharmacology. The goal of a medicalized weapon is to reduce casualties, especially in the case of so-called asymmetric wars wherein nations are fighting insurgent forces. "Not since international law prohibited the development and use of biological and chemical weapons (in 1972 and 1993, respectively) have medical personnel been so directly involved with the design, manufacture, and testing of a weapon," Michael L. Gross, a professor of political science and chair of the Division of International Relations at the University of Haifa, Israel, writes. "Rather than disabling or killing enemy forces by causing traumatic injury, nonlethal weapons temporarily incapacitate their targets by causing physical distress, disorientation, or unconsciousness." Gross argues that even though the principles of medical ethics require that practitioners do no harm, these new types of biological weapons, in the long run, will reduce casualties and protect civilians while causing only temporary harm.

Medicalized Weapons and Modern War

Asymmetric warfare is creating a new frontier for bioethics as military organizations rush to develop nonlethal, medicalized weapons. Faced with small but increasingly sophisticated guerrilla organizations that intermingle at will with the civilian population, the United States and many of its allies are searching for ways to disable insurgents while minimizing harm to civilians. One avenue is to build increasingly sophisticated "precision-guided munitions"—"smart," high-explosive bombs that, in theory, zero in on and destroy their targets without widespread collateral damage. However, these weapons—the purview of electronics and ballistic experts—can only go so far. Very often, there are no clearly defined guerrilla targets, or, as often happens, the targets are destroyed early on. Nonlethal weapons are an increasingly attractive option for rooting out insurgents without bringing catastrophic harm to civilians. Rather than disabling or killing enemy forces by causing traumatic injury, nonlethal weapons temporarily incapacitate their targets by causing physical distress, disorientation, or unconsciousness. These weapons are "medicalized" in that they rely on advances in neuroscience, physiology, and pharmacology and on the active participation of physicians and other medical workers. Not since international law prohibited the development and use of biological and chemical weapons (in 1972 and 1993, respectively) have medical personnel been so directly involved with the design, manufacture, and testing of a weapon. But medicalized weapons place medical practitioners in a bind. Ordinarily trained to relieve pain and suffering, they now face calls to help build weapons that cause some measure of harm, even if nonlethal and transient. Do the principles of medical ethics—particularly the axiom "do no harm"—permit medical personnel to build nonlethal weapons? Asymmetric warfare is creating a new frontier for bioethics as military organizations rush to develop nonlethal, medicalized weapons. Faced with small but increasingly sophisticated guerrilla organizations that intermingle at will with the civilian population, the United States and many of its allies are searching for ways to disable insurgents while minimizing harm to civilians. One avenue is to build increasingly sophisticated "precision-guided munitions"—"smart," high-explosive bombs that, in theory, zero in on and destroy their targets without widespread collateral damage. However, these weapons—the purview of electronics and ballistic experts—can only go so far. Very often, there are no clearly defined guerrilla targets, or, as often happens, the targets are destroyed early on. Nonlethal weapons are an increasingly attractive option for rooting out insurgents without bringing catastrophic harm to civilians. Rather than disabling or killing enemy forces by causing traumatic injury, nonlethal weapons temporarily incapacitate their targets by causing physical distress, disorientation, or unconsciousness. These weapons are "medicalized" in that they rely on advances in neuroscience, physiology, and pharmacology and on the active participation of physicians and other medical workers. Not since international law prohibited the development and use of biological and chemical weapons (in 1972 and 1993, respectively) have medical personnel been so directly involved with the design, manufacture, and testing of a weapon. But medicalized weapons place medical practitioners in a bind. Ordinarily trained to relieve pain and suffering, they now face calls to help build weapons that cause some measure of harm, even if nonlethal and transient. Do the principles of medical ethics—particularly the axiom "do no harm"—permit medical personnel to build nonlethal weapons?

Michael Gross, "Medicalized Weapons and Modern War," Hastings Center Report 40, no 1 (2010): 34-43.

New virtual community to connect bioterrorism experts

The Delaney Center at Mount St. Mary's University has launched a new virtual community that allows intelligence officers, students and even Capitol Hill executives to network with

bioterrorism experts, bodyguards and academics. "It's a great way for students to learn from accomplished experts - people they might never have a chance to meet otherwise," Joe Vince, Delaney Center Director, said. "For professionals, it's a secure way to exchange ideas with colleagues in other disciplines." This new, invitation-only network, which takes place on the Yakabox knowledge sharing systems certified for use in classified environments by the U.S. Government, is an outgrowth of Mount St. Mary's criminal justice program. "It's knowledge transfer at its best, working in both directions," Jeff Sutterman, a Yakabox Customer Advocate, said. "Students caught on to the technology immediately. They led the way for the rest of the group." The Delaney Center Yakabox uses the same security standards as those deployed in the U.S. intelligence community. Mount St. Mary's students have praised the new network, noting that it has more depth than typical social networking tools and allows them to more confidently enter the professional world. "Collaboration fluency really isn't an option anymore," Chris Vince said. "It's rapidly becoming a requirement for intelligence officers, regardless of specialty or years in service. New clue to Georgi Markov umbrella assassin as police see Cold War files. The murder of a Cold War dissident in London with a poisoned umbrella could finally be solved. In a major breakthrough, Scotland Yard officers examined

secret files in Bulgaria about the 1978 assassination of opposition activist Georgi Markov. Counter-terrorism detectives spent two weeks in Sofia sifting through the communist-era archives. They recently returned to discuss other evidence with Bulgarian officials. It has raised new hope that charges could be brought over one of the Cold War's most high-profile unsolved mysteries. Markov, 49, who worked for the BBC and had lived in London since defecting to the West in 1969, was waiting for a bus on Waterloo Bridge in September 1978. He felt a pain and turned to see a man pick up an umbrella and walk off. He died in hospital four days later and a postmortem found a tiny metal pellet laced with deadly ricin in his leg. The case was reopened when Bulgaria applied for EU membership. One Met insider said: "There is still a way to go but we are getting co-operation from Bulgaria and hope to make more progress soon." Already, the files suggest the hit was arranged for £ 50,000. The prime suspect has always been Francesco Gullino, a Dane of Italian origin codenamed Agent Piccadilly. He left Denmark in 1993 but is thought to be still alive. Another key figure is former Bulgarian intelligence chief General Vladimir Todorov.

Colorado Releases Video Describing the 8 Signs of Terrorism

In an effort to educate and increase ordinary citizens' awareness of terrorism planning, the

state of Colorado, its fusion center, and the Denver-based nonprofit Center for Empowered Living and Learning (CELL) have co-produced a video exploring suspicious activities that may indicate terrorist planning. The video was released yesterday by Colorado Gov. Bill Ritter after giving a tour of the CELL, an antiterrorism education center, to Homeland Security chief Janet Napolitano. The film was financed by a $30,400 grant from the Department of Homeland Security (DHS), reported 9News.com. "Eight years after 9/11, it's important to remember that the United States is not immune from terror attacks," Ritter said. "The video will help empower citizens with the knowledge they need to protect our communities, our state, our nation." “The vigilance of individual citizens is critical to protecting our country from the threat of terrorism,” said Napolitano. “This video provides essential information on how to identify the warning signs and emphasizes the vital role of such assistance in state and

local law enforcement's counterterrorism efforts." The eight minute video, "Recognizing 8 Signs of Terrorism," is narrated by Hall of Fame Denver Broncos quarterback John Elway and local news anchor Kim Christiansen. In the opening of the video, Elway explains to viewers that terrorism "can happen anytime, anywhere" as news footage of terrorist attacks of 9-11 and Oklahoma City roll across the screen.

This segues to Christiansen, who lists the eight signs indicate terrorism planning.

- Surveillance
- Elicitation (or trying to get information out of people close to a target)
- Tests of Security
- Funding
- Acquiring Supplies
- Impersonation (e.g. government personnel like mail carriers or company employees)
- Rehearsal
- Deployment

"When you witness any suspicious activities, you should report them to the Colorado Information Analysis Center," Elway says, referring to Colorado's fusion center. That is unless you believe the suspicious activities mean an attack is imminent. If so, contact 911, Christiansen says. The film comes just weeks after federal authorities with the help of state and local Colorado law enforcement arrested Najibullah Zazi, a Denver shuttle bus driver believed to have been planning a terrorist attack against New York City. One of the suspicious activities Zazi engaged in before his arrest was buying hydrogen peroxide and acetone from beauty supply stores around the Denver area.

EMS and Terrorism

Author: Everett Stephens, MD, Assistant Clinical Professor, Department of Emergency Medicine, University of Louisville

Introduction

Although present in various forms and locations for countless years, terrorism has increasingly been the focus of public concern. Emergency Medical Services (EMS) plays a vital role in responding to, evaluating, and intervening in potentially catastrophic events. EMS often co-manages initial scenes in many medium- to large-scale incidents involving large numbers of casualties. EMS may also manage the scene until state or federal agencies arrive. Americans will never forget the tragic events of September 11, 2001. More than 3350 people were killed, and more than 10,000 people were injured in an incredibly complicated and choreographed attack. However, not all remember the WorldTradeCenter bombing in 1993 that killed 6 people and injured more than 1000. In April 1995, the federal building in Oklahoma City was bombed, killing 168 people. A pipe bomb was detonated in CentennialPark during the 1996 Olympic Games in Atlanta, Georgia, killing 2 people and wounding 110. The bombing of 4 commuter trains in March 2004 claimed the lives of 190 and injured more than 1800 people in Madrid, Spain. Such events emphasize the potential loss of life and property caused by terrorist activities. Many authorities consider the United States a continuing high-profile target. For all Americans, the attack on the WorldTradeCenter on September 11, 2001, brought home the tragic realization that America is not immune to terrorism. Philip Stern, an expert on terrorism with the Fairfax Group, said, "As an open society and a democracy, this country is particularly vulnerable. We have free passage, coast-to-coast, anyone can apply for a visa to visit and the population is enormous and diversified." Such an inviting atmosphere and free society may make terrorist activity inevitable. Many of the terrorist groups of today appear more and more willing to use weapons of mass destruction. Perhaps even more disturbing is the potential for terrorists to utilize more technologically advanced weapons and communications. Access to the Internet and information on the World Wide Web facilitates tremendous technological advancement in destructive potential. All of these issues underscore the importance of proper education in

EMS and advance planning. Terrorist activity may have various mechanisms, including chemical or biological weapons and explosives, as well as new and unanticipated methods of destruction. Full response to a terrorist incident requires in-depth interagency planning involving police; fire; EMS; regional, state, and national emergency organizations; as well as a wide array of ancillary community services. Each agency should be assigned respective roles as soon as possible, well in advance of potential terrorist acts. For related information, see Medscape's Disaster Preparedness and Aftermath Resource Center.

Aspects of Terrorism

Weapons of mass destruction (WMD) hold great attraction to terrorists: they have great potential to create fear, both in victims and in the public at large; can be created inexpensively; may be difficult to detect even when being sought; and can be engineered for a delayed onset of symptoms—nerve agents within minutes, vesicants within hours, and biological agents within days. Protecting large populations from exposure to WMD is problematic at best and impossible at worst. The drawbacks of WMD use are largely ignored by terrorists: contempt for users, retaliation, and prohibition treaties are not priorities for terrorist organizations. Deployment dangers, including injury or even death of deploying persons, are rarely considered risks sufficient to prevent use. Determining the actual extent of the terrorist threat in the United States is difficult, as it is poorly defined and rapidly changing. James Alan Fox, Dean of Northeastern University's Criminal Justice Program in Boston, believes the 2 current motivations for terrorism are revenge and attention. Either motivation can be justification for exposing large numbers of the populace to a wide variety of dangerous or deadly toxins. The Morbidity and Mortality Weekly Report, April 21, 2000 states "The public health infrastructure must be prepared to prevent illness and injury that would result from biological and chemical terrorism, especially a covert terrorist attack. As with emerging infectious diseases, early detection and control of biological and chemical attacks depends on a strong and flexible public health system at the local, state, and federal levels."

Preplanning

Effective response to a terrorist incident hinges on comprehensive planning and interagency cooperation. Agencies must address and resolve jurisdictional issues well in advance. After a plan has been devised, it must be updated regularly to reflect changes in resources, population, terrorist activities, or potential targets. Local police, fire, EMS, and Disaster & Emergency Services (DES) agencies should form the first line of response. Other agencies that may be included are as follows:

- Secret Service
- Bureau of Alcohol, Tobacco, and Firearms (BATF)
- State disaster agencies
- Military or reserve units, including National Guard
- Specialized medical units

Depending on the circumstances, state or federal response agencies, such as the Emergency Broadcast System, Federal Aviation Administration, or National Weather Service, may need to become involved. The Federal Bureau of Investigation (FBI) has been designated as lead agency in crisis management response, and Federal Emergency Management Agency (FEMA) is designated as lead agency in consequence management response. The Defense Against Weapons of Mass Destruction Act (Nunn-Lugar-Domenici Bill) of 1996 required the Secretary of Defense to establish a program to advise and train federal, state, and local officials until 1999 and allows the President or Attorney General to request military support for local authorities in chemical/biological incidents. An act of terrorism in a metropolitan area may cause major health and medical consequences that could easily overwhelm all local health facilities; thus, ongoing contact with state and national agencies is recommended for the additional resources they can provide. The FBI is the federally designated lead agency in a confirmed domestic terrorist event. Depending on location, however, some federal agencies

may not be on-site for 24 hours or more. On a national level, the US Government has established the National Disaster Medical System (NDMS). This organization assists in providing medical care and transportation for disaster victims. The NDMS comprises sections of the Department of Health and Human Resources, the Department of Veterans Affairs, the Department of Defense, and the FEMA. Any state can enlist the services of NDMS, which provides assistance at the disaster site, evacuates patients, and finds beds for evacuated patients. Congress also has established a Domestic Preparedness Program that provides enhanced training for local first responders and forms metropolitan medical strike teams in major cities. In evaluating sites of potential terrorist activity, the release of chemical or biological agents into crowded and contained areas, such as sports stadiums, office or public buildings, and transportation systems (eg, the Tokyo subway Sarin incident) should be considered. Such places provide tempting targets despite on-site security. Rapid identification of the chemical or biological agent is critical to proper disposition of patients and to management of affected areas. Disasters involving hazardous materials (HAZMATs), radioactive materials, or chemical agents may produce unfamiliar medical problems that cannot be identified rapidly in the readily available emergency medicine literature. All possible resources should be used early in the incident to ensure proper identification of the agent and prompt initiation of proper protocols.

Incident Management

Most of the principles of terrorist incident management are similar to the principles in the management of mass casualty incidents. The primary concern in potential terrorist incidents is to secure the area and to ascertain the severity and the nature of the threat. Delayed explosives or materials intended to harm rescue workers may have been planted at the site. A safe scene must be obtained to avoid further endangering survivors and health care workers. Primary and secondary perimeters must be established and secured. It should also be determined if a cleared, downwind perimeter is needed, and one should be established if required. The Acronym ASBESTOS can be used to remember the important aspects of exposure:

A - Agent(s) - Type and amount of doses
S - State - Liquid, solids, or aerosolized
B - Body sites - Areas of exposure, lungs, skin, or other
E - Effects - Area of effects; local or systemic
S - Severity, of symptoms
T - Timing of events
O - Other diagnoses to consider
S - Synergism - Interaction between multiple agents or coexisting disease

Early involvement of support and ancillary services, mutual aid agencies, and local agencies in the planning process is prudent. After identifying the potential threat, it should be determined which type of protective equipment is necessary. Emphasis must be placed on protection and decontamination of rescuers and victims. After establishing a decontamination and triage area, rescuers should put on appropriate protective clothing before entering the affected area and beginning rescue efforts. The first focus is on supportive care with emphasis on aggressive airway control and decontamination. Issues associated with simultaneous containment, neutralization, and/or decontamination may be addressed by ancillary agencies. Following initial triage, patients are given primary or aggressive aid depending on their presentation and the resources available. The patients should be decontaminated and transported to a facility that has been informed about the etiology of the incident as soon as feasible. A secure and clean area completes the physical response. Record keeping, analysis of the incident, and investigations conclude the complete response.

Selected Agents of Terrorism: Conventional Explosives

While lacking the cachet of nuclear, biological, or chemical weapons, conventional explosives are more likely to be the instrument of a terrorist attack. Ease of obtaining materials and knowledge make conventional explosives more likely a vehicle than other, more difficult to obtain or manufacture agents. Historical analysis consistently demonstrates that the most likely terrorist weapon causing a mass casualty event is a standard explosive device detonated in a crowded area.. An explosive is a normally stable material that, when introduced into a chemical reaction, converts rapidly from a solid or a liquid to an expanding gas. Explosives cause damage primarily through tremendous increases in atmospheric pressure. The initial shock, called the positive pressure wave, is the almost instantaneous increase of pressure from a blast, and the negative pressure wave immediately follows, as the displaced air rushes in to fill the void caused by the initial pressure wave. Explosives are categorized as either low grade or high grade. Low-grade explosives burn rapidly. Black powder, the original low-grade explosive, served as the basis for the development of smokeless gunpowder and some rocket propellants. Other examples of low-grade explosives are nitrostarch, nitrocellulose, and commercial fireworks. High-grade explosives, also termed detonating explosives, are more stable than low-grade explosives, frequently requiring trauma or shock for detonation. Nitroglycerin is the original high-grade explosive. Ammonium nitrate is another example of the early types of detonating explosives. Composition B, C-3, C-4, and TNT were developed later. Other examples include Amatol 80/20, RDX, PETN, and dynamite. Initiating high-grade explosives are a separate class of very sensitive high-grade explosives, such as lead styphnate and lead azide. Explosions in confined spaces are often associated with much higher mortality. Solid surfaces act to reflect and compound the shock waves, causing magnification of the destructive forces. Similarly, blasts that are channeled by alleyways or hallways can have profound impact far outside the normal blast radius because the forces are focused on a smaller area of effect. Blast injuries can often be categorized as primary, secondary, or tertiary. Primary blast damage is seen as a result of the tremendous pressure changes associated with explosives, in particular high explosives. Bowel, nervous system, cardiovascular system, ears, and lungs are most often affected by the primary blast. Cardiac contusion, esophageal rupture, hemothoraces or pneumothoraces, perforated bowel, arterial gas embolism, or immediate or delayed GI injuries should be suspected as clinically indicated. Burns are also possible, depending on the proximity to the blast. Secondary blast injuries occur when victims are struck with shrapnel or objects sent airborne during the primary blast. Shrapnel can be the result of environmental objects as innocuous as sticks or rocks, or as malevolent as screws and nuts packed within the primary explosive. Tertiary blast injuries occur when victims themselves are thrown due to the incredible pressures from the blast. These injuries can include a wide variety of traumatic etiologies similar to a fall of significant magnitude. "Suicide bombers" often carry a small amount (5-40 lb) of high explosives with an associated detonating device in a clandestine manner seeking to detonate the explosives near a large group of victims. Typical sites include sporting events, restaurants, nightclubs, or other public functions. Shrapnel can serve to extend the injury area, and a suspicion for projectile injuries should be maintained. Extreme care should be exercised in approaching a potential suicide bomber, even if incapacitated. Suspected perpetrators should be evaluated by experienced bomb squad personnel before EMS intervention to ensure a safe environment.

Selected Agents of Terrorism: Chemical Agents

Chemical agents were first used extensively in World War I with dramatic results against unprepared troops. Although far less lethal than conventional explosives, chemical weapons can affect and incapacitate large numbers of troops in a short time. Chemical warfare agents were defined by the United Nations in 1969 as "chemical substances, whether gaseous, liquid or solid, which may be employed because of their direct toxic effects on man, animals, or plants." The ready availability of precursors of modern chemical weapons and copious documentation on their preparation make the use of chemical weapons for terrorist actions far

more likely than use of nuclear or biological weapons. In addition, potential terrorists could easily locate a chemical production facility, sabotage it using chemical or conventional explosives, and allow ambient winds to spread the toxins. The resultant environmental contamination would fulfill many terrorists' objectives of generating fear, trepidation, and panic among the population. Chemical agents are separated into 2 broad categories: lethal and nonlethal. Lethal agents include cyanides, nerve agents, vesicants, and choking agents. Nonlethal agents include lacrimating, emesis-inducing, and incapacitating agents.

Lethal chemical agents

Cyanide compounds

Although they have been used since World War I, cyanide compounds are highly volatile, rendering them less useful than chlorine. The military designates hydrogen cyanide (AC) and cyanogen chloride (CK) as the substances used in warfare. Cyanide and its compounds are among the most rapidly acting chemical agents. Cyanide may be one of the most likely asphyxiant agents used in a terrorist action. Signs and symptoms include air hunger, hyperpnea, apnea, seizures, coma, and death. Cyanide poisoning is treated with a combination of nitrites and thiosulfates. A commercial kit is available, called a Cyanokit. Protective masks, gowns, and gloves are necessary until the patient is completely decontaminated.

Nerve agents

Nerve agents are chemicals that inhibit acetylcholinesterase irreversibly. They combine with acetylcholine (ACH) to prevent transmission at the neuromuscular junction and affect both the sympathetic and parasympathetic nervous systems. Salivation, lacrimation, urination, defecation, and emesis (SLUDGE) are common signs. Muscarinic effects may cause the most serious complications, including bronchoconstriction, laryngospasm, and respiratory depression or arrest. These nerve agents may be delivered by droplet, vapor, or both. Symptoms of skin exposure appear much more slowly than those from inhalation. Onset of symptoms varies from 1 minute to a few hours. If cyanide compounds are inhaled or absorbed through the mucus membranes, death can occur in 1-10 minutes. Therapy includes atropine sulfate, with as much as 10-40 mg required in some instances. Currently, the US Army uses 2-PAM (pralidoxime chloride), although it is not completely effective. It is least effective against Soman (GD). Pretreatment with pyridostigmine competitively inhibits the nerve agent. Pyridostigmine combines reversibly with ACH, which can resume neurotransmission after disassociation. However, such pretreatment does not protect against seizures. Current nerve agents include tabun (GA), sarin (GB), soman (GD), and VX. These more potent agents may be the most likely nerve agents to be used in terrorism. Exposure to these agents can cause dramatic and sudden symptoms, especially when vapors or aerosolized agents are used. Transdermal exposure can produce delayed symptoms, as can exposure to limited amounts of either aerosolized or liquid agents. Local decontamination of these agents includes washing with soap and water. Health care providers should wear full protective gear until the patient is cleared by an environmental health specialist. VX, considered the most toxic of the nerve agents, is also the most difficult to decontaminate because of its low volatility.

Choking agents

Causing pronounced irritation to the upper and lower respiratory tracts, these agents are potentially dangerous because of a period of latency. A victim with dyspnea and mild chest discomfort may deteriorate after several hours to apnea and subsequent death. Chlorine is a widely used chemical that falls into the choking agent class. Chlorine causes upper- and lower-respiratory irritation, lacrimation, chest pain, dyspnea, coughing, laryngeal edema, pulmonary damage, and pulmonary edema. Treatment is symptomatic with nebulized sodium bicarbonate. Decontaminate by copious flushing of affected areas with water. Medical providers need no special protection from chlorine-exposed patients.

Vesicant agents

Vesicant agents, also termed blistering agents, may be toxic to the lungs, eyes, and mucous membranes. They are named for their tendency to cause blisters. Mustard gas is the best-known vesicant, originally used in World War I. It is a primary tissue irritant and has no significant allergenic component. Lesions are primarily cutaneous, but respiratory, ocular, and GI manifestations may occur, as well as cough, bloody sputum, and dyspnea. Areas of exposure become erythematous and progress to bullae, similar to toxic epidermal necrolysis. Symptoms may not occur for several hours after exposure. No antidote is available. Other vesicants include sulfur mustard (HD), nitrogen mustard (HN), agent T, and phosgene oxime (CX). Lewisite, unlike mustard and mustard derivatives, causes immediate pain and skin irritation. Medical providers require protective masks and clothing for patient management. They should decontaminate by blotting and cleansing with soap and water and avoid scrubbing and hot water.

Nonlethal chemical agents

Lacrimator agents

Lacrimator agents (tear gases) are widely used by law enforcement and the military. The most common effects are nasal and ocular discharges, photophobia, and burning sensations in the mucous membranes. Prolonged exposure may produce tightness in the chest, shortness of breath, and malaise and may cause vesiculations or bullae. Physical injuries may be observed from explosive discharge or kinetic effects of projectiles. At least 1 death has been attributed to lacrimator agents. Most patients can be decontaminated fully by undressing, showering, and washing with soap and water. Medical personnel should use protective masks, gowns, and gloves, since lacrimator agents are transmitted by physical contact. Types of lacrimator agents include bromobenzyl cyanide (CA), ortho-chlorobenzylidenemalonitrile (CS), dibenzoxazepine (CR), 2-chloroacetophenone (CN), chloroacetophenone in chloroform (CNC), and chloroacetophenone and chloropicrin in chloroform (CNS).

Emesis-inducing agents

Emesis agents, also termed nausea gases, are not used routinely in the United States. They produce respiratory and skin irritation effects similar to those of lacrimator agents, as well as profound nausea. Examples of such compounds include adamsite (DM), diphenylcyanoarsine (DC), and diphenylchloroarsine (DA). No decontamination is required in the field, and diluted bleach solution has proven effective for definitive cleaning. Ordinary clothing protects against these agents; chemical insert masks and standard gloves are adequate.

Incapacitating agents

The possibility of a nonlethal incapacitating agent has long intrigued military commanders. Several agents have been tested, including lysergic acid diethylamide (LSD), mescaline, psilocybin, and psilocin. The only successful agent in production is benzilate (BZ). BZ is a delayed-onset (1-4 h) agent causing tachycardia, dizziness, vomiting, blurred vision, stupor, confusion, and random activity. Affected persons may be docile, belligerent, stuporous, or confused. They may appear intoxicated. Decontaminate by washing with soap and water or with dilute bleach solution. Protective masks with charcoal filters provide adequate protection. Gloves are not necessary, since the agent is not absorbed through the skin.

Selected Agents of Terrorism: Biological Agents

The Biological and Toxin Weapons Convention of 1972 banned the development, production, and stockpiling of biological weapons not required for peaceful intentions. The United States, United Kingdom, Soviet Union, and 67 other nations signed this document. Despite the fact that no biological agents have been used officially in warfare to date, the prospect of their use raises many concerns. Terrorism's history suggests the potential for the use of biological agents. Many authorities fear the use of biological agents more than the use of chemical agents because antidotes and specific countermeasures are available for some chemical weapons. Use of biological agents in terrorist acts potentially could cause tens of thousands of

casualties and cost the US economy billions of dollars. Various scenarios involving use of biological weapons are possible, from a sudden epidemic to a subacute, prolonged pandemic. Pathogens might be disseminated without anyone's realizing it until after the incubation period ends, by then exposing hundreds or thousands of civilians. Anticipating and controlling the dissemination of biological weapons may be difficult, causing complications for terrorists and intended victims. The effects of a biological agent also could evolve as a slowly developing, hard-to-categorize cluster of widely scattered cases, inadvertently allowing further dissemination of the pathogen until the connection is recognized. Certain aspects of a disease outbreak may combine to prompt suspicion of terrorist activity, including temporal patterns of illness, selected populations of victims, clinical presentation of illness, certain strains or species of pathogens, geographic location, morbidity or mortality patterns, antimicrobial resistance patterns, residual infectivity, route of exposure, weather or climate conditions, incubation period, or concurrence with other terrorist activities. **Biological agents could prove to be a devastating vector; a release of only 30 kg of anthrax spores could cause as many as 30,000-100,000 deaths; in comparison a 1,000-kg atomic bomb would result in approximately 23,000-80,000 deaths.** The number of potential biological agents is nearly impossible to estimate. Agents range from simple viruses to bacteria and compounds derived from vertebrate animals. Biological agents are classified into 2 broad groups: infectious and noninfectious.

Infectious agents

This group includes viruses, bacteria, protozoa, and fungi. The list of potential pathogens is extremely long, although an abbreviated list of agents can be considered that is based on previous use as agents during wartime. The synopsis presented for each disease is meant only as an overview. Consult definitive texts for complete information.

Anthrax

Bacillus anthracis, the causative organism of anthrax occurs naturally, is relatively easy to access, is very durable; it may live for up to 50 years in soil. Even a small number of anthrax spores, enough to fit on the head of a pin (5,000-8,000 spores), is sufficient to cause the inhalational form of anthrax. The inhalational form of anthrax can be difficult to diagnose in the earliest stages and may be very difficult to treat once clinical signs become apparent. Cutaneous clues are necrotic lesions that spontaneously heal, and inhalation can produce a 1- to 3-day incubation period with fever, dyspnea, necrotizing hemorrhagic mediastinitis, and hypotension leading to death. Death usually occurs in 24-36 hours but may be as long as 7 days. Mortality can reach as high as 95% of inhalational exposures. Standard precautions, including masks, gowns, gloves, and isolation are sufficient. Vaccine is available.

Brucellosis

Highly infectious Brucella species are less commonly fatal than anthrax. Fever, malaise, osteomyelitis, and genitourinary (GU) infections may occur. Endocarditis is typically the cause of death. Standard precautions are sufficient. Precautions against direct contact should be included if draining lesions are present.

Encephalitis viruses

Venezuelan, Eastern, and Western equine encephalitis viruses are likely to be used in weapons. Fever, headache, confusion, obtundation, dysphasia, seizures, paresis, and death may be observed. The Eastern variety has the highest mortality rate at 50-75%. A vaccine for Venezuelan equine encephalitis (VEE) is available, and effective vaccines for the others are currently in development. Standard precautions are sufficient; however, mosquito control is suggested, since mosquitoes are a vector.

Clostridium botulinum
An epidemic of descending and progressive bulbar and skeletal paralysis in afebrile patients may suggest botulinum poisoning. Respiratory failure is the most frequent cause of death. Since an antitoxin is available, standard precautions are sufficient.

Yersinia pestis (plague)
Plague usually manifests as pneumonia, culminating in respiratory failure and shock. A vaccine is available, yet precautions are required against pulmonary and droplet exposure.

Coxiella burnetii (Q fever)
A zoonotic disease with domestic livestock as vectors, Q fever varies in its manifestations. Fever, chills, and headache are the most common symptoms, although malaise, diaphoresis, and myalgia often are observed. Mortality rate is low, even when the disease is untreated. A vaccine is under investigation. Standard precautions are sufficient.

Rift valley fever
A hemorrhagic virus infection, Rift valley fever manifests with symptoms such as malaise, fever, prostration, generalized vascular permeability, and abnormal circulatory regulation. Several different varieties of hemorrhagic viruses are documented, including Ebola. Most are highly infectious and cause morbidity. Some carry high mortality rates. Depending on the strain, a vaccine may be available. Precautions against direct contact are recommended. Additional precautions may be necessary if massive hemorrhage is present.

Smallpox virus
Smallpox may be a viable biological weapon, since the last natural case occurred in 1977 and the smallpox vaccine no longer is produced. Aerosol exposure causes viremia, malaise, fever, headache, delirium, and prolonged rash. Morbidity is caused primarily by secondary bacterial pneumonia. Precautions against aerosol infection are necessary.

Francisella tularensis (tularemia)
Tularemia, a zoonotic disease, occurs in ulceroglandular or typhoidal form. Typhoidal form manifests as fever, prostration, and respiratory symptoms. Mortality rate in typhoidal tularemia is approximately 35%. Standard precautions are sufficient. A vaccine is available as an investigational drug.

Noninfectious agents
Allergic agents come from a variety of sources, including mite and insect particles, feathers, epithelium, hair, urine, feces, and powdered enzymes. Problems caused by these agents may include respiratory symptoms, conjunctivitis, and/or dermatitis.

Conclusion
Responding to a terrorist event can represent a considerable drain on resources for all agencies involved. The potential for death and destruction is tremendous. Agencies responsible for responding to terrorist events can only ensure that appropriate preparations are in place should unforeseen circumstances arise. Extensive preplanning and interagency cooperation is essential in mitigating the effects of terrorist attacks. A prepared and determined populace makes a less inviting target for potential terrorists.

Hazmat

One of the most challenging aspects of providing emergency medical care is attending to patients who have been contaminated with hazardous materials. HAZMAT is a term used to describe incidents involving hazardous materials or specialized teams who deal with these incidents. Hazardous materials are defined as substances that have the potential to harm a

person or the environment upon contact. These can be gases, liquids, or solids and include radioactive and chemical materials. Biological organisms, such as viruses and bacteria, are not included as hazardous materials in this article. Most hospitals in the United States lack plans or facilities for attending to patients exposed to hazardous materials, even though this can be a common problem in some areas. Recent terrorist activities in the United States, Japan, Europe, and Asia highlight the need for hospital preparedness. Federal statutes require hospitals to participate in the planning and care of persons exposed to hazardous materials and to train and provide protection for employees who may be exposed while providing medical care. The potential for exposure to hazardous materials in the United States is significant. More than 60,000 chemicals are produced annually in the United States, of which the US Department of Transportation (DOT) considers approximately 2000 hazardous. More than 4 billion tons of chemicals are transported yearly by surface, air, or water routes. These shipments are initiated from more than 100,000 different locations, with more than 1 million people directly involved in the transportation process. More than 500,000 shipments of hazardous materials are made every day, totaling approximately 1.5 billion tons per year. The incidence of hazardous materials exposures cannot be ascertained accurately because a national reporting system does not exist. In an attempt to better define the magnitude of this problem, the Agency for Toxic Substances Disease Registry developed the Hazardous Substances Emergency Events Surveillance (HSEES) system in 1990. Fifteen state health departments participate in the reporting system. **In these states, the system has shown the following findings:**

- About 9000 releases of hazardous substances occur annually, with 75% occurring at chemical facilities and 25% occurring during transportation.
- Most transportation-related incidents occurred during ground transport (85%) and 26% occurred in residential areas.
- Human error and equipment failure account for most releases.
- The most common substances involved were inorganic substances (24%) followed by volatile organic compounds (20%).
- More than 2000 people are victims of hazardous materials releases in these states each year. Approximately 50% of these are transported to hospitals. Respiratory and eye irritation are the most common types of injury. Over a 4-year period, 132 hazardous material–related deaths occurred.
- More than 7500 people required decontamination during HAZMAT events over a 4-year period in these states. Of these, 2643 were decontaminated at medical facilities.

Several important points can be drawn from the above statistics. Most importantly, this is not a rare problem. Cities, prehospital-care providers, and hospitals need to have plans for dealing with these incidents and caring for victims of hazardous material exposures. Because most incidents occur at fixed sites, knowing the industries that operate in the catchment area of a hospital and the chemicals used or stored at those sites is imperative. Trauma centers need to have a plan to care for trauma patients who are contaminated because 25% of the incidents occurred during transportation and 9% of victims of hazardous materials exposure also had traumatic injuries.

Hospital and Community Planning for Hazmat Incidents

There are requirements by several different federal agencies, as well as the Joint Commission for Accreditation of Healthcare Organizations (JCAHO), for hospitals to participate in community planning for HAZMAT incidents. The most important federal statute that hospitals must be familiar with is SARA Title III, a portion of the Superfund Amendments and Reauthorization Act, otherwise known as the Emergency Planning and Community Right to Know Law. SARA Title III states that facilities manufacturing or storing hazardous chemicals must report inventories and every hazardous material release to public officials and emergency health agencies. This act also requires the establishment of state emergency response commissions (SERC) and local emergency planning committees (LEPC). The LEPC

includes local officials, police, fire, and public health authorities in addition to representatives of local hospitals, media, and the community.

Emergency response plans

The primary responsibility of the LEPC is to develop emergency response plans (ERPs) to do the following:

- Identify local facilities using hazardous substances
- Designate community and industrial coordinators
- Establish mechanisms of emergency notification
- Establish procedures for determining the occurrence of a release and an estimation of the affected population
- Identify community emergency equipment facilities
- Establish evacuation plans
- Establish and schedule training programs for emergency personnel

Hospitals are required to be an integral part of the ERP. Additionally, emergency medical services (EMS) units and coordinators have critical roles in the planning and execution of an emergency response. The plan for each community varies depending on the types of industries involved, chemicals used, and resources available. For example, many fire departments in metropolitan areas have developed specialized HAZMAT teams to respond to these situations. These teams are responsible for containing releases and for decontaminating persons exposed to hazardous materials. After decontamination, these patients can be transported safely and treated in the hospital with minimal precautions. In communities where a HAZMAT team is not available, the ERP must consider how persons exposed to hazardous materials will be decontaminated and transported. Hospitals must be capable of caring for severely contaminated patients under the ERP guidelines. Because many hospitals are poorly prepared to attend to a severely contaminated patient, early involvement of hospital representatives in the planning process is critical. Similarly, EMS coordinators must train emergency medical personnel to attend to contaminated patients and to establish contingency plans for their transport and care.

Joint Commission for Accreditation of Healthcare Organizations guidelines

Several JCAHO requirements relating to hazardous materials affect hospitals. Some of the more specific JCAHO guidelines are as follows:

- EC 01.01.01: The hospital plans activities to minimize risks in the environment of care.
- EC.02.02.01: The hospital manages risks related to hazardous materials and waste.
- EP3: The hospital has written procedures, including the use of precautions and personal protective equipment, to follow in response to hazardous material and waste spills or exposures.
- EP4: The hospital implements its procedures in response to hazardous material and waste spills or exposures.
- EP10: The hospital monitors levels of hazardous gases and vapors to determine that they are in safe range. Note: Law and regulation determine the frequency of monitoring hazardous gases and vapors as well as acceptable ranges.
- EM.02.01.01: The hospital has an Emergency Operations Plan. Note: The hospital's Emergency Operations Plan is designed to coordinate its communications, resources and assets, safety and security, staff responsibilities, utilities, and patient clinical and support activities during an emergency.

Occupational Safety and Health Administration regulations

The Occupational Safety and Health Administration (OSHA) has issued several regulations that pertain to any hospital employee who may come into contact with hazardous materials, including those on patients seeking medical care. Regulation 29 CFR 1910.120 (q) standard describes respiratory protection for all employees potentially exposed to hazardous chemical

vapors as well as the minimal degree of training for any employee involved in decontamination. Other standards (ie, 29 CFR 1910.132 [d], 1988) delineates that employers must assess the workplace for potential hazards and have employees use personal protective equipment (PPE) appropriate for that hazard. Under OSHA standards, an emergency response team is defined as an individual or group who responds to a release of a hazardous material, no matter where it occurs. This regulation initially was intended for hazardous waste operators and emergency response personnel at hazardous waste facilities; however, in the case of a patient who has been contaminated, hospital and EMS personnel also may be included. The current regulations state that all ED personnel must be trained at a minimum of first responder awareness level (level 1), and any personnel involved in patient decontamination must be trained to first responder operation level (level 2). OSHA has not fully determined how these standards will apply to hospitals and healthcare facilities that are off-site. Planning the roles of HAZMAT and EMS workers requires familiarity with the definitions and training requirements (described below) of individuals who may respond to a HAZMAT incident as defined by the Hazardous Waste Operations and Emergency Response (HAZWOPER) standards. If emergency medical transport personnel are expected to transport contaminated individuals or to provide medical care in the field prior to decontamination, they at least should have the appropriate level of training. Five levels of HAZMAT responder training are defined in CFR 1910.120 (q).

Environmental Protection Agency
Under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), EMS scene responders are protected under a "Good Samaritan" clause. However, healthcare facilities must contain any runoff from decontamination activities.

Hospital and community planning
Hospitals must have adequate plans for addressing HAZMAT incidents and incorporate these into community plans. Some of the aspects that need to be included in the plans include the following:

- Triage
- Personal protective equipment (PPE)
- Decontamination procedures
- Crowd control
- Dealing with victims who arrive by private vehicle
- Medical care after decontamination
- Public relations and press releases

The responsibility of hospitals cannot stop at the planning stage. Employees must be trained to use the PPE and how to perform decontamination. Incidents of hospital workers becoming ill as a result of chemical exposure when caring for a contaminated patient have been reported. If this occurs, the legal position of the hospital is tenuous. Providing universal guidelines for all communities is difficult. In formulating hospital and community response plans, the most critical aspects to consider are location of and responsibility for decontamination. Ideally, decontamination takes place in the field and is performed by specially trained HAZMAT teams. In this case, subsequent prehospital and hospital care can be performed with little change in the usual routine and with minimal risk to healthcare providers. In situations where several hospitals are located in a given area, it is not financially feasible for all hospitals to have good decontamination facilities. One hospital should be chosen as the receiving facility. The choice of hospital should be based on the availability of decontamination facilities, intensive care facilities, training of ED personnel, and staff trained in medical toxicology. Regardless of whether a hospital is a receiving facility or if it is in an area where a trained HAZMAT team is located, situations always occur when contaminated patients present to other prehospital or hospital systems. In any mass casualty situation, it is likely that victims will leave the scene and travel by private vehicle to the healthcare facility of their choice. For a hospital that was not a designated decontamination facility to send these

patients to another facility prior to decontamination would constitute an Emergency Medical Treatment and Active Labor Act (EMTALA) violation. Consequently, all hospitals should have a plan and appropriate employee training for attending to the contaminated patient.

Hazmat Incident Management

Chain of command

The HAZMAT disaster plan for a community clearly should define who is in charge of a situation. This person ultimately is responsible for protecting public health and the environment and ideally should be a specially trained individual representing either the HAZMAT team or the LEPC. The ERP should clearly delineate the authority of this person, even on private property or private facilities. The ERP must address many aspects other than medical care. The plan should stipulate the reasons for evacuation as well as local evacuation centers. The incident commander must consider public and rescuer hazards from toxic and corrosive materials as well as those from explosive or flammable materials. Finally, the plan must stipulate at what point EMS personnel not trained to attend to HAZMAT issues will interact in patient care. The community disaster response plan delineates the chain of command for a situation and specifies how the EMS system will interact with the HAZMAT team. Defining the point at which the EMS system gets involved with injured persons is not an easy task. Ideally, specially trained HAZMAT workers decontaminate all exposed individuals prior to turning them over to the EMS system. However, in any individual situation, the severity of a patient's injuries and degree and type of contamination must be weighed against the medical training of the HAZMAT worker and the EMS system. The ideal situation is to have the HAZMAT team is made up of specially trained members of the fire department who also are cross-trained as paramedics or emergency medical technicians (EMTs). However, smaller communities commonly do not have this luxury. Especially in situations in which the HAZMAT team is not trained in prehospital care, involving medical control physicians and poison control centers in patient care decisions is essential.

Goals in managing a HAZMAT incident

The goals of managing a HAZMAT incident include the following:

- Recognition of the situation and notification of emergency services
- Establishment of a command center
- Protection of site and emergency workers from any further exposure
- Identification of the hazardous materials involved
- Assessing the hazard risk and the degree of personal equipment required
- Rescuing any victims of hazardous materials exposure that are on-site
- Crowd control and keeping ambulatory exposure victims on-site until they are decontaminated
- Notifying local healthcare facilities of the incident and the number and type of victims
- Decontamination and initial medical care of victims
- Containment of the hazardous material, including runoff from decontamination activities
- Evaluation of further public exposure and evacuation where necessary

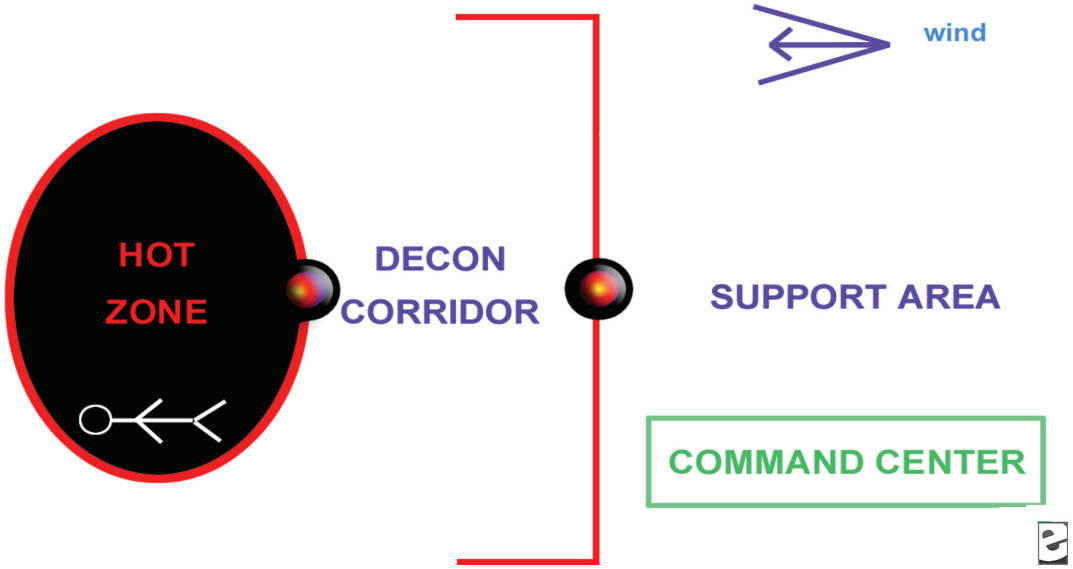
Obviously, many of these functions are performed concurrently. Recognition of the danger may seem a simple matter, but this usually depends on local workers or first responders. Most industrial site workers should be familiar with the site's ERP, including contact information in case of emergency and what to report. Potentially disastrous situations occur with motor vehicle or agricultural accidents in which the first responders are not aware of hazardous material dangers. In one series of HAZMAT incidents, 14% of exposed individuals were first responders. This emphasizes the importance of emergency medical personnel being trained, at a minimum, to the level of first responder awareness.

Site command center

One of the earliest priorities is the establishment of a site command center. Ideally, locate this command center near the incident but far enough away to avoid any exposure. The command center should be located upwind and uphill to avoid contact and should have a wind monitor and alarm system to warn of any shifting wind currents that may carry hazardous materials toward the command center. The command center should have a rapidly deployable communications system. This is critical to maintain contact with on-site workers and off-site emergency management and medical personnel to access information on the hazardous substances involved and necessary containment and safety procedures. The site should be divided and managed within 3 zones:

Zone control of the hazardous materials site.

The contaminated area is known as the hot zone. Only individuals with appropriate PPE and specialized training are allowed into this zone. The intermediate zone, also known as the



decontamination zone, is where patient decontamination should take place. A degree of contamination still is found in this zone; thus, some PPE is required, although it is usually of a lesser degree than that required for the hot zone. The command zone is located outside the decontamination zone. All exposed individuals and equipment from the hot zone and decontamination zone should be decontaminated before entering the command zone. Access to all zones must be controlled. Keeping the media and onlookers well away from the site is critical. After decontamination, victims who require medical care can be picked up in the command zone. Only trained individuals wearing necessary PPE should be allowed into the decontamination zone. This produces a dilemma when persons exposed to hazardous materials require immediate medical attention. If this is the case, the ideal situation is for some EMS personnel to have the appropriate level of training to work in PPE. If this is not possible, the medical control physician and the site commander must make decisions on an individual basis.

Transportation

Placing a contaminated patient in an ambulance is strongly discouraged. This is a closed environment and presents increased risk to those in the ambulance. This action also results in the contamination of the ambulance and its equipment. No further use of the ambulance is allowed until it can be decontaminated appropriately. Ambulances usually are resources that most communities cannot spare. Transportation prior to decontamination increases the amount of time the patient is in contact with the hazardous material. Some have recommended that patients be transported in the back of open trucks. In this situation, these patients are not medically monitored or treated while being transported. Transportation in the

back of an open truck should only be considered in those situations where no decontamination options exist at the scene and the hospital is prepared for decontamination.

Hazard identification

Identification of the hazardous materials involved is critical to all aspects of the rescue operation. As part of the SARA legislation, industrial sites are required to report all hazardous materials at their facility to the local emergency planning agency. In most instances, this information is maintained by the fire department or emergency planning agency. Industries also are required to post this information in a location external to the site, usually in an external electrical box or fire safety location. This assumes that the information contained in the external location or by the fire department is current. Problems may arise when new chemicals are added to an inventory and the lists are not updated. The DOT requires all vehicles carrying chemicals to display placards identifying them. Generally, these are diamond-shaped signs that have specific colors and numbers that define the class of hazardous material that is present. The DOT classes and defining colors of hazardous materials include the following:

- Explosives (solid orange color)
- Nonflammable gases (solid green color)
- Flammable liquids (solid red color)
- Flammable solids (white and red stripes)
- Oxidizers and peroxides (solid yellow color)
- Poisons and biohazards (solid white color)
- Radioactive materials (half white, half yellow with black radiation symbol)
- Corrosives (half white, half black)
- Other (usually white)

Each placard usually contains a descriptive color, symbol, and number. The triple redundancy is so that, in case of an explosion, any remaining portion of it can be used to identify the type of material present. The DOT identification system only identifies the type of hazard present and does not identify specific chemicals or materials. Many placards also contain a 4-digit number, known as the United Nations (UN) identification number. These numbers identify individual chemicals or groups of chemicals. Because several hundred thousand chemicals are known, obviously, only a relatively few can be identified by a 4-digit classification system. For this reason, many chemicals with similar characteristics are given the same UN number.

Personal Protective Equipment

Specialized equipment, known as personal protective equipment (PPE), is required to adequately protect rescue personnel and healthcare providers from secondary contamination. The type of PPE used depends entirely on the situation and the level of training of the user. HAZMAT workers required to enter the hot zone require a greater level of protection than medical personnel providing care to contaminated patients.

Levels of protection for work involving hazardous materials

Four levels of protection have been defined for work involving hazardous chemicals. Although these levels originally were intended for work at hazardous waste disposal sites, they have been adopted widely in other situations, such as rescue work.

- Level A is the maximum level of protection and usually is required only of HAZMAT personnel and others working in areas of very high concentrations of toxic agents, such as those entering the hot zone. It consists of a fully encapsulating chemical-resistant suit, positive-pressure self-contained breathing apparatus (SCBA), double layers of chemical-resistant gloves, and chemical-resistant boots. Airtight seals should be in place between the suit and the inner layer of the hands, face, and feet protection.
- Level B is used when full respiratory protection still is required but dangers to the skin are less. It consists of a SCBA and a chemical-resistant suit with resistant gloves and boots. No airtight seals on the face, hands, and feet are necessary.

- Level C is required when air concentrations are expected to be much lower and less likelihood of skin exposure exists. It consists of a full-face air purification device and a nonencapsulating chemical-resistant suit with gloves and boots.
- Level D level of protection is used only when no danger of chemical exposure exists. It consists of standard work clothes and no respiratory protection.

Most HAZMAT workers who enter the hot zone require Level A protection. This is very expensive, bulky, and requires specialized training in its use. The typical Level A HAZMAT suit costs several thousand dollars and must be cleaned between uses. Manual dexterity is poor, and the suits are very hot, limiting the amount of time that they can be worn. HAZMAT teams usually use Level B or C PPE for decontamination. This takes place away from the hot zone and when the amount of chemical present on a patient is significantly less than those that exist in the hot zone. Also, quantities of chemicals that might present physical hazards, such as explosions, should not be present on a patient. EMS workers and other healthcare providers require less protection than HAZMAT workers, but they still must be protected adequately when attending to contaminated patients. The level of protection required is usually Level C or B. This includes a chemically resistant suit, gloves, and boots; respiratory protection; face protection; and disposable boots. OSHA is still unclear on the level of protection that is recommended for medical personnel performing decontamination. The recommendations previously discussed suggest that Level B should be used in this situation. A considerable difference exists between Level B and Level C. Level B requires an external air source, either by SCBA or by a forced air supply through hoses. Either of these adds considerable expense and training compared with the use of air-purifying respirators used in Level C protection. Several research studies have concluded that Level C protection is sufficient for hospital decontamination. Recommendations for PPE to be used in situations of radiation contamination suggest only Level D–type protection plus a dust filter for respiratory protection.

Protective suits and gloves

For medical applications, inexpensive ($50-100) and disposable chemical-resistant, multilayer polymer suits are available. Suits much more expensive than this commonly are used for surgery involving patients with HIV or other infectious diseases. One common misconception is that Tyvek suits, which are very inexpensive and readily available around hospitals and laboratories, are suitable for decontamination work. This material provides no chemical protection, and most chemicals can penetrate this material immediately, although it suffices for work with dusts, including radioactive dusts and biological agents. These suits are recommended for training exercises but should not be relied upon for chemical protection. Glove material also is an important consideration, because the hands have the most contact with the patient. Unfortunately, no single glove material provides adequate protection against all chemicals. To counter this situation, most HAZMAT workers use several gloves of different materials. An ideal combination is nitrile and Viton. However, this is bulky and markedly limits manual dexterity. Because patients should be washed immediately with large quantities of water during decontamination, actual contact with pure chemicals is generally minimized. Typical latex gloves used in most hospitals offer little chemical protection. Nitrile has much better chemical resistance than latex and is now available in a thin, flexible, disposable glove that permits good manual dexterity. This is presently the ideal glove material for use when providing medical care to a patient who has undergone chemical contamination.
Aldehydes, halogenated hydrocarbons, ketones, aromatic hydrocarbons, nitro-organic compounds, and carbon disulfide rapidly can permeate nitrile. Unfortunately, most common solvents consist of chemicals within these classes. If these are encountered, a thicker overglove, preferably made of Viton, should be used until the patient is at least partially decontaminated. Most chemicals are removed just by removing the clothes. Once no chance exists of coming into contact with large quantities of pure chemical, such as during removal of the patient's clothes, disposable nitrile gloves should be sufficient. Boots should be worn, since the feet are in constant contact with contaminated water during patient decontamination. Because chemicals are diluted, inexpensive disposable boots should suffice. Boots also

provide slip resistance on wet floors. Avoid leather and cloth footings since these materials may wick up contaminants and are impossible to clean. Respiratory exposure to vapors is an additional risk to the healthcare worker. The small quantity of materials present on a patient makes generation of toxic concentrations of vapors unlikely. Respiratory protection especially is important when working in enclosed spaces, such as transport vehicles or medical care rooms.

Available types of respiratory protection - Cartridge respirators and supplied air respirators

Air-purifying cartridge respirators function by allowing the wearer to inhale air through a canister filled with a special sorbent material that binds chemical vapors. Cartridge respirators are inexpensive, portable, and easy to use and store. However, drawbacks exist to their general use. The type of cartridge used must match the chemical vapor in question. Different cartridges must be used to protect from organic vapors, acid gases, chlorine, ammonia, and methylamine. The sorbent materials also have a breakthrough phenomenon, in which chemicals elude off the sorbent after a period of use and then expose the user. Multisorbent cartridges are available that do not require matching with the vapor in question. In general, these have a shorter breakthrough period. These factors limit cartridge respirators to short-term use and to low concentrations of chemicals in the air. This is the situation that exists when patients require decontamination. Cartridge respirators depend on an airtight seal against the face. They require a good fit and cannot be used with facial hair. A moderate amount of work is involved when inhaling across the pressure resistance of the cartridge. All of this requires that any individual using this type of respirator be fitted properly and trained in its use. Cartridge respirators are very versatile for short-term use. They require adequate training of all personnel who may be expected to use them and require someone available at all times to decide which type of cartridge to use. Cartridge respirators are ideal for

performing decontamination outside the ED. To overcome many of the problems with air-purifying cartridge respirators, battery-operated cartridge respirators were developed. These use a battery-operated pump to draw air across the sorbent cartridge and pump it into a hood that surrounds the user's head. These do not require an airtight fit and can be used with facial hair. They do not require the user to work to draw air across the cartridge and, thus, are much cooler and less anxiety provoking. They also require less individual training. They still depend upon the cartridge to remove the vapor in question; thus, the cartridge must match the vapor. The time of use must be limited because of both chemical breakthrough in the cartridge and battery life. Since a clear shield surrounds the face, they provide better eye contact with the victims. These are probably the simplest and most versatile form of air purification device for hospital decontamination use. Supplied air respirators provide a source of clean breathing air through a hose and an external supply. The external supply can be provided from a pump or compressed air. Two types of masks are available: one with a

pressure-actuated valve and one that continuously blows fresh air across the face. The second type uses much more air than the first. The fit is less critical since any leaks always have air flowing from inside to out. The supplied air respirators can be used in all situations and for any length of time without worry about choice of the proper cartridge and breakthrough. Use of supplied air respirators also requires training, although proper fit is less critical, at least with the continuous flow type. Because of the necessary air supply and hoses, supplied air respirators are impractical for use with outside decontamination. Some HAZMAT teams use this method for personnel providing decontamination close to a supply vehicle that can pump the necessary air. If a decontamination room is to be established inside a hospital, supplied air respirators are the ideal choice. Most respiratory protection can be obtained using a half-face design, which covers the nose and mouth, or a full-face design that also covers the eyes. If the half-face design is used, goggles also must be worn to protect the eyes from splashes. However, the eyes are still exposed to vapors that can be irritating or toxic. If respiratory protection is to be used, choosing the full-face version to protect the eyes and entire face makes much more sense. Protection of healthcare workers from hazardous materials exposures can be achieved with some degree of advance planning and training. Chemically protective suits that are inexpensive and disposable are available. Respiratory protection also can be obtained without significant expense; however, the least expensive type, cartridge respirators, requires some additional training. The recommended PPE for decontamination of victims of radiation exposure, usually consists of a filter-type dust mask, gloves, and Tyvek or surgical scrub suit. This was intended to protect the healthcare provider from radioactive dust particles. Unfortunately, this PPE is completely inadequate to protect from chemicals in the liquid or vapor states. Alternatively, PPE designed for chemical protection is more than adequate to provide protection in the case of a patient exposed to radiation. To avoid confusion and simplify the protocol, only one type of PPE is recommended. This may be more elaborate and expensive than that needed for a radiation protocol; however, it can be used in all situations involving persons exposed to hazardous materials.

Decontamination

Decontamination is the process of removing or neutralizing hazardous materials on people or equipment. Removal of chemicals on skin is important for 2 reasons:

- To prevent further absorption and subsequent toxicity because many substances disrupt the integrity of the skin and then become systemic toxins following absorption
- To prevent other persons or equipment from becoming contaminated with substances on the patient's clothes or skin (secondary contamination)

The type of decontamination procedure used depends on the situation. Removing all clothes will also remove most of the contaminants. Most decontamination can be accomplished by simple high-volume dilution with water. Occasionally, mild soaps are required to remove oily or greasy substances. Phenol can be removed better with polyethylene glycol if available. If not available, use water. Also, see CBRNE - Chemical Decontamination. Avoid water in the presence of metallic sodium, potassium, lithium, cesium, and rubidium because these react on contact with water. Dusts of pure magnesium, white phosphorus, sulfur, strontium, titanium, uranium, yttrium, zinc, and zirconium ignite on contact with air. If burning, many of these explode if exposed to water. If these substances are suspected, remove residual metal with forceps and store it in a container of mineral oil. If radioactive particles are on or embedded in the skin, remove them by forceps. The radiation safety officer should dispose of them. Some HAZMAT teams use 4 special solutions recommended by the National Fire Protection Association for patient decontamination. Little evidence exists that these solutions are more effective at decontaminating human skin than water alone. In addition, none of the solutions can be used on open skin, mucous membranes, or the eyes. Collect the water runoff from the decontamination, and do not allow it to enter parking lots or storm drains. However, if a drain is readily available and arranging a collection system will require considerable time, decontaminating the patient and allowing the water to enter the drain may be prudent. Although this action theoretically can result in a fine from the EPA for an unscheduled discharge, to date, this situation has not happened to a hospital. The collected water should be

considered to be contaminated with a hazardous substance. If it is allowed to spread into an open area, it likely will be tracked off-site into private vehicles and homes. Collection of the decontamination runoff is accomplished by using a series of collection pools, which can be specially designed devices or can be as simple as inflatable children's pools. For ambulatory patients, a series of 3 collection pools usually is used, with contaminated patients or workers always starting in the most contaminated pool and finishing in the least contaminated pool. For nonambulatory patients, specialized runoff collection litters are available. Remove clothes and place them in a plastic bag, and mark it as contaminated. Give priority to decontaminate the eyes, mucous membranes, and severely affected areas of the skin. Take care not to wash contaminants onto unaffected areas of the skin. Thoroughly irrigate areas of skin where the surface is broken. Avoid abrasive cleansing. For radioactive materials, a Geiger counter can be used to detect any residual contamination. Unfortunately, no simple instrument is available for the wide range of chemical contaminants. Portable handheld monitors are available for detecting hydrocarbon vapors, but these usually are not available in hospitals. Copious irrigation is the standard rule; however, this should not be to the point of irritating or denuding the skin.

Hospital Protocol for Hazmat Incidents

Hospital care for a person exposed to hazardous materials should begin with adequate planning well before the incident occurs. Failure to have an adequate plan to attend to a HAZMAT situation can result in injury to hospital employees and subsequent liability to the hospital for not meeting OSHA standards. More importantly, most hospital EDs serve integral functions to the hospital and the community. Closure of an ED because of contamination can have dire effects on hospital function and the community's medical resources.

Decontamination plan

Most hospitals are poorly prepared to care for a contaminated patient and have little protection for hospital employees who are involved. This is even more reason to be involved in the community planning process. If hospitals are unprepared to decontaminate persons exposed to hazardous materials, every effort should be made to decontaminate patients in the field. Even if this is the case, hospitals should have some plan to decontaminate victims who arrive by private vehicle or by an inadvertent ambulance transport. In the worst-case scenario, the contaminated patient should be held outside the ED until the community HAZMAT team can assist with the decontamination. Whatever the situation, decontaminating the patient prior to entering the ED is essential. The first decision to be made in formulating a HAZMAT plan for the ED is where decontamination is to take place. An inside decontamination area is ideal, although it often may not be practical or possible. Locate an inside decontamination room so that it can be accessed without entering the hospital or the ED. The room can be used for other purposes, although anything inside the room should be easy to remove. An advantage of an inside area is proximity to ED personnel, supplies, and electrical and water sources. Monitoring patients and providing critical medical care obviously is easier in a room adjacent to or in the ED. Controlling access to a single room also is much easier. However, after the room is used, provisions need to be made to clean the room and remove wastes. Performing decontamination outside the ED is probably more practical in most situations, although it detracts from the care of the patient who is critically ill. If the decontamination area is located inside, it should be adjacent to an entrance, preferably the ambulance entrance. Gaseous, liquid, and solid wastes must be collected. The room should be under negative pressure and have a separate ventilation system that discharges to the outside. Contaminated irrigation water should not be discharged into the general hospital drain system but should be collected in a specialized holding tank under the decontamination room. The expense of installing a tank for this purpose is difficult to justify unless a new room is being constructed specifically for decontamination. Alternatively, liquid wastes can be collected in inflatable plastic children's swimming pools or expandable plastic containers designed for this purpose. For patients who are not ambulatory, specialized litters are available to collect water runoff in special collection barrels. Plans need to be made for eventual removal and disposal of

collected wastewater. Planning for outside decontamination is simpler and less expensive than equipping an indoor decontamination room. Ventilation is not a significant problem outside, although the decontamination team should wear respiratory protection if indicated by the type of hazardous material. The prospective site must have a water hose for decontamination. Ideally, the water supply should be temperature controlled. The wastewater still must be collected and not allowed to run over lawns or pavement into sewer drains. Portable pools can be used for collection, but provisions must be made to prevent access to these prior to removal. Similarly, solids must be collected and properly stored prior to disposal. Two of the drawbacks to outside decontamination are patient privacy and weather. These problems can be handled by using tarps and portable heaters. Portable showers that can be assembled easily are now available commercially. External decontamination shelters that are portable and easily assembled are now available. Some have access for ambulatory patients as well as patients on stretchers. Pumps are provided to store water in barrels. All that is required is a water supply and a power source. Providing medical care to patients who are critically ill is more difficult if decontamination is performed outside. If medically indicated, portable monitors and portable oxygen may be needed. This equipment must be cleaned thoroughly or discarded after use. A special portable communication system may be needed if the decontamination team is using respiratory protection. Additional personnel are needed to obtain necessary medications and supplies from inside the hospital. Finally, if the decontamination is to be performed outside, the area must be secured properly. Encircle the area by rope or tape; security personnel are required to prevent unauthorized entry. The area may need to be secured for several days until all wastes are removed. The goal of decontamination is to remove enough of the contaminating material so that any danger of secondary contamination to those providing medical care or to the patient no longer exists. Ideally, decontamination should require only 10-20 minutes, although patient stabilization may prolong this period. After decontamination, the patient can be moved into the general treatment area and treated as any other patient. Limit treatment to only basic life support measures and life-saving procedures within the decontamination area. The choice of which procedures will be performed in the decontamination area must be made on an individual

basis. Any medical interventions will prolong decontamination and the time until the victim

can be moved into the ED for more definitive care. While conditions such as tension pneumothorax, cardiac dysrhythmias, or respiratory distress should be treated immediately; most conditions can be treated with basic stabilization until the patient has been decontaminated. Consider any item used in the decontamination area contaminated until it has been cleaned thoroughly. Postpone the acquisition of radiographs, ECGs, and routine blood work until the patient is moved out of the decontamination area. One observer outside the decontamination area should monitor how long team members are working in PPE and limit each individual's time. The equipment can be very hot, and the situation is stressful. Any team member who appears fatigued or stressed should be immediately removed. Decontamination team members should be trained in the proper method of removing the personal protective gear. Equipment should be removed in the opposite order from which it was initially put on. An inner layer of disposable gloves should be the last item removed. Care should be taken to not handle the chemical-resistant suit with bare skin. Items that need to be reused, such as respirators and masks, should placed in a separate area. Some published radiation protocols recommend long lists of supplies to be maintained in the decontamination area. This should not be a problem if the decontamination area is in or adjacent to the ED, where all necessary supplies should be readily available. Using a runner for needed items is much more efficient.
The hospital protocol should include guidelines that outline who is to perform decontamination. Although having a single team to train is easier, training at least 1-2 members of each shift is more practical. HAZMAT situations occur spontaneously and with no advance notice. The delay of calling a special decontamination team from home is not practical. In the protocol and training, specify how team members are to remove PPE, where the contaminated materials can be stored until they can be disposed, and who is responsible for the disposal of contaminated material.

Conclusions

- Hospitals are required to participate in community disaster planning for HAZMAT incidents according to SARA Title III.
- Hospitals are required to protect their employees from hazardous materials exposures, including exposure that may occur as a result of patient care.
- Patient decontamination ideally should be performed in the field.
- Unprepared EMS units should not transport contaminated patients.
- Adequate PPE for healthcare providers not in a hot zone includes a chemical-resistant suit (Tyvek is not sufficient), nitrile gloves, disposable boots, and full-face cartridge or supplied air respirator. This equipment is less expensive than some operating suits.
- Healthcare providers need training prior to using PPE.
- Hospitals should have plans to attend to patients contaminated by hazardous materials.
- Decontamination can be accomplished safely outside the ED or in specially prepared rooms indoors. Contaminated patients should not enter the main areas of the ED or hospital.
- If a hospital is unprepared to handle a contaminated patient, one option is to call the local HAZMAT team. However, this should be worked out in advance and there still needs to be a plan if they are not available.

Disaster Planning

A disaster occurs somewhere in the world almost daily; however, to most people, disasters of the type discussed in this article are unusual events. A recent group of disasters, starting with the September 11th terrorist attacks and continuing through the tsunami affecting countries throughout the Indian Ocean, the South Asia earthquake in Pakistan, and the 2005 and 2008 Gulf Coast hurricanes have focused people's attention upon this topic. Despite the increase in general awareness with recent events, the relative infrequency of major catastrophes affecting defined populations, leads to a certain degree of complacency and

underestimation of the impact of such an event. The result of complacency is relative reluctance to devote the necessary resources for adequate disaster preparedness. Indeed, several authors note that the best time to propose major changes for disaster preparedness, including its funding, is immediately following a major disaster, even if the event has occurred in a remote location. In the United States, large multiple-casualty events are exceptionally rare by world standards. Only 10 disasters in US history have resulted in more than 1000 fatalities (see Table 1). The vast majority of major events have resulted in fewer than 40 fatalities. According to data from the Centers for Disease Control and Prevention, the September 11th attacks caused 2819 deaths. Compared with 44,065 deaths from motor vehicle accidents in 2002, this number is small. However, the dramatic nature of disasters, with a relatively large death toll and psychological impact for a short time period can overwhelm an unprepared health and response system.

Table 1. US Disasters With Greater Than 1000 Casualties*

Year	Event	Deaths
1865	Steamship explosion	1547
1875	Forest fire, Wisconsin	1182
1889	Flood, Pennsylvania	>2000
1900	Hurricane, Texas	8000
1904	Steamship fire	1021
1906	San Francisco earthquake	>3000
1928	Hurricane, Florida	2000
1941	Pearl Harbor Attack	2403
2001	September 11 Attack	2819
2005	Hurricane Katrina	>1300**
1865	Steamship explosion	1547
1875	Forest fire, Wisconsin	1182
1889	Flood, Pennsylvania	>2000
1900	Hurricane, Texas	8000
1904	Steamship fire	1021
1906	San Francisco earthquake	>3000
1928	Hurricane, Florida	2000
1941	Pearl Harbor Attack	2403
2001	September 11 Attack	2819
2005	Hurricane Katrina	>1300**

*Exact death tolls can be difficult to calculate, and some of these numbers are estimates. **Even in modern times, death tolls can be difficult to establish. Debate still exists about the actual number of people who died during Hurricane Katrina and its aftermath. An article by Brunkard et al published in Disaster Medicine and Public Health Preparedness in August 2008, puts the Louisiana death toll at 971 plus another 15 deaths among evacuees. An Associated Press article from 2006 claims the total number of bodies recovered from Louisiana and Mississippi was more than 1300. There is also ongoing investigation into the possibility that the storm caused deaths during subsequent months and years due to myriad causes (eg, inadequate medical care, relocation stresses).

When a disaster strikes, the general population expects public service agencies and other branches of the local, state, or federal government to rapidly mobilize to help the injured and the community in general. Preservation of life and health are of paramount importance to those individuals injured in the disasters. For this reason, medical professionals must be included in all phases of disaster planning, as well as in the immediate response to these

events. Adequate preparation has become particularly important following the problematic response seen during Hurricane Katrina.

Classifying Disasters

Natural versus technological disasters

Disasters are classified in a variety of ways. A common system divides incidents into natural and technological (human-made) disasters. For planning purposes, this distinction provides little conceptual help as there are frequent crossovers. For example, artificial structures may collapse as the result of hurricanes or earthquakes. During Hurricane Katrina, emergency personnel had to contend with fires while rescuing people from flooded areas. Certain generalizations, however, may be made about natural disasters. Tornadoes may be quite lethal but are generally short-lived. Hurricanes cut a wider swath than tornadoes, tend to last longer, and have more long-term recovery effects. Tornadoes, hurricanes, and floods tend to occur in certain geographic locations. Volcanoes also may be quite lethal but have become more predictable in recent years. Until recently, the most devastating natural phenomena, with regard to numbers of fatalities, were thought to be earthquakes. However, the December 2004 tsunami affecting countries throughout the Indian Ocean, with an official death toll of 224,228 people, ranks as one of the most lethal disasters in recorded history. Technological disasters tend to be more contained but can be quite lethal. Fires have caused some of the largest numbers of casualties in this country. Toxic spills (ie, release of cyanide gas in Bhopal, India) and nuclear mishaps (ie, Chernobyl) have caused short- and long-term havoc, death, and destruction.

War and terrorism

Other incidents with potential for mass casualties and disaster include war and terrorism. Since the 9/11 attacks on the World Trade Center in New York City, terrorism has become a major focus of disaster response and preparedness. Although the world has yet to experience a terrorist-related nuclear disaster, the raw materials and technology exist to develop nuclear devices as small portable units such as "dirty-bombs." No geographical location is immune from the devastating effects of terrorism. These activities have become more frequent and lethal in recent years with no forewarning, as evidenced by the 9/11 attacks, the Madrid and London bombings, and the more distant, but still tragic, Sarin nerve agent attack on the Tokyo subway system.

Classifying disasters

Disasters are often classified by the resultant anticipated necessary response.

- A Level I disaster is one in which local emergency response personnel and organizations are able to contain and deal effectively with the disaster and its aftermath.
- A Level II disaster requires regional efforts and mutual aid from surrounding communities.
- A Level III disaster is of such a magnitude that local and regional assets are overwhelmed, requiring statewide or federal assistance.

Disaster preparation

Various methods have been developed to assist planners in disaster preparation. One such method is a modification of the Injury Severity Score. It is based on cause and effect, the area involved, the number of casualties, and other parameters. The potential injury creating event (PICE) system is designed to identify common aspects of a disaster and of response capabilities. Such systems are especially valuable tools in planning for disaster mitigation. The PICE system uses 4 modifiers to describe a particular disaster (see Table 2). The first modifier describes the potential for additional casualties. The second identifies the degree to

which local resources are disrupted. The third modifier identifies the geographic boundaries of involvement. The final modifier, crisis staging, indicates the likelihood of needing outside assistance to augment or replace local resources. It is important to note that in the PICE methodology, identical disasters may have differing descriptors depending on the location of the event and the availability of resources.

Table 2. Potential Injury-Creating Event Algorithm

A	B	C	Stage
Stable	Static	Local	0
Dynamic	Disruptive	Regional	I
	Paralytic	National	II
		International	III

Definitions and Terminology

Disaster medicine is difficult to conceptualize. It can be broadly defined. The World Health Organization defines a disaster as a "sudden ecological phenomenon of sufficient magnitude to require external assistance." The American College of Emergency Physicians (ACEP) states that a disaster has occurred "when the destructive effects of natural or man-made forces overwhelm the ability of a given area or community to meet the demand for health care." Other definitions exist, but the common denominator calls for a disruption of such magnitude that the organization, infrastructure, and resources of a community are unable to return to normal operations following the event without outside assistance. To further clarify the contrast between normal emergencies and disasters, ACEP states, "emergency medical services routinely direct maximal resources to a small number of individuals, while disaster medical services are designed to direct limited resources to the greatest number of individuals." In contrast to disasters, multiple casualty incidents (MCIs) have as their primary effects morbidity and mortality to individuals, while the community infrastructure remains relatively intact. A passenger train accident with 500 injured or dead occupants is considered an MCI. However, if this morbidity and mortality were the result of the release of chlorine gas from a hazardous material accident, a much higher potential for additional casualties would exist. Normal operations and activities of daily living would be disrupted for a longer period, which would be considered a disaster by most experts.

Phases of Disaster Response

A disaster cycle has 4 phases, and all responses must pass through each:
(1) mitigation,
(2) planning,
(3) response, and
(4) recovery

Pitfalls during transitions can occur throughout the phases. Generalized awareness, proper planning, and contingencies may reduce the overall effect of any specific inadequacy in response.

Mitigation

In certain cases, some of the devastating effects of disasters can be reduced before the actual event. For example, evacuations may be orchestrated before hurricanes or floods. Early warning allows residents to seek shelter from tornadoes. Sprinkler systems in businesses and homes can reduce overall risk of total fire destruction.

Planning
Disaster planning is discussed more thoroughly in External and Internal Planning. It cannot be stressed enough, however, that a disaster plan is not synonymous with disaster planning. Many communities have detailed, "paper" plans, which, when tested, are found to be either based on faulty assumptions or to be totally unworkable in the context of the initial response.

Response
A number of events occur during initial response to a disaster. If there is forewarning, certain aspects of the response may take place even before the event. Unfortunately, significant forewarning is rare.

Activation

Notification and initial response
During this phase, organizations involved in disaster response and the potentially affected populations are notified. In the event that the disaster is anticipated, this phase takes place even before the disaster. Many locations in hurricane areas require more than 24 hours for full evacuation.

Organization of command and scene assessment
Once the activation phase has begun, the prearranged command and staff structure (for details, see Incident Command System below) for responding to the disaster should be arranged and initial communications nets established. This is one of the most crucial steps to take once the disaster occurs. Historically, valuable time may be lost during a disaster response while the central system coordinating the response effort is being prepared. During this phase, initial reports leading to overall scene assessment begin to arrive. For static disasters, required response assets may need to be determined. Often, the only initially known fact is that the disaster is an ongoing process. However, even this fact is important in determining whether outside assistance is needed, leading to timely activation of those resources.

Implementation

Search and rescue
Depending on the structure and function of the incident command system (ICS), search and rescue may fall under the direction of fire, emergency medical service (EMS), or police (security) forces. In contained, geographically localized incidents, the search and rescue effort is fairly straightforward. In larger disasters, especially ones that are ongoing or may involve terrorist activities, a cooperative approach is necessary and the very act of search and rescue must be highly organized to ensure adequate and complete coverage of all areas.

Extrication, triage, stabilization, and transport
Extrication has evolved into a fire services function in most of the country. In addition to specialized technical and trench rescue teams, fire services have more experience with building collapse and secondary hazards (eg, floods, fires) than other organizations. The concept of triage involves providing the most help for as many as possible. A complete description of triage is beyond the scope of this review. Medical personnel are accustomed to providing extensive, definitive care to every patient. When confronted by numerous patients simultaneously in a disaster situation, it is easy to become overwhelmed, even for an experienced disaster worker. Triage must occur at multiple levels, and patients must be reassessed during every step of the process. Transport must be both organized and orchestrated to equitably distribute victims to capable receiving facilities. During recent civilian disasters and even in Operation Desert Storm, the majority of critically injured individuals were taken to only one or two receiving facilities, which were almost overwhelmed. This occurred at a time when other facilities sat dormant awaiting patients.

Definitive scene management
While scene control and containment may be relatively simple in a local, static disaster, dynamic disasters and those that paralyze response systems may take several days to contain and stabilize. As the length of time of the disaster increases, additional resources must be made available, as rescue crews reach exhaustion, supplies are depleted, and additional hazards develop.

Recovery
The recovery phase is frequently underemphasized in disaster plans, but it is crucial for the affected community. During this phase, some semblance of order is restored, public utilities are reestablished, and infrastructure begins to operate effectively. Scene withdrawal and a return to normal operations usually occur simultaneously. Treatment of the responders is also vitally important during this phase for critical incident stress debriefing and other support services that have evolved for this purpose.

Debriefing
Valuable lessons may be learned during debriefing. It is of utmost importance to obtain as much information as possible from all parties involved in the disaster response effort. Without full disclosure, similar weak responses will impede future efforts.

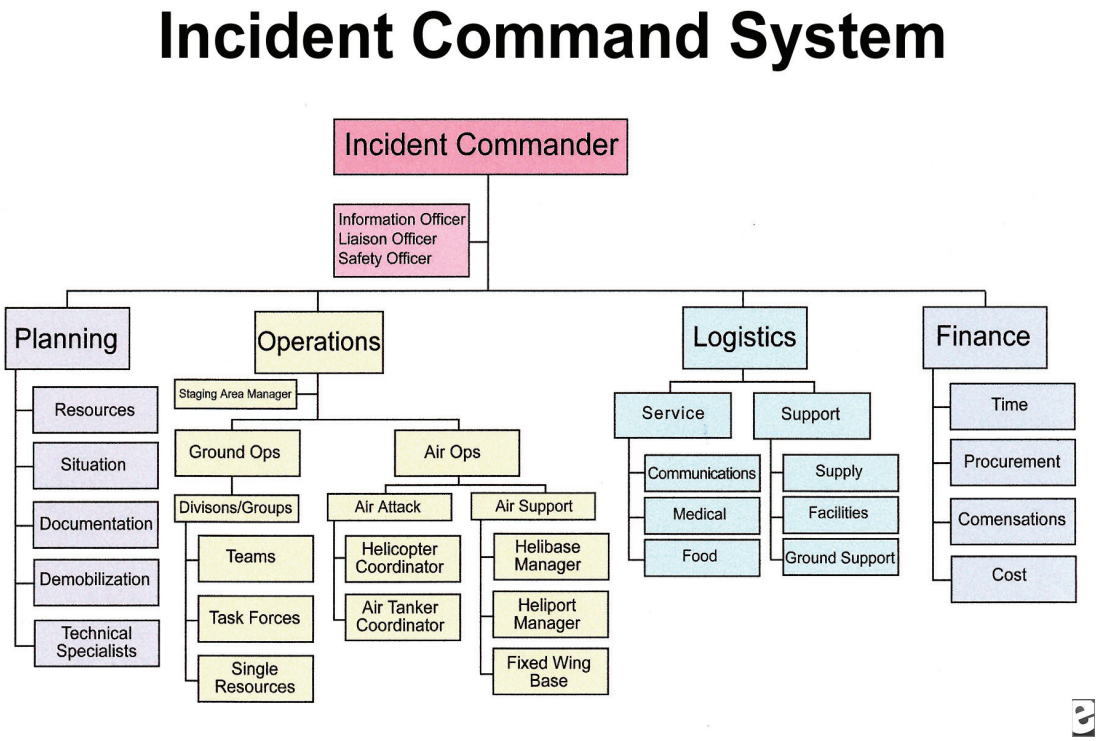
External and Internal Planning

External planning
Disaster planning should to the extent possible incorporate formal disaster research findings. Disaster plans sometimes rely on faulty assumptions that do not prove true in actual disasters. For example, planners may logically assume that the sickest patients will be transported first during a disaster, when, in reality, this may not happen in many instances. A disaster plan encompassing both local and regional areas must focus on 3 possible scenarios:

- The disaster occurs within the region and is confined and controlled with existing resources.
- The disaster occurs in a neighboring region, and regional assets are requested through mutual aid agreements.
- The disaster area is the region and requires state or federal assistance for an effective response.

Incident command system

After a series of fires in California in the 1970s, the Fire Suppression Services developed the ICS concept to organize an effective response to major disasters. The ICS structure includes 5 functional units: command, operations, logistics, planning, and finance. Most disaster plans include similar organizational structures that are often modified depending on normal



operations of the various agencies. In developing a disaster plan, leaders should remember that it is impossible to plan for all contingencies; therefore, plans must be relatively general and expandable. Most disasters that can be contained using local or regional resources have fewer than 100 fatalities and fewer than 500 major casualties. If plans are developed for larger-scale disasters, the plan should focus on the first 48 hours of the disaster until state and federal assistance teams can arrive and to address high initial fatality rates during the first 24 hours.

Rehearsal

All phases of the disaster response must be addressed in a disaster plan. Functional job descriptions and responsibilities of all agencies and organizations involved should be delineated clearly. More importantly, these plans should be exercised and rehearsed. The ideal exercise includes participation by all parties involved. Since these exercises, by their very nature, disrupt normal operations and are costly in personnel and material utilization, disaster agencies frequently conduct a proxy exercise on the "tabletop." This is a simulation of an emergency situation for training and testing plans and procedures that does not involve movement of response resources. Tabletop exercises are good training tools because they allow people in leadership positions to work through major problems without the cost of running vehicles, using staff and volunteer time, or using supplies. They can quickly highlight areas of weakness where additional support may be needed.

Organization

As part of the Federal Response Plan, the National Disaster Medical System was developed in the 1980s by the Department of Defense, the Veteran's Administration, the Federal Emergency Management Agency, and the Department of Health and Human Services. The Federal Response Plan calls for the development and response of up to 12 functional units to assist, but not direct, the disaster response initiative on declaration of a state of emergency by

a territory or state government. Approximately 1000 stateside beds were identified in preparation for Desert Storm, although no simulation exercise was performed, leading to criticism from the Government Accounting Agency. Disaster medical assistance teams (DMATs) are groups composed of volunteer physicians, nurses, EMS personnel, and others who are transported to disaster sites to participate in the triage, stabilization, transport, and treatment of patients. As examples of use of these teams, DMATs responded to the Oklahoma City Federal Building bombing, Hurricane Katrina, and have prestaged at certain critical events, such as the Atlanta Olympic Games.

Internal planning

Hospital disaster planners must take into account the scenarios previously described, including the possibility that the disaster may involve the hospital. For such rare events, aspects of hospital involvement such as mass decontamination, multiple triage and staging areas within the confines of the hospital, recall of critical personnel, and provisioning of adequate supplies and resupply must be anticipated. The Joint Commission (formerly Joint Commission on Accreditation of Hospitals [JCAHO]) requires hospitals to exercise disaster plans periodically and to form disaster committees. These committees should comprise key departments within the hospital, including administration, nursing services, security, communications, laboratory, physician services (including, but not limited to, Emergency Medicine, General Surgery, and Radiology), medical records, and maintenance/engineering. The hospital disaster plan should include protocols and policies that meet the following needs:

- Recognition and notification
- Assessment of hospital capabilities
- Personnel recall
- Establishment of a facility control center
- Maintenance of accurate records
- Public relations
- Equipment resupply

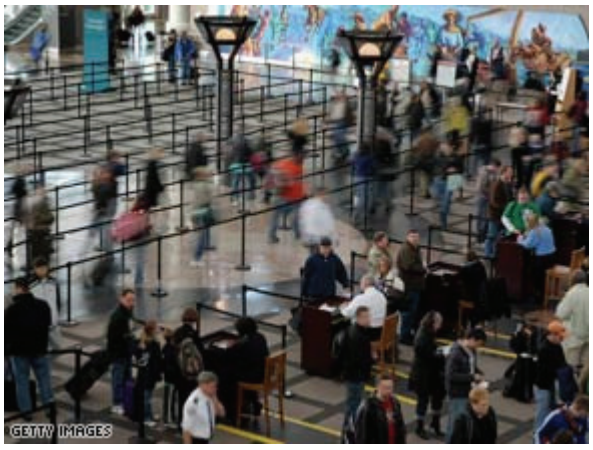
New, more stringent requirements for health care organizations were approved by the Joint Commission in 2000 and went into effect in 2001. Probably most significant are the requirements to integrate hospital disaster planning into community plans, to ensure that disaster programs address all phases of the disaster cycle, and to have the capability to evacuate the entire hospital staff and patients and relocate and operate from an independent facility. Discussions are continuing with the Joint Commission to further strengthen requirements concerning decontamination, polices, and training in response to terrorist activities involving chemical, biological, radiological, nuclear, and explosive agents.

Summary

Disaster planning is a regional effort. Every jurisdiction should plan for MCIs and disasters. All plans must be simple and based on normal daily operations of the various components involved in the disaster plan. Personnel potentially involved must be familiar with the disaster plan. It should be exercised frequently, even if only by tabletop exercises. Contingency plans for mutual assistance and state or federal response also must be considered and reviewed.

Scanning Crowds for Bombs

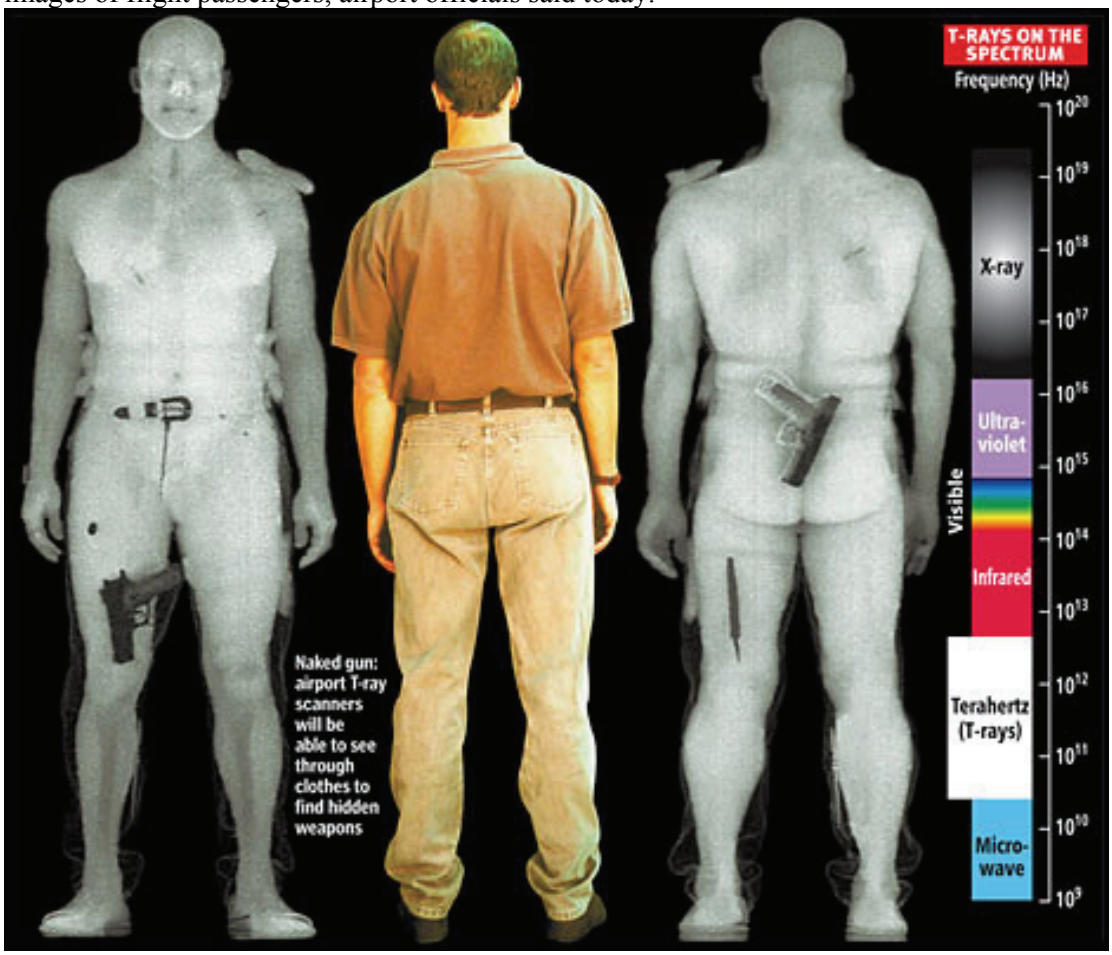
The airport checkpoint is a linchpin of aviation security, but one of its unintended consequences imparts vulnerability: the long, weaving line of travelers who await screening.



The lines present suicide bombers with a potential target that is common not only to airports but also to public events where masses must pass through security screening. Passive millimeter wave scanners can spot suspicious objects under clothes, and someday, laser spectrometers may spot explosive residue on clothing yards away. Both technologies still, however, would require that people pass through choke points, as these technologies can only scan one person at a time. With these threats in mind, the Air Force Research Laboratory (AFRL) at Wright-Patterson Air Force Base, Ohio, pitted students from rival colleges against one another in a competition to see which school could better detect simple improvised explosive devices (IEDs) across large areas and groups. The winning entry, fielded by students from the University of Michigan, relied on sensors linked by a wireless network, with software that processed data from the sensors to spot potential threats. The concept holds the promise of scanning large areas and crowds for explosive threats. The AFRL based the competition's scenario in part on an historical event—the 1996 Olympic Park bombing in Atlanta, where Eric Rudolph detonated a fairly rudimentary IED—a pipe bomb composed primarily of metal. Teams from Michigan and arch rival The Ohio State University were challenged to detect similar threats as they passed through a 100-square-foot area packed with vehicles and volunteers that re-created a pregame tailgate party. Knowing the threat objects would likely contain large amounts of conductive metals, the Michigan team mounted their own homemade magnetometers atop skinny traffic cones and arranged them around the perimeter of the competition area. These devices transmitted data back to a notebook computer, which used the team's software to analyze the data and project potential threat objects onto a top-view rendering of the area. Ohio State developed a "system of systems" that included a magnetometer, an infrared camera, and a radar system that, when coupled with an electromagnet, could detect large metal objects. But, software woes plagued the radar, and Ohio State only detected one of six bombs, compared to four of six detected by Michigan. Michigan team member Ashwin Lalendran notes that magnetometers alone may not catch explosives that contain little or no conductive metal. The persistent limitations of spectroscopy and millimeter wave, however, have led even the government's top researchers to reexamine magnetometers for wide-area explosives detection, says Nick Lombardo, project manager with Pacific Northwest National Laboratory's Department of Homeland Security Standoff Technology Integration and Demonstration Program. Lalendran sees the greatest value in Michigan's software system. As commercial devices used to detect traces of hazardous materials, explosives, biological agents, and radioactivity grow smaller, cheaper, and more sensitive, they might be incorporated into networked sensors that could scan wide areas for threats. The Air Force agrees, and hired Lalendran to continue his work at AFRL. The challenge was one of four the Air Force is holding this year. The laboratory pits interscholastic rivals against one another and gives competitors a tight deadline and a limited budget to create a pressure cooker, says David Shahady, the lead of AFRL's Innovation Program. "If you take a fairly serious problem and give it to these students, they're young, energetic, and creative. And you create an environment where there's not much time and there's competition, you find that they come up with these great solutions," Shahady says.

'Strip search' scanner suspended for children at Manchester Airport

Children will be not be subjected to a new X-ray body scanner which produces "naked" images of flight passengers, airport officials said today.



Manchester Airport managers have had a rethink on allowing under-18s through the scanner after child protection experts warned that they risked breaking the law by creating indecent images of juveniles. The RapiScan machine being trialled at the airport's Terminal 2 shows up a clear outline of passengers' bodies as well as breast enlargements, piercings and false limbs. Travellers can opt out of the virtual strip search but the airport had planned to let children take part if their parents gave consent. Terri Dowty of Action on Rights for Children, a UK internet based group supporting the United Nations convention on the rights of the child, said: "It's not right to put the machine operators in the position where they are being asked to break the law. Under present legislation the taking of images of children in this way cannot be done." A Manchester Airport spokeswoman said: "Experts in child protection have told us that this is a grey area. On this basis, if these experts tell us that there might be a problem then we'll work with them to establish a definitive position. In the meantime no under 18s will participate in the trial when adult passengers start being invited to take part in a couple of weeks."

Fake students smuggled in on visa scam

STUDENT visas are being exploited to smuggle people into Australia via a network of unscrupulous migration and education agents, landlords and employers, the head of the nation's biggest overseas student recruitment agency said yesterday. Tony Pollock, the chief executive of IDP Education Australia, the main recruiter for Australia's $16 billion industry in foreign students, described a "chain of exploitation". Some overseas students had become

victims of deception from "a highly integrated chain" of misrepresentative and exploitative education and migration advice, access to dodgy colleges, part-time work and accommodation, he said. "This could be construed as people-smuggling." At a minimum, it involved hundreds of students coming to Australia every year, he said. Mr Pollock said the practice caused "deep resentment" among students who were being mercilessly exploited by countrymen, and had to be rooted out. An investigation by The Australian has revealed that the racket starts overseas with the bogus student being offered a "package" of the finance necessary to satisfy Australian student support requirements, plus fake documentation, access to a dodgy private college, accommodation and even part-time work. In order to get a visa, students are required to have at least $12,000 in a bank account, but under the scam the education agents lend the bogus students the money they need to circumvent financial requirements. The loan is given at a high rate of interest, and in some cases the bogus student must make an immediate upfront payment of up to one-third of the total back to the agent. The bogus student is then provided with false English language documentation to study in Australia at a certain educational level, and enrolled in a college owned by the agent or a relative in Australia. Once in Australia, the student does not even show up for class but is marked as fully attendant to satisfy strict visa requirements, provided fees are paid. To complete the package, the bogus student is provided with accommodation and often a part-time job in a restaurant or taxi owned by one of the principals in the chain. An Indian migration agent, who would not be named, said it was common for agents linked to Australian colleges and businesses to recruit students and provide hefty high-interest loans: "They are all part of one syndicate. They are linked by someone's brother or someone's cousin in a different name. The students are under threat. The students are scared." The Australian revealed in September that a Korean education agent was found to be running a house in Sunnybank, Brisbane, that was housing up to 37 foreign students. A law firm that deals with migrant visas has accused education agents of taking kickbacks for finding jobs and accommodation for the students they recruit. "Unscrupulous education agents are the first point of contact for an overseas student and a level of trust is built, which some take advantage of," Visa Lawyers Australia principal Aristotle Paipetis said. "International students may do things and tell agents things the agent may use as a means of exploiting them." Education Minister Julia Gillard said yesterday the government deplored unscrupulous operators and investigated all allegations onshore. "Ultimately we have no sovereign power over unregistered agents operating in other countries," she said. Ms Gillard urged people to report such operators to police.


THE AUSTRALIAN

New face of humanity

PM's $50m Indon solution

Chopy suits ever shorter

Song's over for the Lanky Yank

australia's best airline as voted by you. fly with us.

Mushroom fruit could aid in clean up of bioweapons

A strange new natural contender in aiding in the fight against biological weapons has stepped forward, with researchers learning that the fruit of mushrooms can be used in cleaning up following a biological attack. Mushroom researcher Paul Stemets has discovered that mycelium from mushrooms may be able to break down and detoxify biological warfare agents. Mycelium, the fruit of a mushroom, breaks down hydrocarbons. Hydrocarbons form the base for many pollutants and biological weapons. In forests, mycelium's main role is

breaking down and recycling nitrogen, carbon and plant and animal debris. Mushroom mycelia have also proven effective in breaking down lead and mercury as well as removing industrial toxins from soil, including pesticides, chlorine, dioxin and PCBs. It has also shown to be effective in killing E. coli and Staphylococcus sp. Mycelium act as a filter, absorbing compounds from the soil and water that surround it and removing any usable materials. Once all usable materials are absorbed, mycelia break down any remaining contaminants. In soil contaminated with diesel fuel, following an inoculation with mycelia from oyster mushrooms, the soil was found to have lost its toxicity in only eight weeks. In the event of a groundwater based attack, mycelium can also be used to cleanse the water of contaminants and pollutants.

Roving, early-warning WMD detector

"QinetiQ North America announced today [08Feb10] that it is working with Brewer Science and Applied Systems Intelligence on a program to develop an autonomous, self-deploying sensor that will serve as a roving, early-warning detector of biological warfare activity. The program is being funded by the U.S. Army Research Office. Work on the project will be performed primarily at the Jordan Valley Innovation Center (JVIC) at Missouri State University, Springfield, Mo., and the Waltham, Mass., office of QinetiQ North America's Technology Solutions Group. All three companies involved in the project are members of JVIC.The program is designed to meet a stated Department of Defense need for a tactical chemical and biological defense as well as an intelligent network that can communicate and direct sensors so they provide real-time notice of a threat."

Poisonous gas munitions to remain off Helgoland

Ninety tonnes of poisonous gas shells from World War II sunken off the coast of the North

Sea island Helgoland will not be raised out of safety concerns, authorities in the state of Schleswig-Holstein said on Thursday. Experts have decided that removing the artillery shells would be more dangerous than allowing them to remain at the bottom of the ocean, the state's Deputy Interior Minister Volker Dornquast said. He said the shells, which are full of toxic nerve agent tabun, would likely explode from the change in pressure if they surface and suggested a fishing ban and a reduction of naval exercises in the area instead. “It sounds paradoxical, but the grenades would be really dangerous if we tried to remove them,” he said. The British military apparently ordered that the weapons be sunk some four kilometres south of the island in 1949. They now lie between 45 and 55 metres below the surface and contain almost 12 tonnes of tabun. Some 60 years after the end of World War II they are said to be in “problematic state,” but pose no concrete danger if they remain in the water, Dornquast said.

Experts believe that most of the tabun, which is water soluble, has likely washed out of the grenades over the years, he added.

Destroying Chemical Weapons: US Army Reviews Technology

To destroy chemical weapons, the US Army can't just throw them in an incinerator. They

have to be destroyed carefully so that no harmful chemicals are released into the air or water supplies. In 2009, the US Army, working with the National Research Council (NRC), tested 4 technologies – 3 private-vendor systems and 1 Army-developed explosive destruction system

(EDS) – to destroy chemical weapons. Tests were conducted at the Blue Grass Army Depot in Kentucky and the Pueblo Chemical Depot in Colorado. The developers of one of the systems tested – US-based Versar and Japan's Kobe Steel – announced [pdf] Feb 9/10 that they received a $13 million subcontract from URS Corp. to deliver their Detonation in a Vacuum Assisted Chamber (DAVINCH) system to the Deseret Chemical Depot in Tooele, UT for chemical weapons destruction. In addition to supplying the system, Versar will provide project management at the depot. The Army testing revealed some interesting facts about the DAVINCH system… The 3 private-vendor systems tested by Army and the NRC were the DAVINCH system developed by Kobe Steel and Versar, the transportable detonation chamber T-60 model supplied by US-based CH2M Hill, and the static detonation chamber SDC2000 model from Sweden's Dynasafe.

A report prepared on the testing by the Board on Army Science and Technology describes how each system works:

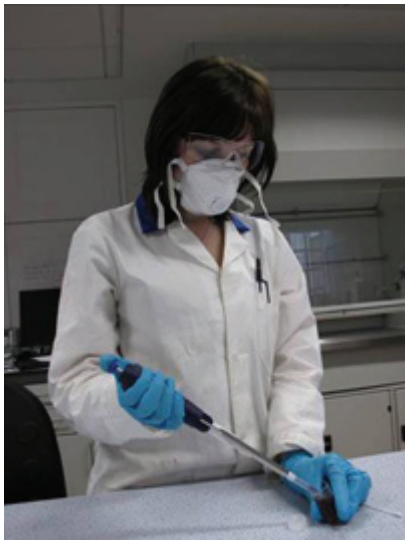
DAVINCH: "The process uses a detonation chamber in which chemical munitions are destroyed when donor charges surrounding the munitions are detonated. Offgases are produced that require secondary treatment….The offgases resulting from agent destruction in the DAVINCH vessel are filtered to remove particulates and, with oxygen from an external supply, are pumped into the cold plasma oxidizer, which oxidizes CO to CO2. Condensate water is then recovered from the exhaust gas; the gas is passed through activated carbon and exhausted to the atmosphere."
T-60: "The TC-60 has three main components: a detonation chamber, an expansion chamber, and an emissions control system. A munition wrapped in explosive is mounted in the detonation chamber. The floor of the chamber is covered with pea gravel, which absorbs some of the blast energy. Bags containing water are suspended near the projectile to help absorb blast energy and to produce steam, which reacts with agent vapors. Oxygen is added when destroying munitions containing mustard agent. After the explosive is detonated, the gases are vented to an expansion chamber, then to the emissions control system. The offgas treatment system includes a reactive-bed ceramic filter to remove acidic gases and to collect particulates such as soot and dust from the pea gravel. A catalytic oxidation (CATOX) unit oxidizes hydrogen, carbon monoxide, and organic vapors from the gas stream before the stream is vented through a carbon adsorption bed and released to the atmosphere."

SDC2000: "The detonation chamber is a nearly spherical, armored, high-alloy stainless steel vessel. The vessel is double-walled, with the inner wall considered to be armored….Chemical munitions are placed in a cardboard box or carrier, which is transported to the top of the system. The boxed munitions are fed into the detonation chamber through two sequential loading chambers. The boxed munitions are dropped onto a heated (550°C-600°C) shrapnel (scrap) bed at the bottom of the detonation chamber, resulting in deflagration, detonation, or burning of the munition's explosive fill. The chemical agent in the munitions is destroyed by the shock wave from the detonation or by decomposition due to the high heat in the chamber. The offgas treatment system includes a cyclone for removal of large particulates and a flameless thermal oxidizer that converts carbon monoxide and hydrogen to carbon dioxide and water. This is followed by a fast quench system to minimize dioxin and furan formation, acidic and basic (caustic) scrubbers, and an absorber/particulate filter system that uses Sorbalite, a mixture of calcium oxides and carbonates with activated carbon."

Army EDS: "The U.S. Army's EDSs are trailer-mounted mobile systems originally intended to destroy explosively configured chemical munitions that are deemed unsafe to transport. The system has been used to destroy chemical munitions with or without explosive components. At the heart of the EDS system is an explosion containment vessel. The EDS Phase 2 (EDS-2) containment vessel is designed to handle munitions containing up to 4.8 lb TNT-equivalent of explosives. The EDS uses explosive shaped charges to access the agent cavity and to destroy any energetics in the munition. After detonation of the shaped charges, reagents appropriate to the agent to be neutralized are pumped into the vessel and the vessel contents are mixed until the treatment goal has been attained. After the concentration of chemical agent falls below the treatment goal, as determined by sampling the contents of the chamber, the liquid waste solution is transferred out of the chamber into a waste drum. The drummed EDS liquid waste is normally treated further at a commercial hazardous waste treatment, storage, and disposal facility."

For destruction of 155-mm mustard gas munitions, the report determined that the DAVINCH and SDC2000 were the most effective. For destruction of M55 rocket motors, the report found that the T-60 was most effective.

New Technology Detects Chemical Weapons in Seconds



Scientists at Queen's University Belfast are developing new sensors to detect chemical agents and illegal drugs which will help in the fight against the threat of terrorist attacks. The devices will use special gel pads to 'swipe' an individual or crime scene to gather a sample which is then analysed by a scanning instrument that can detect the presence of chemicals within seconds. This will allow better, faster decisions to be made in response to terrorist threats. The scanning instrument will use Raman spectroscopy which involves shining a laser beam onto the suspected sample and measuring the energy of light that scatters from it to determine what chemical compound is present. It is so sophisticated it can measure particles of a miniscule scale making detection faster and more accurate. Normally this type of spectroscopy is not sensitive enough to detect low concentrations of chemicals, so here the sample is mixed with nanoscale silver particles which amplify the signals of compounds allowing even the smallest trace to be detected. Dr Steven Bell from Queen's University Belfast who is leading the research said: "Although we are still in the middle of the project we have finished much of the preliminary work and are now at the exciting stage where we put the various strands together to produce the integrated sensor device. For the future, we hope to be able to capitalise on this research and expand the range of chemicals and drugs which these sensors are able to detect." It is hoped the new sensors will also be the basis for developing 'breathalyzer' instruments that could be of particular use for roadside drugs testing in much the same way as the police take breathalyzer samples to detect alcohol. At present, police officers are only able to use a Field Impairment Test to determine if a person is driving under the influence of drugs. The accuracy of this method has been questioned because of concerns that it is easy to cheat. To ensure the technology is relevant, senior staff members from FSNI (Forensic Science Northern Ireland) will give significant input into the operational aspects of the technology and give feedback as to how it might be used in practice by the wider user community. Stan Brown, Chief Executive of FSNI said: "We consider the work being carried out by researchers at Queen's University extremely important and potentially very useful in driving forward the effectiveness, efficiency and speed of forensic science practice. The combination of leading edge research and hands-on experience of FSNI's practitioners has already proven very fruitful and is likely to lead to significant developments in forensic methodologies across a range of specialisms." In the future this technology could have a number of important applications and according to Dr Bell: "There are numerous areas, from medical diagnostics to environmental monitoring, where the ability to use simple field tests to detect traces of important indicator compounds would be invaluable."

Smiths Detection, AeroVironment and US Army Collaborate on Chemical Agent-Detecting UAV

Smiths Detection today announces the successful creation and demonstration of an unmanned aircraft chemical detection and identification system capable of warning troops against chemical warfare agents. The detection and identification system, able to fit in the interchangeable nose cone of a Raven® UAV, is a result of the collaborative efforts between Smiths Detection, AeroVironment, Inc. (AV) (Nasdaq: AVAV), the U.S. Army Edgewood Chemical Biological Center and other U.S. Department of Defense (DoD) laboratories. To provide safe and effective standoff detection and identification capability of chemical hazardous events, the sophisticated chemical sensor nose cone was developed specifically to

fit into AV's RQ-11B Raven as part of a DoD program funded by the Joint Program Manager Nuclear, Biological and Chemical Contamination Avoidance, the Defense Threat Reduction Agency, and the U.S. Army Product Manager, Small Unmanned Aircraft Systems. Mal Maginnis, President, Global Military and Emergency Response for Smiths Detection, said: "We have all leveraged our core strengths to provide the DoD with a unique, valuable solution for remote chemical detection and are delighted with the results of this outstanding effort which can enable troops to avoid life-threatening situations." In a successful demonstration at the U.S. Army's Dugway Proving Grounds, a chemical sensor-equipped Raven was flown into a chemical cloud and successfully detected and identified the chemical, tracking the chemical vapor plume autonomously. Thousands of Raven air vehicles have been deployed and are in use by U.S. and several allied military forces. John Grabowsky, Executive Vice President and General Manager, AV Unmanned Aircraft Systems, said: "A 'plug and play' chemical sensor payload for Raven represents a new capability that could help war fighters operate more safely and effectively, and could assist in a variety of disaster response scenarios. As the most widely deployed unmanned aircraft system, adding chemical sensing to the Raven system's existing streaming color and infrared video payloads would expand the utility and value of this important solution to our customers." The chemical sensor Smiths Detection developed for the Raven is based on its Lightweight Chemical Detector (LCD), the commercial variant of the DoD's Joint Chemical Agent Detector (JCAD) program. The LCD has been radically modified into a new cylindrical form factor unit known as the Chemical Sensor Module (CSM), yet it retains all of the critical chemical detection and identification capabilities of the LCD. Because of the size and weight, the CSM can be integrated into AV's Raven Small Unmanned Aircraft System (SUAS) to make it capable of automatic detection, identification and quantification of dangerous chemical warfare agents. Advanced control algorithms developed by DoD labs allow the Raven to operate in a semi-autonomous mode analyzing the data collected by the CSM and determining chemical cloud size, direction and density in real-time.

China detects deadly nerve gas at border with NKorea: report

China has detected deadly nerve gas at its border with North Korea and suspects an accidental release inside the secretive state, a Japanese news report said Friday. The Chinese military is strengthening its surveillance activities after detecting the highly virulent sarin gas in November last year and in February in Liaoning province, the Asahi Shimbun newspaper reported, citing anonymous sources from the Chinese military. Sarin gas, which was developed in Germany before World War I, was used in the deadly 1995 nerve gas attack on the Tokyo subway by a doomsday cult. The Chinese special operations forces found 0.015-0.03 microgrammes of the gas per cubic metre when they were conducting regular surveys while there were winds from the direction of North Korea, the report said. China suspects that there were some experiments or accidents in its neighbouring country, it said.

British Intelligence Halted Al-Qaeda Bioweapons Acquisition Attempt

A new book says the British domestic intelligence agency MI5 in 2000 inadvertently prevented an effort by the terrorist organization al-Qaeda to acquire material that could be used in acts of bioterrorism, the Associated Press reported yesterday. Agents discovered that Pakistani microbiologist Rauf Ahmad was carrying suspect materials and equipment in his luggage while in the United Kingdom for a conference, according to "The Defense of the Realm," a history of MI5 by Cambridge University historian Christopher Andrew. Ahmad had made contact with al-Qaeda deputy chief Ayman al-Zawahiri, according to U.S. intelligence officials. Extremists still hope to use a weapon of mass destruction to cause large numbers of deaths, Andrew said. "It is not a question of if, it is a question of when such weapons will be used," he said. The 100-year-old British service was "slow to see the coming

menace of Islamist terrorism," and appeared surprised by the U.S. focus on al-Qaeda leader Osama bin Laden in the 1990s, according to Andrew. It was also not able to prevent the July 2005 bombings of the London transit system that killed 52 people. However, MI5 has headed off a number of significant terrorist plots that targeted the United Kingdom, such as the planned use of liquid explosives to destroy passenger aircraft heading to North America. British intelligence officials think that "though a major Islamist terrorist attack would remain a serious danger for the foreseeable future, the observable threat had stopped increasing," according to the book. Added Andrew: "It is too early to tell whether the 'chilling effect' is a short-term fluctuation or a long-term trend".

Nanotechnology sensor detects living bacteria at ultralow concentrations

A pathogen is an organism (bacterium, virus, parasite) that causes disease in another organism. According to data from the U.S. Centers for Disease Control and Prevention (CDC), known pathogens account for an estimated 14 million illnesses, 60,000 hospitalizations, and 1,800 deaths each year in the United States. In addition to the food supply, microbacterial infections are a major issue in hospitals. Other CDC data estimates that infections acquired in hospitals alone affect approximately 2 million persons annually. In the U.S., between 44,000 and 98,000 people die every year from infections they picked up in hospitals. The numbers for Europe are equally scary. Add to that the potential for terrorist attacks with pathogen-based bioweapons and it becomes clear that the development of fast and reliable biosensors is a major issue. The problem today is that analytical tools for the rapid detection of pathogens tend to be slow. Traditionally, identifying a pathogen such as E. coli, Salmonella or Listeria requires cell culturing, which takes time – time that often means more contamination and illnesses or even deaths. Here is an example from the FDA's recommended method for determining E. coli: Weigh 50 g food into sterile high-speed blender jar. Add 450 mL of Butterfield's phosphate-buffered water and blend for 2 min. Prepare decimal dilutions with sterile Butterfield's phosphate diluent. Number of dilutions to be prepared depends on anticipated coliform density. Shake all suspensions 25 times in 30 cm arc or vortex mix for 7 s. Do not use pipets to deliver <10% of their total volume. Transfer 1 mL portions to 3 LST tubes for each dilution for at least 3 consecutive dilutions. Hold pipet at angle so that its lower edge rests against the tube. Let pipet drain 2-3 s. Not more than 15 min should elapse from time the sample is blended until all dilutions are inoculated in appropriate media. Incubate LST tubes at 35°C. Examine tubes and record reactions at 24 ± 2 h for gas, i.e., displacement of medium in fermentation vial or effervescence when tubes are gently agitated. Re-incubate gas-negative tubes for an additional 24 h and examine and record reactions again at 48 ± 2 h. Perform confirmed test on all presumptive positive tubes (which takes another 2 days).

Researchers have managed to develop much faster detection systems based on nanotechnology. The fastest assays however, those that have reaction times in the minutes range, require pretreatment steps to condition the test samples and to perform cell lysis to extract the suitable target DNA. A major drawback which complicates testing considerably. In their effort to develop a fast, sensitive, selective, inexpensive, and easy-to-use method for detecting and quantifying pathogenic bacterial cells, researchers in Spain have now demonstrated a carbon nanotube based potentiometric

biosensor for selectively detecting one single colony-forming unit of the bacterium Salmonella Typhi in close to real time. An aptamer attached to an electrode coated with single-walled carbon nanotubes interacts selectively with bacteria. The resulting electrochemical response is highly accurate and reproducible and starts at ultralow bacteria concentrations, providing a simple, selective method for pathogen detection. (Reprinted with permission from Wiley-VCH Verlag) According to F. Xavier Rius, a professor at the Rovira i Virgili University in Tarragona, Spain, who heads the Chemometrics, Qualimetrics and Nanosensors Group, "the most important strength of this biosensor is that simple positive/negative tests can be carried out in real zero-tolerance conditions and without cross reaction with other types of bacteria. The ease with which measurements are taken in potentiometric analysis opens the door to greater simplicity in microbiological analysis." To build their sensor, the Spanish team linked carboxylated single-walled carbon nanotubes (SWCNT) to an aptamer. Aptamers are not only highly suitable receptors for the selective and high-proficiency detection of a wide range of molecular targets, including bacteria, they have also shown to self-assemble on carbon nanotubes. This hybrid nanomaterials has already been demonstrated as effective nanobiosensors. The hybrid material aptamer-SWCNT acts as both the sensing and the transducing layer of the biosensor. The presence of target bacteria promotes a conformational change in the aptamer that separates the phosphate groups, largely ionized at pH 7.4, from the SWCNT sidewalls, inducing a charge change to the SWCNT and the subsequent change of the recorded potential. Ruiz' team also found that their biosensors show a high degree of electivity, i.e. no response was shown for bacteria other than the target bacterium Salmonella Typhi. It appears that this new biosensor makes the detection of pathogens as easy as measuring the pH value. Ruiz and team have reported their findings in a recent issue of Angewandte Chemie International Edition

Darpa Looks to Upgrade Bio-Threat Detectors

Infectious microorganisms are on the rise, and the Pentagon's on a mad dash for better detection, treatment and even all-out prevention. With a need for turbocharged response, it's

no surprise that Darpa, the military's mad-science division, is playing a major role in combating bioterror attacks and natural threats like H1N1. Now the agency's requesting proposals for a device that would enable faster, more accurate detection of a broad range of biological agents. The Antibody Technology Program hopes to create a biosensor that would identify viral and bacterial threats, and do so using a natural first-line of defense: human antibodies. This isn't the first time Darpa's asked for better, more versatile microorganism detectors. In 2002, they launched the Biosensors Technology Program, to figure out the fastest, most effective way to detect a wide array of bio-agents with a single device. Among the contenders were mass spectrometry, a technique to separate and identify molecules based on mass, and hand-held nucleic acid sensors, which would analyze the DNA and RNA of potentially dangerous substances. According to Darpa's new solicitation, antibody biosensors offered the most reliable detection, across the broadest range of bio-agents. And now, they want to make the sensors even better. Darpa's asking for proposals that would address the two downsides of antibody-based biosensors. Antibody proteins are fragile, so they're unable to withstand extreme

temperatures or survive longer than a few weeks in storage. That's hardly practical for civilian medical centers, let alone a war-zone. Darpa wants the new biosensors to be as resilient as possible. They're asking for molecular manipulation of the antibodies, so that the biosensors will be stable for five years, and work at temperatures that range from 25 to 70 degrees Celsius (77 to a sweltering 158 degrees Fahrenheit). When they haven't been tinkered with in a lab, antibodies are produced by the body in reaction to a foreign viral or bacterial threat, called an antigen. A particular antibody can only bind to a single antigen, but science has already created antibodies that can bind to several different ones. Now, Darpa wants them to have even an more diverse "affinity level": the ability to bind to a potentially endless array of viral or bacterial antigens. The tip of an antibody is extremely variable, which is why different antibodies attach to different antigens. It's this binding that's used by biosensors to identify various microorganisms, and distinguish between them. Darpa wants to control, or "fine-tune" antibody affinity, so that one "master antibody" can bind with millions of antigens. Darpa's request isn't specific about how they expect the master antibody, and it's accompanying biosensor, to be created. But artificial antibodies have been in-the-making for years, offer a cheaper, more easily manipulated platform, and are becoming more reliable thanks to new technology. Plus, researchers at Portland State University have already manufactured a hand-held antibody biosensor, so chances are good that the detection of biothreats will look cooler than a throat swab, too.

Darpa Finds a Flu-Fighter

Early in the decade, Darpa, the Pentagon's blue-sky research arm, started pouring money into an effort to make troops stronger, smarter, and tougher to kill. Along the way, Darpa-backed scientists may have just discovered a way to beat back to flu. It's the latest turn in a Pentagon program that has already gone in a number of counterintuitive directions. With Darpa funds, biochemist Mark Roth turned rodents into virtual zombies. Biologist Craig Heller created a "glove" that lets wearers endure extreme heat, and cold. Veterinarian Michael Davis examined how sled dogs' amazing endurance might be translated into humans. Microbiologists at the Agricultural Research Service (ARS) sorted through swine manure, to figure out how pigs digest what humans usually can't: cellulose, the main fibrous part of plants. Geneticist Jasper Rine investigated how "genetic variation" might affect troops' "peak and sustainable performance levels." Oxford University biochemists looked for ways to take mitochondria — the body's powerhouses, which ordinarily turn sugars into energy — and put them on the equivalent of the Atkins diet, instead. University of South Carolina and Clemson University researchers, funded by Darpa, gave mice quercetin, a naturally occurring substance found in fruits and vegetables, and discovered that the rodents were "less likely to contract the flu," according to a statement from the American Physiological Society. "The study also found that stressful exercise increased the susceptibility of mice to the flu, but quercetin canceled out that negative effect." If quercetin can do the same in humans, soldiers could be able to go through grueling training regimes or battlefield conditions, with a reduced chance of getting sick. Mice tend to get upper respiratory illnesses when they exercise a bunch. And that was

certainly the case during the experiments from the South Carolina and Clemson team, lead by physiologist J. Mark Davis. The scientists put the rodents on treadmills, and exposed 'em to a common flu virus, H1N1. The mice that exercised had a 91% chance of developing the flu, versus a 63% chance for the control group. Those mice also got sick much sooner — 6.9 days versus 12.4 days. But Davis' crew gave some of the rodents quercetin. The researchers noticed that "mice that exercised and took quercetin had nearly the same rate of illness as those that did not exercise. In other words, quercetin canceled out the negative effect of stressful exercise," the American Physiological Society notes. Quercetin also "had protective effects for the mice that did not exercise." Darpa has also repeatedly honed in on quercetin, during its peak soldier performance program. Pathologist Lan Bo Chen searched for something that would boost the overall production of mitochondria, regardless of what the cellular powerhouses consumed. Eventually, he blended quercetin with a B-vitamin cocktail; it sent mitochondria production skyrocketing in lab rats, tripling the animals' endurance. Then, the drink was given to high-performance cyclists in a series of trials at Pepperdine University. The results weren't nearly as dramatic – just an average three percent improvement in a 30 kilometer ride. But considering these athletes' races are often decided by tenths of a second, the study was considered a major breakthrough.

Yellowcake instead of drugs, Iraq flashback to Vietnam

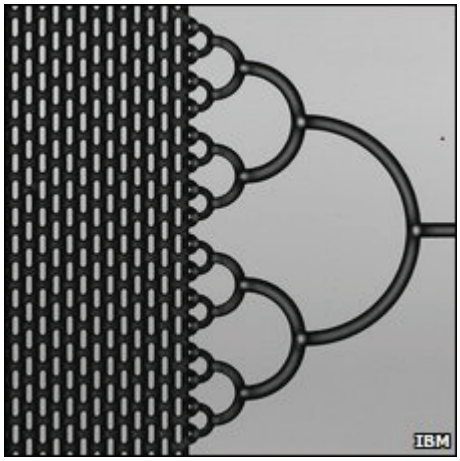
During the Vietnam War, secret US operations transported drugs in the body bags of US soldiers. During the Iraq War, the US secretly transported Iraq's uranium to a private company in Canada, Cameco. It is the same uranium mining company that Lakotas are fighting in their territory in Nebraska and First Nations are battling for poisoning their land and water in Canada. The US secretly transferred 500 tons of uranium out of Iraq to Cameco.

The US spent 70 million taxpayer dollars doing this in the summer of 2008. During the Vietnam War, the US smuggled drugs out of Vietnam in body bags of soldiers, a fact exposed by CIA agents at the time. Iraq's yellowcake was transferred from Tuwaitha, 12 miles south of Baghdad and then to Diego Garcia, a British territory in the Indian Ocean where the United Kingdom and the United States operate a joint military base. Finally it was transported to Montreal. "While yellowcake alone is not considered potent enough for a so-called 'dirty bomb' — a conventional explosive that disperses radioactive material — it could stir widespread panic if incorporated in a blast. Yellowcake also can be enriched for use in reactors and, at higher levels, nuclear weapons using sophisticated equipment," according to MSNBC. The cleanup in Iraq was by Iraqis trained at Chernobyl. Why? The media seems to have forgotten about this secret shipment of Iraq's yellowcake. But Cameco will not go away. Cameco is exploiting and poisoning Indigenous lands with uranium mining and gold mining, from Saskatchewan to Wyoming and Kazakhstan. Currently, Lakotas are fighting Cameco in court in Nebraska over uranium mining. The question remains why the majority of gold, copper and uranium mining corporations that are exploiting and assassinating Indigenous Peoples around the globe are based in Canada.

Tiny chip could diagnose disease

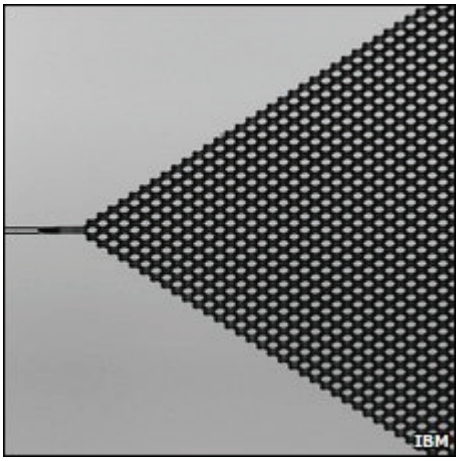
Researchers have demonstrated a tiny chip based on silicon that could be used to diagnose dozens of diseases. A tiny drop of blood is drawn through the chip, where disease markers are caught and show up under light. The device uses the tendency of a fluid to travel through small channels under its own force, instead of using pumps. The design is simpler, requires less blood be taken, and works more quickly than existing "lab on a chip" designs, the team

report in Lab on a Chip. It has a flexible design so that it could be used for a wide range of diagnostics. Much research in recent years has focused on the chemical and medical possibilities of so-called microfluidic devices at the heart of lab-on-a-chip designs. These microfluidics contain between dozens and thousands of tiny channels through which fluids can flow, and as micro-manufacturing methods have advanced, so has the potential complexity of microfluidics. Now, scientists at IBM's research labs in Zurich have developed a cheap lab-on-a-chip that has the potential to diagnose dozens of diseases.



Bind and shine

The device relies on an array of antibody molecules that are designed to latch on to the protein-based molecular markers of disease in blood. The antibodies are chemically connected to molecules that emit light of a specific colour when illuminated - but only when they have bound to the disease markers. "There are devices that have been developed in microfluidics to do analysis of proteins, but most of them use active pumping and electrical components," said Luc Gervais, a co-author on the study. "They're very complex systems; this makes them less easy to use by non-trained personnel - and it makes them a lot more expensive to manufacture," Dr Gervais told BBC News. Instead, the new device exploits capillary action, the tendency of fluids to climb through narrow channels - the same phenomenon that drives water into a sponge placed on a wet surface. The speed with which blood is drawn through the chip can be controlled by the design of the micro-channels on the device. Those channels can be designed with incredible precision on a silicon chip - something with which IBM has significant experience. The microchannel-patterned chip is then sealed with a special polymer called polydimethylsiloxane, to which the "detector" antibodies easily bond. Different antibodies can be placed in a number of distinct channels, making it possible to diagnose a range of different diseases simultaneously. Such wide-ranging studies can be done in large analysers, found in the central laboratories of hospitals. "Typically you'll take a couple of millilitres of blood, send it to the central lab and it can take up to an hour or even more to get the results," Dr Gervais said. "In our case you can get a quantitative analysis of the patient's blood within just a few minutes at the bedside of the patient." What is more, it can be done with just a few microlitres of blood - a thousand times less - an amount that could be collected with a prick of a finger instead of a syringe. While the approach will make diagnosis cheaper, co-author Emmanuel Delamarche said the key aspect of the approach is its speed. "We are giving back precious minutes to doctors so they can make informed and accurate decisions right at the time they need them most to save lives."



Russian Site Finishes Disposal of Sarin Nerve Agent

A Russian chemical weapons disposal site has finished elimination of 232.6 metric tons of the nerve agent sarin, Interfax reported yesterday. The Maradykovsky facility in the Kirov Region destroyed 4,866 munitions filled with the chemical warfare material. Progress has also been made in preparations to begin disarmament operations for a cache of munitions filled with a mixture of mustard and lewisite blister agents. There are 150 metric tons of the

material waiting for disposal. "The facility has completed the construction of a line for the destruction of mustard-lewisite mixture," said the Kirov Region government in a statement. "In late November, hook-up and commissioning work will start at the line, testing the technology for destroying this toxic substance." Full chemical weapons destruction at Maradykovsky is expected to be finished by 2012.

Cell phone sensor aims to crowd source chemical attack information

NASA scientists have developed a new chemical sensor that allows iPhones to identify low airborne concentrations of chemicals including ammonia, chlorine gas and methane. The

postage-stamp sized chemical sensor was developed by Jing Li, a Physical Scientist at NASA's Ames Research Center in California. The project was developed with other researchers as part of Homeland Security's Cell-All program, which was created to put more mobile sensors in the hands of every cell phone user. The sensor works by using a puff from a sample jet that helps sense any airborne chemicals. Information from the sensor is then processed by a silicon chip with 16nano-sensors and then sent to another phone or computer through any Wi-Fi or telecom network. The sensor, it is hoped, could be used to alert first responders to the presence of a chemical agent stemming from an accident or attack. The device would work even if the cell phone user loses consciousness from the chemical's presence. The Department of Homeland Security's program aims to integrate isotope and biological GPS-coupled-sensors into cell phones to monitor chemical, biological or radiological environmental conditions and report incidents as they occur. The proposed Cell-All sensors would not only alert the phone's user to the presence of chemicals but, through crowd sourcing, transmit information about the chemicals to first responders and federal emergency operations center.

New bioweapon detector

Universal Detection Technology has demonstrated its latest development in bioweapon technology at the 2009 Milipol Conference, a five-agent biodetection handheld assay. "There are bio-weapon monitoring tools immediately available for public and private entities, easy to implement and cost effective," Jacques Tizabi, CEO of Universal Detection Technology, said. "Universal Detection Technology's biodetection kits are the first step in meeting the needs of bioterrorism prevention and planning." UNDT, which develops early-warning monitoring technologies to protect against bioterrorism and other infectious health threats, showcased its TS-10-5 biodetector, which boasts no setup time, no decontamination requirements and no false negatives or false positives. Earlier this year, UNDT's biodetection kits were certified by the U.S. Department of Homeland Security as an "Approved Product for Homeland Security." The kits are currently the only hand-held assay designed to both detect and identify up to five separate threats with only one sample. The kits provide first responders with an effective tool for rapid onsite detection for anthrax, ricin, botulinum toxin, plague and Staphylococcal Enterotoxin B. Detection time by the kits takes less than three minutes. "Bio-weapon detection should be a top priority for all public entities, because for terrorists, [bio-weapons] can be purchased or engineered at relatively low costs, can induce mass casualties and are oftentimes undetected by on-the-ground law enforcement," Tizabi said.

Biomedical scientists develop new anti-toxin

A number of people with biomedical science jobs have developed a new anti-toxin. Researchers at the Defence Science and Technology Laboratory (DSTL) in Wiltshire have been working on a substance to combat the effects of ricin poisoning. Speaking to the BBC, the institution's Dr Jane Holley revealed they have succeeded in coming up with the first anti-toxin that has gone into production. She commented: "In the past there has been lots of research carried out using different methods." However, never before has this been translated into production techniques, the expert added. The principal scientist in biomedical sciences at DSTL - which is an agency of the Ministry of Defence and aims to supply impartial, scientific and technical research to the government - said the product should be available within the next couple of years. Ricin, which is extracted from castor beans, is considered a threat by security experts as it has the potential to be used in a terrorist attack.

Wearable Sensors

GE Global Research, the technology development arm of General Electric Co., said Tuesday it will get $2 million federal grant to develop wearable sensors that alert people to chemical weapons and diseases. Radio-frequency identification sensors are commonly used to track materials, including in baggage at airports. GE's sensors would combine the tracking capability with gas sensors that could detect harmful chemicals in the air. Because they can be smaller than a penny, GE says the sensors could be integrated into identification badges or serve as part of warning systems. GE said it also will develop sensors that can analyze breath and pick up early signs of diseases such as diabetes and cancer. The grant is from the National Institute of Environmental Health Sciences, which is part of the National Institutes of Health.

Hidden Threat From al-Qaeda Sleeper Cells – UK

Security services fear Al-Qaeda terrorists are exploiting loose visa and immigration rules to enter Britain. Counter-terrorism police and Whitehall officials believe dozens of extremists could have arrived here by posing as students or legitimate visitors. They are concerned both by the relatively lax checks that are made on the visitors before they arrive and by the ease with which they can outstay their visas without anyone noticing. As many as 13,000 visa applicants may have entered the country from Pakistan in a seven month period since October last year without any checks on their supporting documentation. The security services fear that because most do not mix with home grown terrorists, they are able to operate under the intelligence radar, acting as sleeper cells until ready to launch attacks in Britain. Every year around 100,000 visitors arrive in Britain from Pakistan alone, which has been described by the Prime Minister as being part of a “crucible of terror” along with Afghanistan. They are supposed to be checked by Home Office visa staff working in Abu Dhabi in the United Arab Emirates. But according to an official watchdog, the Independent Monitor for Entry Clearance, many visa officers do not have “enough time to go through applications carefully”.

Living Weapons tackles biowarfare

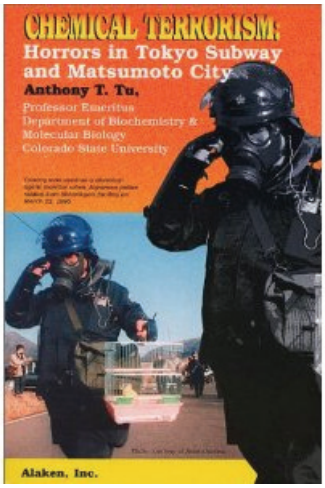
In the age of industrial microbiology, aerobiology led to the advent of large-scale distribution and implementation of bioweapons. In the way of dissemination, Koblentz discusses two types of munitions: point source, which would involve explosives or gas releasing agents from a stationary location, and line source, which would involve the release of biological agents from a moving source - usually perpendicular to the wind. As the U.S. developed nuclear weapons, however, the desire to employ biological agents as weapons of mass destruction decreased significantly. Finally, biotechnology has affected the use of bioweapons. Genetic engineering has enabled the creation of more virulent pathogens and toxins. Fortunately, there is some hope for using biotechnology defensively. For example, new breakthroughs will allow a greater variety of vaccines to be created and distributed. Koblentz proceeds to discuss why bioweapons are uniquely challenging to security. He points out that biological weapons favor the attacker in a number of ways. They are extremely potent and, for a low cost, they have a large destructive capability. For example, the cost of the 2001 anthrax scare was approximately $2,500. The total cost of the state's response, though, was upwards of $6 billion. Additionally, bioweapons are easy to secretly develop and difficult to defend against. For these reasons, controlling bioweapons is a very difficult task. Verification of the existence of weapons, one of the key principles of international arms control, is uniquely hard when dealing with biological weapons, because biotechnology is mutliuse in nature meaning that it can be applied to both civilian and military programs. Additionally, since civilian programs have an incentive to hide their technology - for national security or to protect proprietary information - it is difficult to determine malevolent activity. Difficulties in verification, combined with intense secrecy, can lead to intelligence failures. The author examines Operation Iraqi Freedom, which was justified under the assumption that Iraq was pursuing offensive biological weapons capability. As it turns out, this was grossly inaccurate.

ΣΣ: Με ιδιαίτερη χαρά πληροφορήθηκα τη βράβευση του εξαίρετου επιστήμονα Καθηγητού Antony Tu από τον Ιάπωνα Αυτοκράτορα. Η συνεργασία μαζί του είναι πάντα διδακτική και εποικοδομητική και η μετάφραση του βιβλίου του αποτελεί ιδιαίτερη τιμή!

Colorado State Professor Honored by Japan for Help Solving '90s Sarin Gas Attacks

FORT COLLINS - Emeritus Professor Anthony Tu's expertise about a deadly nerve gas helped the Japanese identify and catch suspects in the sarin gas attacks in the 1990s – assistance that has now earned him one of the nation's highest honors. On Nov. 9, the Japanese Emperor bestowed the Colorado State University emeritus professor with the distinction of The Order of the Rising Sun, Gold Rays with Neck Ribbon. Tu, 79, was one of 61 individuals including 10 U.S. citizens to receive the honor this fall. Past recipients have included some of the world's most prominent academics, politicians and authors. Actor Clint Eastwood accepted the same medal earlier this year for his movies on the Battle of Iwo Jima. "This is a well-deserved honor for Professor Tu, who has been devoted to both basic and applied science for his entire career," said Rick Miranda, interim provost and executive vice president at Colorado State University. "This is indicative of the impact our professors are having around the globe." "This prestigious award recognizes the contributions of basic science to some truly practical and timely issues on the world stage," said Shing Ho, chair of the Department of Biochemistry at Colorado State. Tu, a biochemistry professor whose research focused on snake venom, published papers in Japan on

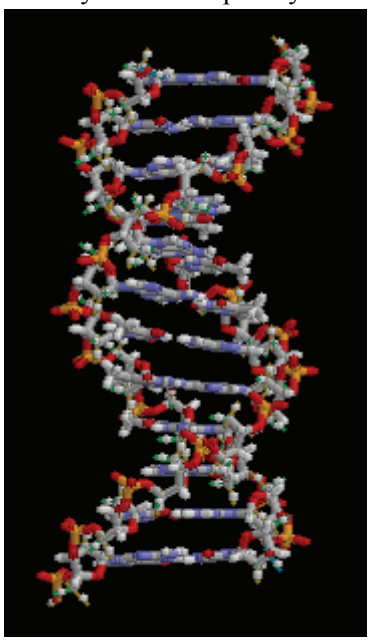
chemical warfare just before the Matsumoto attack in 1994 that killed seven people and poisoned 500 others. Police asked Tu for help with the case and the ensuing nerve gas attack



on the Tokyo subway in 1995 that killed 12 and injured about 3,800 more. Japanese officials used Tu's assistance to analyze the sarin and its byproducts to identify the manufacturing facility where the religious sect Aum Shinrikyo produced 70 tons of the deadly nerve gas. Tu's knowledge of chemicals produced from the degradation of sarin in soils was instrumental in linking Aum Shinrikyo definitively with the manufacture and use of sarin, evidence that helped convict the sect's leader, Shoko Asahara, who was later sentenced to be hanged. Tu wrote a book about the experience in 2002 titled "***Chemical Terrorism: Horrors in Tokyo Subway and Matsumoto City***." He has received numerous awards for his efforts in Japan including a medal of honor from the National Institute of Police Science and the certificate of Honorary Membership from the Japanese Society of Forensic Toxicology. He currently is the only foreign member of this organization.

DNA Sensors Getting Ready to Sniff Out Terrorist Attacks

Sensors often are the first line of defense against a chemical or biological attack, but up until now they've often relied on lasers to detect the minute quantities of substances needed to identify an attack quickly. That's made them expensive to build and difficult to maintain.



Now, researchers at the MITRE Corporation are developing genetically engineered bio-sensors, and while they're still a few years from the marketplace, these sensors promise to be even more accurate than today's detection devices - and they'll cost far less. That's because in the micro and nano-scale realms in which sensors operate, it's a lot easier to replicate and test DNA strands than it is to assemble mechanical or electronic parts. "Mass producing low-cost sensors will allow thousands of them to be deployed in large public areas that are subject to terrorist attack," said John Dileo who leads the MITRE effort in synthetic biology.

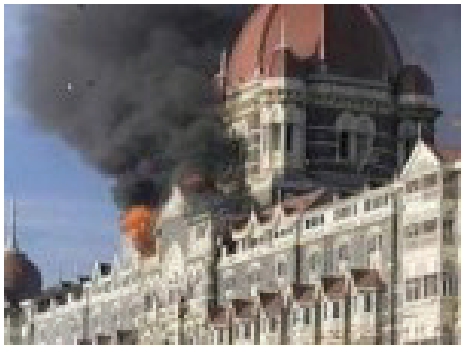
Bio-sensors could also be continually replaced with advanced versions designed to spot new threats as they emerge. Just as the human immune system can fine tune itself to detect any number of diseases, biologists working in this area believe that as they better understand how to assemble synthetic strands of DNA, they'll be able to design bio-sensors able to spot far more harmful substances than sensors employed today. Adding yet another protective layer, the sensors can be networked and overseen by intelligent computer algorithms that can quickly pinpoint the source of an attack, while also monitoring and predicting its spread.

MITRE is collaborating with an academic group led by Jean Peccoud, associate professor at the Virginia Bioinformatics Institute at Virginia Tech. They believe genetically engineered cells could function as intelligent threat detection devices - mini computers, if you will. "Cells possess innate abilities that make them ideal for environmental sensing applications," they explain in a paper entitled Co-Design in Synthetic Biology: A System-Level Analysis of the Development of an Environmental Sensing Device to be presented in January 2010 at the Pacific Symposium on Biocomputing. Specifically, cells are inherently able to detect small concentrations (parts per billion) of chemicals (or combinations of chemicals) in their environment and respond to it, usually with an amplified signal." Genetically tweaked in just

the right way, cells can even function in a sequential manner that's akin to how a computer linked to a mechanical sensor might operate. Peccoud's group identified three tasks their synthetic cell would need to perform in order to be an effective threat detector: an input layer, where a dangerous substance was introduced to the cell; the processing layer, where the substance was identified as being dangerous, and an output layer, where the cell was programmed to sound an alarm. Even finer calibration is possible, Peccoud's group demonstrated, so the synthesized cell only emits a detectable optical signal when two or more suspicious substances are present. "Many substances are benign on their own, but potentially lethal if combined with other substances," noted James Valdes, a US Army Senior Advisor for Biotechnology based at the Edgewood Chemical and Biological Center. "Mustard gas, for example, is made up of a compound called thiodiglycol, which is employed as a solvent in dyes, and phosphorous trichloride, a chemical often used to make organic phosphorous-containing products." Genetically-engineered material within the cell can be calibrated so that it will fail to respond if just one reactant is present but send a chemical message when it detects a pair of chemicals. In a manner similar to the way labs-on-a-chip today perform myriad tests at once, the cells chemical signals can be converted to electrical alarms when they are received then transmitted to a remote computer for analysis. "Just like electrical engineers are used to partition the design of electronic devices between hardware and software implementations, bioengineers need to learn how to partition their designs between hardware, software, and wetware," said Matthew Lux, one of the article's lead authors. In the future, as terrorist groups become more and more adept at using readily purchasable substances to make WMDs, researchers may react to intelligence agency warnings of the latest potential threats and design bio-detectors ready to spot those threats should they occur. It's a scenario similar to how world health officials today order vaccines to combat the latest flu strains each year, and it may well become just as necessary and commonplace. Mark Ingebretsen wrote regularly about homeland security issues as a healthcare and biotech columnist for the Online Wall Street Journal. As a regular contributor to IEEE Intelligent Systems magazine, he covers topics such as forensic data mining, pandemic disease detection and emergency response.

Could A Mumbai Style Terror Attack Happen again?

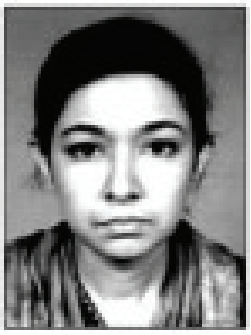
Are US cities prepared for a Mumbai-style terror attack? Gerald Posner watches a mock assault on Miami, and reveals the answer. A year ago tomorrow, millions of people worldwide began watching a terror attack play out live for three days in Mumbai. Ten gunmen staving off the police, special forces, and army troops captured world attention while slaughtering 173 people and wounding more than 300. As the Mumbai victims are remembered this week, federal terrorism intelligence experts have quietly embarked on a campaign to help some major metropolitan police forces in the U.S. learn the lessons of Mumbai. Two weeks ago, I was the first journalist allowed to sit in on a two-hour briefing conducted by John Miller, the assistant deputy director of intelligence analysis for the Office of Director of National Intelligence, to 200 top Miami police officers, SWAT team leaders, and leaders from the fire department. The briefing, conducted at the Miami Police Department's headquarters, was a sobering PowerPoint presentation. Miami was the third city, after Los Angeles and Boston, to get Miller's briefing. In the exercise set up for Miami, a Mumbai-type attack meant the first shooting was along the business district in Coconut Grove. Less than 30 minutes later, a car bomb went off in crowded Little Havana. "Mumbai signaled a turn in terror operations," says Miller, the former co-anchor of ABC's 20/20, best known for his 1998 cave interview of Osama bin Laden, who has worked with the government on the terror front since



2001. “With al Qaeda being hit hard, less centralized and having more trouble raising money, Mumbai is the format for the future: low tech, low cost and high yield. It was a strategic and technical success that got them the biggest bang for the buck, creating a lot of fear while getting great media attention.”

Dr Aafia Siddiqui – al Qaedas Mystery Woman

Aafia Siddiqui, a Pakistani neuroscientist and mother of three is to stand trial in New York for attempted murder. But shadowy questions about her life remain, including her links to al-Qaida and her five ‘lost’ years. As reported on National Terror Alert last year, The capture of Aafia Siddiqui, most likely saved many innocent lives however; the information she may be able to provide authorities may prove even more valuable in the long run. Earlier reports stated that handwritten notes about a “mass casualty attack” that listed New York City landmarks like the Empire State Building and the Statue of Liberty were found on Siddiqui. It has also been reported that Siddiqui carried lists of other locations like Wall Street, the Brooklyn Bridge and Plum Island and notes about “dirty bombs,” chemical and biological weapons and other explosives.



The mystery of Dr Aafia Siddiqui Written by Declan Walsh, The Guardian
On a hot summer morning 18 months ago a team of four Americans – two FBI agents and two army officers – rolled into Ghazni, a dusty town 50 miles south of Kabul. They had come to interview two unusual prisoners: a woman in a burka and her 11-year-old son, arrested the day before. Afghan police accused the mysterious pair of being suicide bombers. What interested the Americans, though, was what they were carrying: notes about a “mass casualty attack” in the US on targets including the Statue of Liberty and a collection of jars and bottles containing “chemical and gel substances”. At the town police station the Americans were directed into a room where, unknown to them, the woman was waiting behind a long yellow curtain. One soldier sat down, laying his M-4 rifle by his foot, next to the curtain. Moments later it twitched back. The woman was standing there, pointing the officer’s gun at his head. A translator lunged at her, but too late. She fired twice, shouting “Get the **** out of here!” and “Allahu Akbar!” Nobody was hit. As the translator wrestled with the woman, the second soldier drew his pistol and fired, hitting her in the abdomen. She went down, still kicking and shouting that she wanted “to kill Americans”. Then she passed out.

A technical evaluation of the Fordow fuel enrichment plant

Revelations about Iran's secret Fordow fuel enrichment plant have been seen as proof that Tehran is pursuing nuclear weapons. But the facility's small capacity makes enriching either reactor-grade or even bomb-grade uranium extremely time-consuming and impractical. Although it is significant that Iran has officially declared that there are no further secret nuclear facilities such as Fordow inside the country, it's possible that this facility could be one of several that has been either built or planned. When Iran's Fordow fuel enrichment plant first became public on September 25 at the G-20 meeting in Pittsburgh, the underground facility, located near the holy city of Qom, was widely portrayed as proof that Tehran was pursuing nuclear weapons. In particular, U.S. President Barack Obama, French President Nicolas Sarkozy, and British Prime Minister Gordon Brown claimed that the clandestine enrichment plant's "size and configuration" were "inconsistent with that of a peaceful program." For its part, Tehran has steadfastly denied that it's pursuing nuclear weapons and rejects accusations that it hid the Fordow enrichment plant from the international community.

Iran has defended its lack of disclosure and the nature and location of the facility (in a bomb-proof tunnel, under a mountain, near a military base) by citing its legal right under the Nuclear Non-Proliferation Treaty to enrich uranium, persistent Israeli military threats, and a different interpretation of its obligations to reveal new facilities to the International Atomic Energy Agency (IAEA) under the Subsidiary Arrangements to its Safeguards Agreement. Because it has been exposed, the Fordow facility is now subject to IAEA inspection, just as any other declared Iranian nuclear facility. (The IAEA's technical assessment of Fordow also plays a wider political role, to determine whether Iran has violated its obligations under the Safeguards Agreement and arbitrate between Western accusations and Iranian claims of a peaceful nuclear program.) According to IAEA Director-General Mohamed ElBaradei, inspectors who visited the site in late October didn't find anything immediately alarming. But according to the IAEA report PDF, larger questions regarding the chronology and purpose of the site still remain.

The facility's capacity

The October inspection confirmed that so far construction corresponds to the design specifications for the facility provided by Tehran to the IAEA. Iran ultimately plans to install about 3,000 centrifuges at Fordow, which is consistent with U.S. estimates. The inspection revealed that none of the centrifuges had been installed but that footings and piping were in place. Although Iran has mentioned that it may install more advanced centrifuges in the future, current plans call for IR-1 machines, the well-understood design that the Iranians operate at their Natanz enrichment facility. This substantially narrows the uncertainty in estimating Fordow's potential enrichment capacity. Since centrifuge cascades used for nuclear fuel differ in arrangement from those used for bomb material, inspectors have photographed the cascade piping to evaluate whether it's consistent with declared enrichment levels and the declared number of machines. Their conclusions are forthcoming. What is known about the facility's size, however, is perplexing. It will be 6 percent of the ultimate capacity of Natanz, making it, as Western nations have pointed out, far too small to be useful for enriching fuel for civilian nuclear reactors. In fact, it would take almost 90 years for the cascades at Fordow

to fuel a single 1,000-megawatt commercial nuclear power plant for just one year. Therefore, many nuclear experts have indicated that Fordow was more likely designed to be a clandestine facility devoted to enriching uranium for weapons, in accord with U.S. statements that the facility is inconsistent with a peaceful nuclear program. But Fordow may be too small even for that. In theory, the plant is conveniently sized to manufacture enough highly enriched uranium (HEU) for one nuclear weapon per year, if it were to use already enriched, reactor-grade uranium as the feedstock. This scenario, a favorite among nonproliferation experts, would require enriched uranium to be sneaked out of the Natanz facility, which has been under safeguards since it became operational in 2003. The IAEA's goal for detection of a "significant quantity" of uranium, that is, enough to be of worry for making a bomb, is one month--much shorter than the time it would take the cascades at Fordow to enrich such an amount. If Iran did want to enrich uranium for a weapon, it would be far easier to oust inspectors from Natanz and proceed with much more rapid HEU enrichment there. The Fordow option would be more plausible if it used machines with a significantly higher separative capacity than the IR-1 centrifuges--a possibility that will need revisiting when the devices actually are installed at Fordow. Since it would be difficult to divert enriched material from Natanz, Fordow still could be used to enrich natural uranium to HEU levels (although it would take four years to enrich enough natural uranium for just one bomb, hardly a viable breakout option). To remain undetected, this would require a covert uranium hexafluoride conversion plant, which converts uranium to gas for use in the cascades. So far, no clandestine Iranian conversion facility has been detected. (Iran's only known conversion plant is at Isfahan, and it is under safeguards.) The facility's purpose. In its initial statement to the IAEA, Iran described Fordow as a pilot plant protected by "passive defense" systems. Tehran has justified placing the facility in a hardened mountainside tunnel as a response to barely veiled threats by the United States and overt threats by Israel to destroy its nuclear program. In another letter, cited in the agency's report, Iran described the facility as a so-called contingency enrichment plant, designed to prevent enrichment from being suspended in the event its declared nuclear facilities were destroyed by military attack. The Iranian Revolution Document Center [in Farsi], a pro-government Iranian research institute dedicated to documenting and analyzing the Islamic Revolution, suggests that Fordow's strategic purpose is to deter an attack on Natanz. Even though Fordow is much smaller than Natanz, this makes some sense. Such an attack would not be meant to cripple Iran's commercial nuclear fuel production, but to stop a weapons program. If Fordow is invulnerable and could alone carry a weapons program forward, the value of attacking Natanz is greatly diminished--although Fordow's limited enrichment capability is still an issue. Another more disturbing possibility is that Iran has a number of similar secret facilities--along with the required uranium hexafluoride conversion plants--and that Fordow is simply the only one to have been discovered. The IAEA report raises this possibility, but says that Iran has declared to the agency that it has no other undeclared nuclear facilities. Any further discoveries would be hard to explain away as being for peaceful purposes--and we doubt that Iran would make such a blanket statement in light of its poor track record at hiding its nuclear facilities. It also is possible that Fordow was the first of several planned secret facilities, and that, with its discovery, Iran has put further plans on hold. From a technical perspective, it's too soon to know how Fordow fits in with Iran's larger nuclear ambitions. Although the facility's capacity is not viable for large-scale nuclear fuel production by itself, it is not ideal for weapons production either. The facility's legality. The chronology of Fordow's planning and construction is important to know whether Iran has met even its own recognized obligations to the IAEA. If Tehran's story is inconsistent, it shows an intent to deceive the agency (with the implication, of course, that it was covering up a covert weapons program). According to the IAEA, Iran should have declared the facility as soon as it decided to construct it, as it is legally obligated to do under revised Code 3.1 rules of the Subsidiary Arrangements to its Safeguards Agreement. But Tehran unilaterally withdrew from these provisions in March 2007 to protest what it thought was unfair censure by the U.N. Security Council. Under the version of Code 3.1 that Iran does recognize, it is obligated to declare any nuclear facility six months before material is introduced. Iran announced Fordow in a letter to the agency on

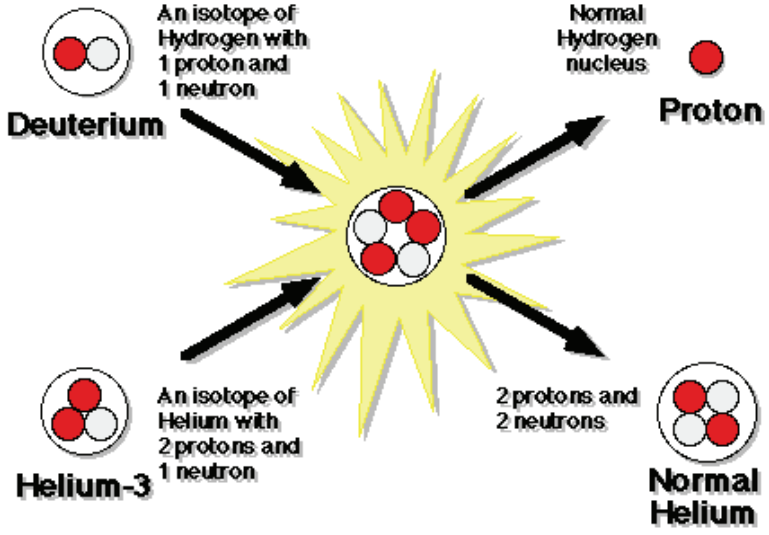
September 21 and stated later that the plant would become operational in 2011, meaning that it was well within its obligations as it recognizes them. According to U.S. officials, however, the timeline is much shorter--the facility was "at least a few months, perhaps more" from operation, suggesting that Iran would be in violation of its own recognized obligations and that the 2011 date was retroactively fabricated to put the facility in compliance. Although there was no comment by inspectors on whether the facility's construction seemed consistent with a declared 2011 operational date, the IAEA report concluded that Fordow was at an "advanced stage of construction" with centrifuge mounts, piping, and auxiliary equipment already installed. At Natanz, Iran took about a year to complete the installation of the facility's initial 3,000 centrifuges. But it brought them online as they were being set up rather than wait for all 3,000 machines to be set in place, so initial operation began in less than a year. Either way, it would be difficult to prove that Fordow could become operational in less than six months because Iran always could stall construction to match its stated schedule of 2011. When the decision to construct Fordow was made and when actual construction started also remains unclear. Washington believes that construction began before 2007, meaning that, even by Iran's standards, it should have been declared to the IAEA much earlier. According to Iran, Fordow was part of a wider Iranian initiative to construct generic contingency centers based on increased military threats. Iran maintains that it acquired "one of those constructed and prepared centers" in late 2007, indirectly confirming that construction of the tunnel in which the enrichment plant is located had commenced prior to 2007. It denies, however, that the site was previously slated for an enrichment plant. The question is, was the tunnel

constructed with a centrifuge plant in mind? Moreover, if design work for the facility started in 2006, as the United States maintains, and U.S. intelligence was positive that it was intended to be "a covert centrifuge facility," why did the 2007 National Intelligence Estimate conclude that Iran had halted its nuclear weapons program in 2003? It's possible that U.S. intelligence identified that construction was taking place, but it lacked information on what was being built at Fordow. This is not inconsistent with Iran's story that in 2007 nothing was at the site except for an empty tunnel that didn't have a specified nuclear use. The facility's political implications. The revelations regarding Fordow have fueled suspicions that Iran has built a clandestine enrichment facility as part of its nuclear weapon "breakout" plan. Contrary to Western speculation, initial IAEA inspections at the facility revealed no smoking gun, but the episode raises many questions and exacerbates worries about Iran's intentions. Although the IAEA flatly rejects Iran's unilateral withdrawal from its revised Code 3.1 requirements, the

agency was relatively mild in its latest report, merely claiming that the Fordow declaration is "inconsistent with [Iran's] obligations." The agency also abstained from making comments on the chronology or how close to completion the facility was. It seems as though the IAEA was providing leeway for Iran to explain itself or at least is allowing Tehran to further cooperate in the future. It's also possible that Iran was not trying to deceive the international community. Even though Iran's actions appear suspicious, one legitimate explanation is that Tehran acted strictly by what it perceives to be its most narrow and legal obligations. Iran might be acting this way out of national pride and because it feels that it is being unfairly discriminated against, rather than a desire to cover-up a covert weapons program. Of course, Iran's actions also can be explained as an attempt to deceive. A physical inspection of Fordow can't prove intent one way or the other. To do so, the IAEA needs access to the papers that document the decision to build Fordow in the first place. Based on past experience with Iran over the Natanz enrichment facility, essential questions such as the chronology of development and the role of the facility will be answered only gradually, if at all. (Previously, the IAEA was able to make substantial progress in uncovering Iran's uranium enrichment program in part because Tehran had signed and agreed to implement the Additional Protocol, which allows inspections to facilities not included in the Safeguards Agreement--such as uranium mines and centrifuge workshops. Iran has since refused to ratify the Additional Protocol and suspended its application. With limited access to additional facilities, the agency will have a harder time detangling the facts behind Fordow than it did with Natanz.) What is known about Fordow is this: It is neither ideal for commercial nor for military purposes, and Iran's contingency and deterrence arguments are weak. The facility's size and capacity would make the most sense if it were part of a network of clandestine nuclear facilities, but Iran has formally declared it has no other undeclared facilities. This is significant since if additional hidden facilities are discovered, there will be no innocent explanation. Fordow, however, could be the first of a network of clandestine plants, and decisions to construct them could legally (according to Iran) be made in the future. In any event, it is good news that Fordow was discovered and that it will now be under IAEA safeguards. With Fordow under watch, the risks that it could be used to secretly enrich uranium for a nuclear weapon are far smaller than what was already possible at its declared Natanz facility.

Shortage Slows a Program to Detect Nuclear Bombs

The Department of Homeland Security has spent $230 million to develop better technology for detecting smuggled nuclear bombs but has had to stop deploying the new machines because the United States has run out of a crucial raw material, experts say. The ingredient is



helium 3, an unusual form of the element that is formed when tritium, an ingredient of hydrogen bombs, decays. But the government mostly stopped making tritium in 1989. “I have not heard any explanation of why this was not entirely foreseeable,” said Representative Brad Miller, Democrat of North Carolina, who is the chairman of a House subcommittee that is investigating the problem. An official from the Homeland Security Department testified last week before Mr. Miller’s panel, the Investigations and Oversight Subcommittee of the House

Science Committee, that demand for helium 3 appeared to be 10 times the supply. Some government agencies, Mr. Miller said, did anticipate a crisis, but the Homeland Security Department appears not to have gotten the message. The department had planned a worldwide network using the new detectors, which were supposed to detect plutonium or uranium in shipping containers. The government wanted 1,300 to 1,400 machines, which cost $800,000 each, for use in ports around the world to thwart terrorists who might try to deliver a nuclear bomb to a big city by stashing it in one of the millions of containers that enter the United States every year. At the White House, Steve Fetter, an assistant director of the Office of Science and Technology Policy, said the helium 3 problem was short-term because other technologies would be developed. But, he said, while the government had a large surplus of helium 3 at the end of the cold war, "people should have been aware that this was a one-time windfall and was not sustainable." Helium 3 is not hazardous or even chemically reactive, and it is not the only material that can be used for neutron detection. The Homeland Security Department has older equipment that can look for radioactivity, but it does not differentiate well between bomb fuel and innocuous materials that naturally emit radiation — like cat litter, ceramic tiles and bananas — and sounds false alarms more often. Earlier this year, the Pacific Northwest National Laboratory, part of the Energy Department, said in a report, "No other currently available detection technology offers the stability, sensitivity and gamma/neutron discrimination" of detectors using helium 3. Helium 3 is used to detect neutrons, the subatomic particles that sustain the chain reaction in a bomb or a reactor. Plutonium, the favorite bomb-making material of most governments with nuclear weapons, intermittently gives off neutrons, which are harder for a smuggler to hide than other forms of radiation. (Detecting the alternative bomb fuel, enriched uranium, is a separate, difficult problem, experts say.) Helium 3 is rare in nature, but the Energy Department accumulated a substantial stockpile as a byproduct of maintaining nuclear weapons. Those weapons use tritium, which is the form of hydrogen used in the H-bomb, but the hydrogen decays into helium 3 at the rate of 5.5 percent a year. For that reason the tritium in each bomb has to be removed, purified and replenished every few years. It is purified by removing the helium 3. The declining supply is also needed for physics research and medical diagnostics. The Energy Department used to make tritium in reactors at its Savannah River Site, near Aiken, S.C., but those were shut after many operational problems. It enlisted the Tennessee Valley Authority to make some tritium in a power reactor, using the same method it had used at Savannah River, breaking up another material, a form of lithium, with neutrons. One of the fragments is tritium. But that project has run into technical problems as well. Mr. Miller estimated that demand for helium 3 was about 65,000 liters per year through 2013 and that total production by the only two countries that produce it in usable form, the United States and Russia, was only about 20,000 liters. In a letter to President Obama, he called the shortage "a national crisis" and said the price had jumped to $2,000 a liter from $100 in the last few years, which threatens scientific research.

Dolphins and Sea Lions Ready To Fight Terrorism

The Navy has approved a plan to step up anti-terrorism efforts at a Washington base by sending specially trained dolphins and sea lions into surrounding waters. A Naval base near Washington's Puget Sound is stepping up its security by employing aquatic mammals to patrol its restricted waters. The animals' deployment in 2010 will mark the realization of a program that has been more than three years in the making. The dolphins and sea lions to defend the base were trained as part of the Navy Marine Mammal Program in San Diego. Working with human handlers, dolphins will search surrounding waters for rogue divers and swimmers. Tom LaPuzza, a spokesman for the

program, told Scientific American that upon finding a diver, the dolphin will return to the handler and the handler will assess the severity of the threat."[T]he handler will place a strobe light or a noisemaker on the dolphin's nose … The dolphin is trained to swim to the intruder, bump him or her from behind—which would knock the device off its nose—and then quickly swim away while military personnel take over."Sea lions are trained to carry cuffs in their mouths that clasp shut around a diver's leg when bumped by the sea lion. Cuffs are attached to a tether, so military personnel can haul in the intruder after he is cuffed.

Preventing Synthetic Pathogens from Getting Into the Wrong Hands

In March 2007, the Homeland Security Today cover report, Viral Visions, explored emerging concerns over disturbing new developments in synthetic genomics and biological research that provide the potential for new and lethal designer pathogens. Deadly pathogens that can be created virtually from scratch. In late November, the Department of Health and Human Services took the first step toward imposing controls on the synthetic genomic industry in the form of guidelines for companies to follow to screen for suspicious orders for customized DNA sequencing placed by companies and individuals. Because of post-9/11 concerns over bioterrorism, the National Science Advisory Board for Biosecurity (NSABB) was charged with identifying the potential biosecurity issues raised by the ability to synthesize "Select [controlled biological] Agents" and providing advice on whether current government policies and regulations adequately cover the de novo synthesis of these Select Agents. The panel's report, Addressing Biosecurity Concerns Related to the Synthesis of Select Agents, was formally transmitted to the government in March 2007. The NSABB determined that the technology "employed in the field of synthetic genomics to create sophisticated live vaccines and to discover new therapeutics for infectious diseases ... can be misused to generate dangerous pathogens de novo that are subject to oversight, thus circumventing the extant regulatory framework for controlling the possession and use of such organisms." "This dichotomy illustrates the dual use nature of synthetic genomics and underscores the need to develop strategies to address the possibility that knowledge and technologies emanating from vitally important biological research will be misused to threaten public health or national security," the report determined. "In this regard," the NSABB report concluded, "rapid advances in DNA synthesis technology and the open availability of pathogen genome sequence data have raised concerns in the scientific community and general public regarding the possible use of this technology and information to generate biological agents that could threaten public health, agriculture, plants, animals, the environment, or material. Special concern has been voiced about the use of this technology to generate Select Agents de novo. Continuing, the report stated that "while traditional recombinant DNA technology has raised similar or related concerns, approaches based on de novo synthesis avoid any need for access to the naturally occurring agents or naturally occurring nucleic acids from these agents, and greatly expand the potential availability of these agents. The National Science Advisory Board for Biosecurity has been charged with identifying the potential biosecurity concerns raised by the ability to synthesize Select Agents and providing advice on whether current United States Government policies and regulations adequately cover the de novo synthesis of Select Agents or whether additional biosecurity measures are necessary." The NSABB Working Group on Synthetic Genomics' assessed the adequacy of the current regulatory framework to safeguard against the misuse of this science and made recommendations to address their concerns. The recommendations were approved by the NSABB on October 25, 2006. "Toward this end," on November 27, the Office of the Assistant Secretary of Preparedness and Response (ASPR) within the Department of Health and Human Services issued the Notice of proposed rulemaking, "Screening Framework Guidance for Synthetic Double-Stranded DNA Providers." ASPR is the lead agency in a broad interagency process to draft the guidance stemming from the NSABB's recommendations. The Notice stated that "technologies that permit the directed synthesis of polynucleotides, which underlie synthetic biology and more specifically synthetic genomics, could enable individuals not authorized to

possess [physical biological] Select Agents to gain access to them through their de novo synthesis. Such synthesis obviates the need for access to the naturally occurring agents or naturally occurring genetic material from these agents, thereby greatly expanding the potential availability of these agents." The draft voluntary guidelines for the gene and genome synthesis industry explained that "synthetic biology, the developing interdisciplinary field that focuses on both the design and fabrication of novel biological components and systems as well as the re-design and fabrication of existing biological systems … is not constrained by the requirement of using existing genetic material. Thus, technologies that permit the directed synthesis of polynucleotides have great potential to be used to generate organisms, both currently existing and novel, including pathogens that could threaten public health, agriculture, plants, animals, the environment, or material." In order "to reduce the risk that individuals with ill intent may exploit the commercial application of nucleic acid synthesis technology to access genetic material derived from or encoding Select Agents or Toxins, the US Government has developed recommendations for a framework for synthetic nucleic acid screening" to identify suspicious intent on the part of purchasers of synthetic genomic products from commercial suppliers, the Notice stated. The proposed rulemaking "is intended to provide guidance to producers of synthetic genomic products regarding the screening of orders so that these orders are filled in compliance with current US regulations and to encourage best practices in addressing potential biosecurity concerns." The Notice declared that "the US Government acknowledges that there are synthetic nucleic acid sequences from non-Select Agents or Toxins that may pose a biosecurity concern," and therefore "the primary goal in developing guidance for synthetic nucleic acid providers is to minimize the risk that unauthorized individuals or individuals with malicious intent will gain access to toxins and organisms of concern through the use of nucleic acid synthesis technologies." The CIA began worrying in earnest about designer pathogens soon after the October 2001 anthrax attacks provided evidence indicating the anthrax had been weaponized. An expert panel was convened to study the problem and to make an assessment of the seriousness of a synthetic viral threat. Following an outcry from some of the scientists it empanelled to study the issue, the CIA Intelligence Directorate's Office of Transnational Issues quietly released a short, unclassified synopsis of the academician's November 2003 report, The Darker Bioweapons Future. The report concluded that the "growing understanding of the complex biochemical pathways that underlie life processes has the potential to enable a class of new, more virulent biological agents engineered to attack distinct biochemical pathways and elicit specific effects." Although the two-page abstract provided no details concerning the expertise, equipment and facilities required to develop engineered pathogens, nor a time estimate for how long the development process might take, more than five years later the CIA—and other IC components —continue watching developments very carefully. Indeed. Synthetic bio-threats are carefully being monitored by American intelligence authorities and bio-weapons experts. And apparently there's reason for them to be more concerned than they were more than two years ago when the Viral Visions report noted that the ability of individuals to create frightening new viruses in their basements was rapidly growing. Last May the Wall Street Journal tackled the problem in the story, In Attics and Closets, 'Biohackers' Discover Their Inner Frankenstein. Under the subhead, Using Mail-Order DNA and Iguana Heaters, Hobbyists Brew New Life Forms, the report highlighted that "do-it-yourselfers tinker with the building blocks of life in the comfort of their own homes." The report asked whether these "biohackers [pose] a threat to national security?" The report quoted "a senior official in the FBI's Weapons of Mass Destruction Directorate saying the bureau is working with academia and industry to raise awareness about biosecurity, 'particularly in light of the expansion of affordable molecular biology equipment' and genetic databases." A variety of federal officials who had expressed these same concerns to Homeland Security Today more than two years ago recently reiterated their worries to HSToday.us, pointing to the very sorts of home basement virology labs that were described in the Wall Street Journal report. "The ability to create nasty pathogens like your hybrid rabies virus in your bathroom is becoming easier and easier," one of the authorities said [see the HSToday.us Kimery Report, Zombies, Rabies and Synthetic Genomics]. The official was referring to the description of a synthetic virus in the

Viral Visions report – a highly contagious "designer" rabies virus that not only makes the victim mad, but mad enough to want to run around biting people. In the world of synthetic hybrid pathogens, zombies are "possible," a virologist who helps the Intelligence Community keep track of the work being done in the field of synthetic genomics had earlier told Homeland Security Today. "The emergence of this field is driven by recent advances in the underlying technology of commercial DNA synthesis that allow biologists to produce and assemble segments of DNA quickly and cheaply with almost perfect accuracy," wrote John Dileo in a MITRE publication report. "While the synthesis of small segments of DNA has been possible for two decades, the use of these early techniques to produce a genome (the complete blueprint, in the form of DNA, for the construction of an organism) would have required years of work and been prohibitively expensive," Dileo continued. But today "DNA production and assembly techniques have advanced to the point that a medium-sized virus can now be constructed in weeks. In addition, these improvements have led to a rapid increase in the number of companies that offer whole gene synthesis. The resulting competition has lowered prices to within the budgets of most researchers." Several years earlier, in the paper, A Practical Perspective on DNA Synthesis and Biological Security, published in Nature Biotechnology, the authors stated that "few developments have leapfrogged over predecessor technology as quickly and extensively as synthetic biology. Based on cutting-edge DNA synthesis technology, synthetic biology has already fueled an expansion of opportunities in biological engineering, with advanced capabilities that surpass those provided by traditional recombinant DNA technology." But while "synthetic biology promises vast improvements to our well-being and our understanding of the living world," the paper's authors cautioned, they also pointed out that "like any powerful technology, DNA synthesis has the potential to be misused. In the wrong hands, the new capabilities enabled by synthetic biology could give rise to both known and unforeseeable threats to our biological safety and security." And "current government oversight of the DNA synthesis industry falls short of addressing this unfortunate reality," the authors warned. The group of academics who authored the paper called "for the immediate and systematic implementation of a tiered DNA synthesis screening process." "In order to establish accountability at the user level," they wrote, "individuals who place orders for DNA synthesis would be required to identify themselves, their home organization, and all relevant biosafety level information." It's just that sort of information the federal government wants the synthetic genomics industry to collect and scrutinize when fulfilling orders for customized DNA sequencing. Seeing the scores of companies that pop up under the Google search, "customized DNA sequencing," and it's easy to understand the concern and reasoning behind the proposed rulemaking.

Researcher contracts "rabbit fever" at laboratory

A military researcher at the United States Army Research Institute of Infectious Diseases (USAMRIID) has contracted what appears to be a laboratory-acquired infection of tularemia. The researcher was working on developing a vaccine for the disease at the institute. She is currently being treated with antibiotics and is recuperating at home. Tularemia, also known as rabbit fever, is caused by the bacterium Francisella tularensis. This is one of several dangerous pathogens being researched at USAMRIID. The disease in people depends on how it's acquired. After infection, incubation can be a couple of days to weeks, with non-specific symptoms like fever, chills, headache, sore throat and diarrhea. The way the organism enters the body frequently dictates the disease and degree of systemic involvement. Fatalities do occur. Tularemia is treatable with antibiotics (streptomycin and gentamicin).

There is no person to person transmission of this bacterium. F. tularensis is of concern as a possible agent of bioterrorism and biowarfare.

ΣΣ: Έχοντας ζήσει από κοντά, κατά τη διάρκεια υγειονομικής εκπαίδευσης μου (μέσω προγράμματος του OPCW) στο στρατιωτικό νοσοκομείο της Τεχεράνης, το δράμα των ατόμων που επέζησαν της επίθεσης στη Halabja, είναι ιδιαίτερα ευχάριστη η παρακάτω είδηση της επανένωσης μιας οικογένειας που βίωσε τον τρόμο των χημικών όπλων…

Kurdish boy who 'died' in Halabja gas attack is reunited with his mother

For two decades Fatima Hama Saleh thought that she had lost all her children in a poison gas attack carried out by Saddam Hussein against the Kurdish town of Halabja, in what was the single worst atrocity of the former Iraqi dictator's rule. Now, however, she has been reunited with her son, Ali Pour, in a dramatic meeting after DNA tests confirmed that the young man, now 21, was the infant she lost when chemical weapons rained down on the Kurdish market town. "I'm in a dream," Mr Pour said, as he embraced his weeping mother. She replied: "I wonder if it is a dream or a gift from God." Mother and son had to talk to each other through an interpreter as Mr Pour only speaks his adopted tongue, Farsi, and not his native Kurdish or Iraq's official language, Arabic. Mrs Saleh revealed his birth name, Zimnaku Mohammed Saleh, and recalled the day that Halabja was attacked, including the panic that the family felt when their home was enveloped by a deadly cocktail of mustard gas and the nerve agents tabun, sarin and VX. "We didn't know where to go," Mrs Saleh said. "Zimnaku, the four-month-old, was on my lap and suddenly my older son screamed, 'Mother, I feel like I'm burning'. "I tried to help him and my other sons, too. But it was in vain. I saw them dying in front of me. I collapsed and the next thing I remember is lying in a hospital bed in Tehran." Mr Pour's adoptive uncle explained what happened next. "The baby, Ali, survived for three days," Habib Hamid Pour said. He was found by the Iranian military, which moved into Halabja after the attack, and taken to Iran along with other survivors. Eventually, he was placed with a family in the eastern Iranian city of Mashhad and was raised as an Iranian boy. "My adopted mother was nice," Mr Pour said, dressed in traditional Kurdish clothing of baggy pants, tunic and scarf tucked into his belt. "When I entered primary school at age 6, she told me I am from the Kurdish people of Halabja. She said I should return some day to meet my relatives." Four months ago his adoptive mother was killed in a car accident. "I felt lonely and I felt a strange feeling calling me to return to the arms of my relatives," Mr Pour said. "I decided to go back." He contacted Iranian officials who kept records on the Halabja survivors brought to Iran. They contacted the Halabja government, which said that six families were missing a boy who would now be Mr Pour's age. A judge ordered a DNA test to be carried

out by a medical lab in Jordan.The massacre in Halabja on March 16, 1988, was part of Saddam's 1987 to 1988 Anfal campaign that killed up to 200,000 Kurds. Three quarters of the 5,000 killed in Halabja were women and children. Four of Mrs Saleh's five children died in the attack, as well as her husband, Mr Pour's father. After the reunion, she said: "I will not die in sorrow and grief after all the miseries I have experienced." She had first learnt that a surviving child was looking for his family from a television report and applied to do the DNA test. At the meeting of the six participating families shouts of joy eventually broke the intense silence that had greeted the announcement. Mrs Saleh stood up and then fell to her seat as she took in what had been said. "Thank you, God! You brought back my son Zimnaku," she cried. "It's like my whole family has come back to life. My son has returned."

.

Massacre of the Kurds

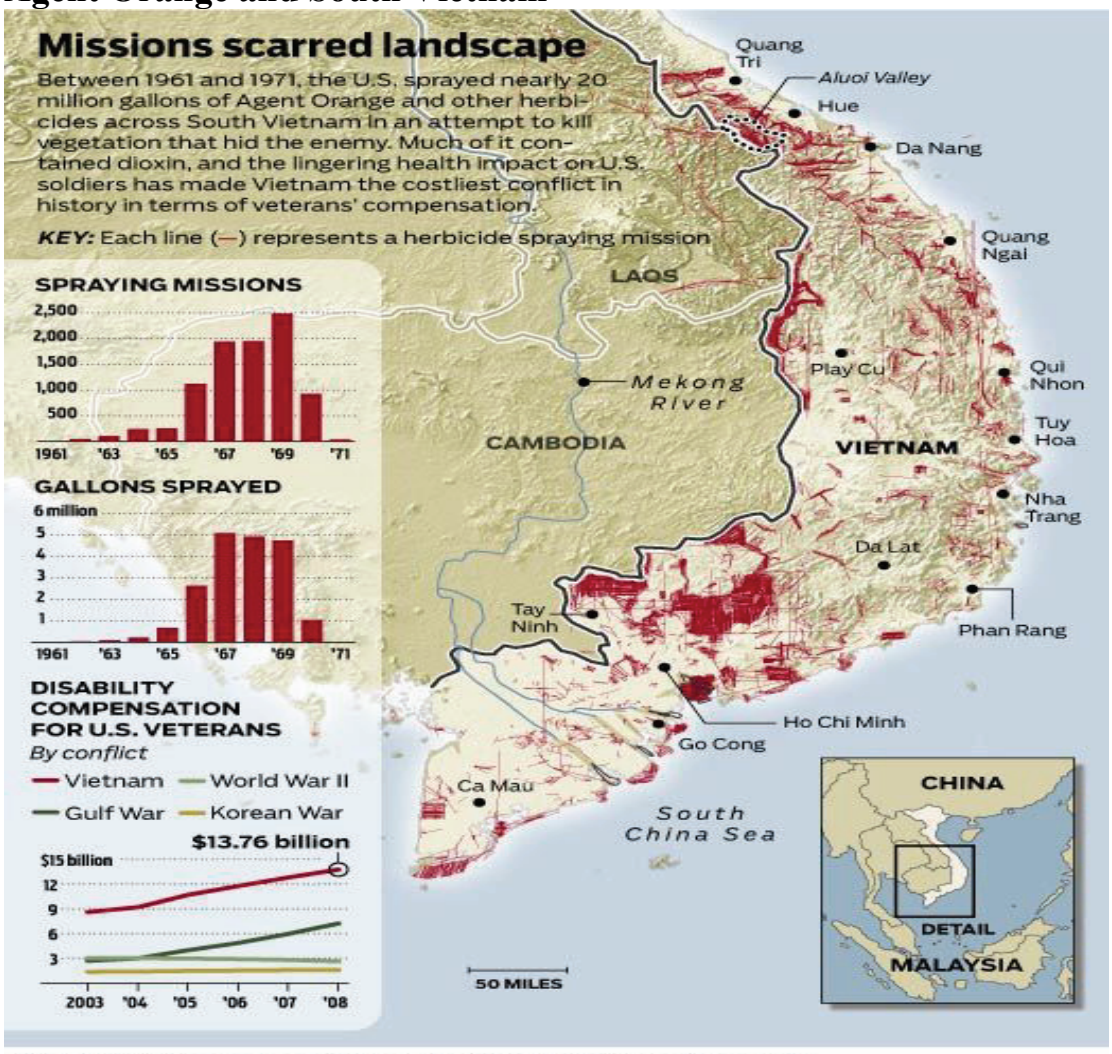
• The Halabja massacre was the most infamous episode in Saddam Hussein's Anfal campaign, in which 4,000 Kurdish villages were attacked and up to 100,000 killed

• In the eighth year of the Iran-Iraq war, on March 16, 1988, aircraft dropped poison gas bombs on the town, which had a population estimated at 70,000

• Halabja had recently been captured by Iranian and Kurdish forces, and many families had hidden in their basements from shelling by the Iraqi military

• The aircraft made up to 14 sorties, each time with seven or eight aircraft, dropping a cocktail of mustard gas and the nerve agents tabun, sarin and VX

Agent Orange and South Vietnam



SOURCE: U.S. Department of Veterans Affairs, Herbicide Exposure Assessment-Vietnam

MAX RUST AND PHIL GEIB/TRIBUNE

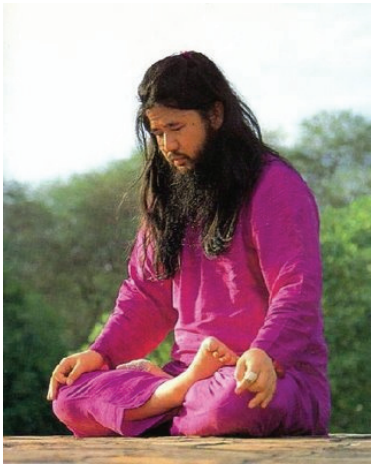
Daily seizures
(Tribune photo by Kuni Takahashi / June 25, 2009)
Do Thi Hang, 19, experiences a seizure as her father Do Duc Diu, 58, tries to keep her from injuring herself. Hang suffers from frequent seizures as a result of fluid that accumulates in her brain, which has been linked to her father's exposure to Agent Orange.

Stephen Price
(Palmer family photo)
Amanda Price Palmer, below, poses with her father, Stephen Price, and her mother, Brenda Price, of Brownsburg, Ind., for a family self-portrait as Stephen Price lay dying in a hospital in 2008 of cancer related to herbicides sprayed during the Vietnam War.

In honor of Jack Cooley
(Tribune photo by Chris Walker / September 12, 2009)
A U.S. Army soldier presents a folded U.S. flag to Christina Cooley at the memorial service in Evanston's Sheil Chapel for her father, Jack Cooley. Exposed to Agent Orange during his service in Vietnam, he died in July of multiple myeloma. At right is Christina's brother, John.

Death penalty for cult member

Japan's Supreme Court rejected an appeal on Thursday against the death penalty handed to a senior member of the doomsday cult behind the 1995 deadly sarin nerve gas attack on the Tokyo subway. The ruling makes Yoshihiro Inoue, 39, the ninth member of the Aum Supreme Truth cult awaiting execution after final rulings by the country's highest court. Among 13 Aum members originally sentenced to death, he was the only defendant whose earlier rulings were divided between a lower court's life sentence and a death sentence given by the Tokyo High Court. Four sect members are awaiting rulings on appeals against their death sentences. The Supreme Court upheld the high court's verdict on Inoue, deciding that he 'played an essential and significant role on his initiative' in the 1995 sarin attack, said presiding judge Seishi Kanetsuki. According to the ruling of the high court, Inoue plotted the attack, which killed 12 people and injured thousands, with Aum Supreme Truth sect leader Shoko Asahara. The court also ruled he kidnapped and murdered Kiyoshi Kariya, then 68, who tried to shelter his sister after she escaped from the sect. The bearded guru was revered as a god by his sect, which preached a blend of Buddhist and Hindu dogma mixed with apocalyptic visions. He was obsessed with Nazi-invented sarin gas and paranoid his enemies would attack him with it.



NASA Technology Could Have Biodefense Uses

Technology developed for NASA could have additional uses in the detection of disease agents that could be used in acts of bioterrorism, a California firm announced last week. Universal Detection Technology announced that it was answering a U.S. Homeland Security Department request for research and development proposals that focus on the detection and containment of biological agents such as anthrax. The UDT technology employs a molecule found only in bacterial spores that can be prodded into producing a luminescent glow when exposed to ultraviolet light, allowing for detection. The technology was first licensed through NASA's Jet Propulsion Laboratory. Universal Detection Technology is seeking funding to adapt the method for use as a "nonimmunological approach" to detecting bacterial agents. "As part of the effort to deter biological terrorism and strengthen the capabilities of the biodefense and public health laboratory response, it is important to explore both classic and alternative methods and approaches to address the critical need to rapidly detect bacterial biothreat agent antigens and toxins of interest," the company said in the press release.

Libya Receives Chemical Disarmament Deadline Extension

Libya has received another extension of the deadline to eliminate its stockpile of chemical warfare materials, the Organization for the Prohibition of Chemical Weapons announced Friday. Tripoli is believed to hold about 25 metric tons of a sulfur-mustard mixture stored in bulk containers. Libya in 2004 joined the Chemical Weapons Convention, which originally required the state to eliminate the chemical arsenal by April 2007. Member nations to the convention in 2006 gave Libya its first deadline extension, allowing the nation until the end of 2010 to finish off the banned materials. The new final deadline is May 15, 2011. As of late October, construction of Libya's chemical-material destruction plant was not believed to have started. Representatives from 122 of the 188 CWC states met in The Hague, Netherlands, for their annual meeting from Nov. 30 to Dec. 4. They approved the appointment of Turkish diplomat Ahmet Üzümcü as the next OPCW director general and signed off on the agency's 2010 budget of $109 million.

Israel's Home Front Command simulates CBRN strike

Israel's Home Front Command has begun joint exercises with Magen David Adom and the Shaare Tzedek Medical Center to prepare for chemical, biological, radiological and nuclear missile attacks. The simulated attacks, which consist of three missiles hitting a Jerusalem neighborhood in quick succession, leave hundreds of people injured by a chemical substance. The victims are rushed by Home Front Command and Magen David Adom ambulances to a large site prepared by Shaare Tzedek Medical Center. Before the injured can receive medical attention, they must first be cleaned of the chemical substance. They are covered with a talc-based powder to absorb the chemical before being rinsed and taken to receive appropriate medical procedures. The Shaare Tzedek Medical Center is able to treat several hundred wounded during emergency situations. To test its capacity, the exercise sends 200 wounded citizens through its door, taking two hours to decontaminate them all. More than 100 soldiers took part in the exercise, which was deemed a great success, acted as a means of reassuring the

government and citizens to the readiness of its soldiers for a biological or chemical attack."I am very satisfied," Col. Yoram Lev-Ran, Commander of the Home Front Command Jerusalem District, told the Israel Defense Forces. "The civilian and military medical staff cooperated very well during the exercise. The system treating civilians in this kind of situations isn't natural, it's made up of a lot of bodies and organizations. We work on connecting them as well as possible, and I think that this sends a strong message to the Israeli public." More exercises will be performed by the Home Front Command over the coming months at hospitals throughout the country to practice and improve preparedness in emergency situations.

Call for 'more realistic' chemical attack drills

More "realistic" exercises should be conducted to improve emergency responses to any chemical and biological attacks on civilians, the Royal Society warns today. Training operations have failed to test the preparedness of the NHS, and the Government Decontamination Service (GDS) "has conducted only desktop" rehearsals, according to a study by the UK's leading independent scientific academy. In a follow-up to an earlier critical assessment published in 2004, the society acknowledges that progress has been made in planning for terror attacks and major contamination incidents. But training exercises were found to be inadequate. "There is a need for more scenario-based exercises to underpin all risks generic response … The GDS is a particular concern having only conducted desktop exercises. "One major issue is that current exercises stop at the door of the accident and emergency departments and therefore do not test the entire medical response. This is a particular problem given that hospitals are at full capacity and in the case of an emergency there will be the additional burden of the worried well." The report, Making the UK safer – a five year review, has been produced by a scientific committee chaired by Herbert Huppert, a Cambridge University geophysicist. It welcomes the creation of the Department of Health's medical intelligence unit and a newly established medical intelligence staff with MI5's joint terrorism analysis centre. But the report calls for more doctors to be educated in the treatment of victims of chemical and biological incidents. Some lessons could be learned from the NHS's preparation for the flu pandemic, it is suggested. Huppert told the Guardian: "We would like to see more openness and the involvement of more academic scientists in counter-terrorism work. The GDS needs a complete overhaul and rethink, so as to be more effective and better connected and be able to carry out the decontamination at the time of an incident. "There has been no real involvement of civilians [in exercises], to determine how they would react, nor a situation where the details are unknown to all those taking part, which is what will happen in a real event. The exercises have often not continued into hospitals and so hospital staff have not been prepared for a large inflow of seriously ill patients." The study also cautions that the public has not been informed sufficiently about potential dangers, while responsibility for military and government co-ordination is "dispersed" across too many agencies. "Concerns remain over the central co-ordination and direction of the work required to improve the UK's capability for detection and response to chemical and biological incidents," the paper states. Responsibility currently rests primarily with the Home Office, and its Office for Security and Counter-Terrorism (OSCT). There is also a counter-terrorism science and technology centre in the Ministry of Defence that deals with chemical and biological detection and contamination. The government rejected a key recommendation in the Royal Society's initial 2004 report that a unified centre should be established to coordinate

preparations. The Royal Society notes that: "UK capabilities are dispersed over several institutions and organisations making fully co-ordinated and cross-cutting scientific research difficult. Concerns that OSCT is understaffed [on chemical, biological and radiological issues] and that there is a lack of continuity of expertise reflect the need to consolidate efforts across government." Equipment purchased is not standardised and there is a "lack of interoperability" between the police and other emergency services, the study says. Much of the funding for research on chemical and biological detection and decontamination comes from the US and too little from the UK and Europe. The study also criticises the technical knowhow of the GDS. "Significant concerns have been raised in recent years over the science capability of the GDS, which operates as a broker for contractors rather then providing decontamination capability," the report adds. On communication with the public, the Royal Society suggests: "It is possible to mitigate panic and influence behaviour if reliable information is provided in advance of an incident and if clear messages can be provided during an incident." A Home Office spokesperson said: "The UK currently faces a substantial threat from international terrorism. The government is committed to doing everything it can to reduce this threat. "By 2011, we will be spending £3.5bn a year on countering terrorism. A wide range of exercises, from table top to full operations, are held to test and improve the UK's response to a number of threats."

Pentagon Looks to Breed Immortal 'Synthetic Organisms,' Molecular Kill-Switch Included

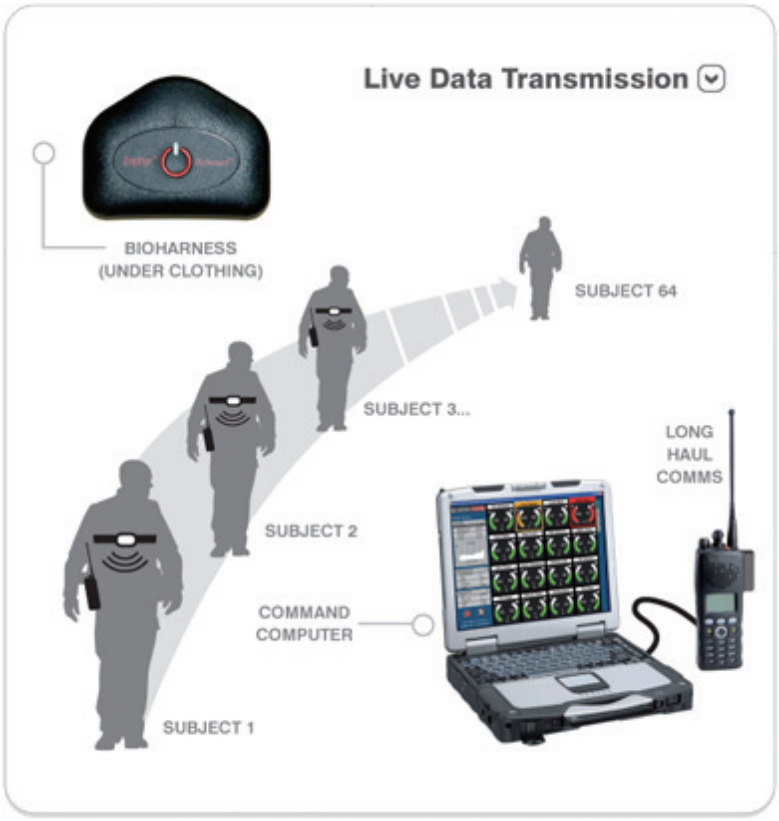
The Pentagon's mad science arm may have come up with its most radical project yet. Darpa is looking to re-write the laws of evolution to the military's advantage, creating "synthetic organisms" that can live forever — or can be killed with the flick of a molecular switch. As

part of its budget for the next year, Darpa is investing $6 million into a project called BioDesign, with the goal of eliminating "the randomness of natural evolutionary advancement." The plan would assemble the latest bio-tech knowledge to come up with living, breathing creatures that are genetically engineered to "produce the intended biological effect." Darpa wants the organisms to be fortified with molecules that bolster cell resistance to death, so that the lab-monsters can "ultimately be programmed to live indefinitely." Of course, Darpa's got to prevent the super-species from being swayed to do enemy work — so they'll encode loyalty right into DNA, by developing genetically programmed locks to create "tamper proof" cells. Plus, the synthetic organism will be traceable, using some kind of DNA manipulation, "similar to a serial number on a handgun." And if that doesn't work, don't worry. In case Darpa's plan somehow goes horribly awry, they're also tossing in a last-resort, genetically-coded kill switch: Develop strategies to create a synthetic organism "self-destruct" option to be implemented upon nefarious removal of organism. The project comes as Darpa also plans to throw $20 million into a new synthetic biology program, and $7.5 million into "increasing by several decades the speed with which we sequence, analyze and functionally edit cellular genomes." Of course, Darpa's up against some vexing, fundamental laws of nature — not to mention bioethics — as they embark on the lab beast program. First, they might want to rethink the idea of evolution as a random series of events, says NYU biology professor David Fitch. "Evolution by selection is nota random process at all, and is actually a hugely efficient design algorithm used extensively in computation and engineering," he e-mails Danger Room. Even if Darpa manages to overcome the inherent intelligence of evolutionary processes, overcoming inevitable death can be tricky. Just ask all the other research teams who've made stabs at it, trying everything from cell starvation to

hormone treatments. Gene therapy, where artificial genes are inserted into an organism to boost cell life, are the latest and greatest in life-extension science, but they've only been proven to extend lifespan by 20 percent in rats. But suppose gene therapy makes major strides, and Darpa does manage to get the evolutionary science right. They'll also have a major ethical hurdle to jump. Synthetic biology researchers are already facing the same questions, as a 2009 summary from the Synthetic Biology Project reports: The concern that humans might be overreaching when we create organisms that never before existed can be a safety concern, but it also returns us to disagreements about what is our proper role in the natural world (a debate largely about non-physical harms or harms to well-being). Even expert molecular geneticists don't know what to make of the project. Either that, or they're scared Darpa might sic a bio-bot on them. "I would love to comment, but unfortunately Darpa has installed a kill switch in me," one unnamed expert tells Danger Room.

PSM Responder

The Zephyr™ First Responder System (FRS) offers visibility into the physical status of personnel deployed in the most challenging environments. Deployed over existing digital radio equipment, FRS offers a low hassle, cost effective way to help improve the safety of you team, and to help optimize mission outcomes. Designed for squads of people deployed in the harshest environments, the Zephyr™ FRS enables the monitoring of multiple individuals and teams simultaneously. The Zephyr™ FRS is for Fire Fighter teams, HAZMAT, WMD CST, or any teams that deploy into potentially hazardous, challenging environments. Knowing the real-time physical status of personnel can assist Incident Commanders and Safety Officers in their decision making at the fire-ground. The FRS deploys over existing voice radio systems, thus increasing a fire-fighter's situational awareness, while minimising weight, hassle and the cost of deployment. The Smart Fabric strap can be worn as a chest strap, or as a fully integrated shirt. Being fabric based, the BioHarness™ strap does not impact the wearer's ability to perform their duties and does not result in skin irritation over time.



Seventy percent of Army's chemical weapons stockpiles destroyed

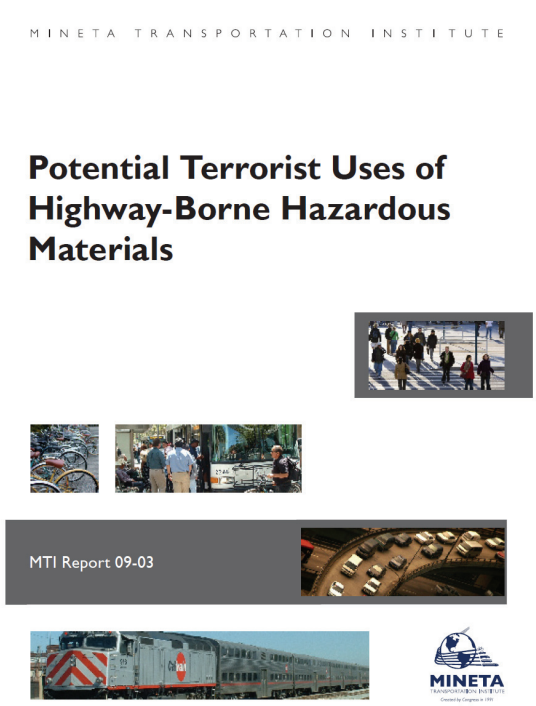
"U.S. Army officials have announced that more than 70 percent of the Army's chemical weapons stockpiles have been destroyed with the majority expected to be destroyed by 2012. The United States' arsenal includes 31,500 tons of chemical weapons, made up of sarin, VX and mustard agents. To date, 22,322 tons of that arsenal have been destroyed. 'It is a tremendous success story,' Carmen Spencer, deputy assistant Secretary of the Army (Elimination of Chemical Weapons), told Army.mil. 'Not only is the U.S doing all it can to meet its international commitments, but more importantly the Chemical Materials Agency is contributing to the national security of the United States in the process. These weapons in the wrong hands can do harm. They are safely and securely storing and destroying them while providing maximum protection to the public and environment.'"

Death sentence for ex-Aum member Niimi finalized

"The death sentence for former senior AUM Shinrikyo cult member Tomomitsu Niimi has been finalized for his roles in 11 crimes killing 26 people as the Supreme Court rejected the defendant's objection [to] the top court's earlier ruling. With the decision by the court's Third Petty Bench dated Tuesday, Niimi, 45, will become the 10th person whose death sentence has been finalized over a series of crimes involving the cult group, which include the 1989 murder of a lawyer and his family, and two deadly sarin nerve gas attacks in 1994 and 1995." (Mainichi Daily News; 18Feb10)

Study on motor carrier hazmat transport theft and its possible use in terrorism

"The Mineta Transportation Institute (MTI), has published Report 09-03, Potential Terrorist Uses of Highway-Borne Hazardous Materials, which evaluates security risks created by truck-borne hazardous materials, particularly gasoline tankers. The Department of Homeland Security requested the report from MTI's National Transportation Security Center of Excellence (MTI's NTSCOE). MTI has also issued a companion report, MTI Report 09-04, Implementation and Development of Vehicle Tracking and Immobilization Technologies, a study by Brian Michael Jenkins, Bruce Butterworth, and Dr. Frances Edwards. It details specific developments in tracking and immobilization technology that can increase security. 'We consider gasoline tankers, and to a lesser extent, propane tankers to be the most attractive options for terrorists seeking to use highway-borne hazmat because they can create intense fires in public assemblies and residential properties,' said Brian Michael Jenkins, Director of MTI's NTSCOE. 'We strongly urge that DHS, State governments and the industry take a renewed look at flammable liquids and gases as a weapon of opportunity, and at a strategy to improve security measures and technology.'



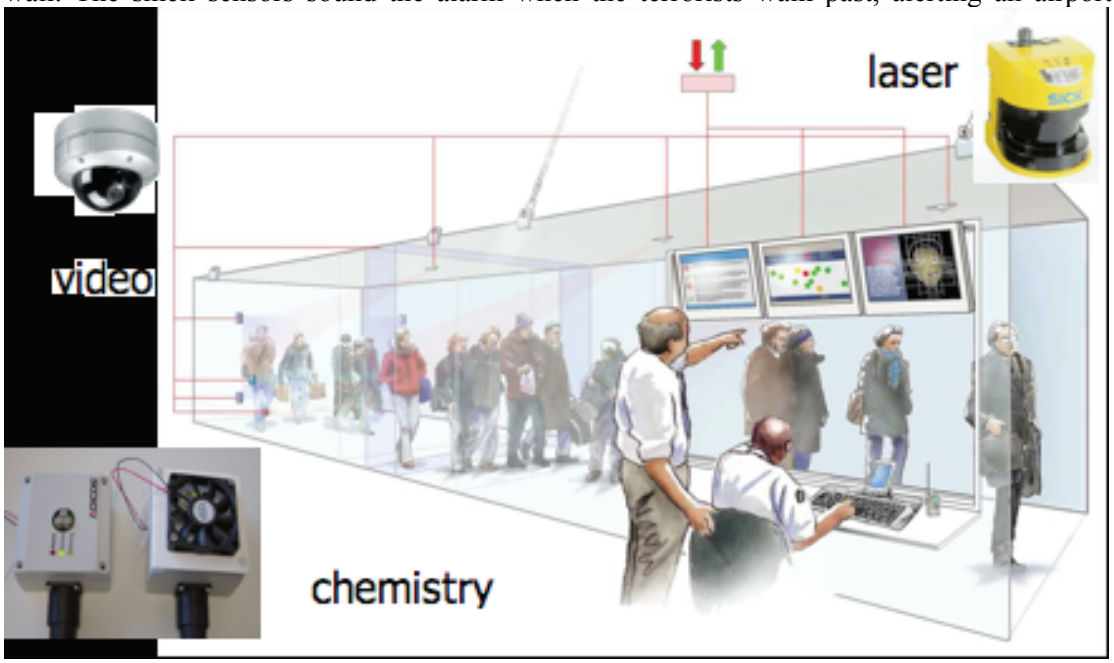
Al Qaeda's Quest for the Bomb

Recently the directors of CIA, FBI, and National Intelligence told Senator Dianne Feinstein that an attempted terrorist attack on the United States in the next few years was "a certainty." If Osama bin Laden and Ayman al-Zawahiri have anything to do with it, the attack is not likely to be an amateurish effort similar to that of the pathetic underpants bomber, Umar Farouk Abdulmutallab, who tried to blow up an airliner on Christmas Day. Nor will it be limited to blowing up buses and trains in London or Madrid. That may be good enough for European targets, but for the United States Al Qaeda seems determined to better 9/11 and do something really spectacular. This is the view of Rolf Mowatt-Larssen, a former C.I.A. official and Director of Intelligence and Counterintelligence at the Department of Energy. In a paper, written for Harvard's Belfer Center, Mowatt-Larssen details Al Qaeda's patient, decade-long effort to steal or construct an improvised nuclear device — the ultimate horror. The quest explains why Al Qaeda has not sought "the production of tactical, more readily available weapons such as 'dirty bombs,' chemical agents, crude toxins and poisons" that might do damage and take lives, but cannot compare to "the benefits of producing the image of a mushroom cloud rising over a U.S. city." Like 9/11, such an attack would alter "the course of history," Mowatt-Larssen writes. This could explain why bin Laden's deputy, Zawahiri, called off an attack on the New York subway system, holding out for "something better." A relatively easy attack using tactical weapons would not achieve the goals that Al Qaeda leaders have set for themselves, Mowatt–Larssen argues. Al Qaeda may be holding out for a truly strategic blow. Mowatt-Larssen details the efforts Al Qaeda has gone to get a nuclear weapon beginning in late 1993 and early 1994. According to an Al Qaeda defector, an attempt was made to buy nuclear material in South Africa in order to build an "improvised nuclear device" for $1.5 million. In 1996 Zawahiri himself was detained in Russia, but released by the security services. The speculation was that he was trying to buy a bomb. Zawahiri once said that for $30 million it should be possible to buy a suitcase nuke from a disaffected former Soviet scientist. In 1998 he took personal control of Al Qaeda's nuclear and biological weapons programs. That same year bin Laden issued a "fatwa" saying that it was a good Muslim's duty to "kill Americans and their allies, civilians and military ..." It was followed by the embassy bombings in Tanzania and Kenya. That December, bin Laden told a Time Magazine reporter that acquiring weapons of mass destruction "for the defense of Muslims is a religious duty." In 1999 a secret Al Qaeda biological weapons program was set up in a Kandahar laboratory. Anthrax seems to have been the weapon of choice. In the summer of 2001 a man matching the description of the 9/11 bomber Mohammed Atta tried to buy a crop-duster airplane in Florida. Zacarias Moussaoui, now serving a life sentence, was caught with crop-duster manuals. The list goes on. The Pakistani nuclear proliferator, A.Q. Khan, reportedly turned down an Al Qaeda request for help building a bomb. Ramzi Yousef, the World Trade Center bomber, planned to have cyanide gas "engulf the victims trapped in the North Trade Tower" in his failed attempt to bring down the building in 1993. But the explosion incinerated the gas. Despite its interest in chemical and biological weapons, Al Qaeda seems focused on the nuclear option. Its stated goal is to kill four million Americans. America's NATO allies with troops in Afghanistan might also be vulnerable. While the world focuses on Iran as the greatest potential source of nuclear proliferation, the clearest danger may be forming somewhere in Pakistan under the direction of Zawahri and bin Laden. And unlike Iran, Al Qaeda would have no reason to develop a bomb other than to use it.

Sniffing Out Terrorists

A new intelligent system has been developed to help identify terrorists carrying explosives. Sensitive electronic noses capture the smell of the explosives; the system processes the acquired data, correlates it with individuals' movements ... and ultimately tracks down the suspects. Literally hundreds of people are hurrying through the long airport corridor between Terminals A and B. Among them are two terrorists, who've hidden themselves in the crowd.

They're carrying small containers of chemicals in their jacket pockets, individual components for an explosive. But there's something the criminals don't know. As well as being observed by security cameras, they're also being "sniffed out" by chemical noses hidden in the corridor wall. The smell sensors sound the alarm when the terrorists walk past, alerting an airport



security guard who notes the problem on his monitoring equipment. At this point in time, he can't tell precisely who is carrying hazardous chemicals - but he knows the sensor network will continue to "sniff out" and track down the suspects. Researchers at the Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE in Wachtberg have built a prototype security system to replicate just such a scenario. They've named it HAMLeT, which stands for Hazardous Material Localization and Person Tracking. "HAMLeT will alert security personnel to suspicious individuals," says head of department Dr. Wolfgang Koch from the FKIE. The system involves a network of highly-sensitive smell sensors which follow an explosive's trail. There are oscillating crystals on the sensor chips, and whenever the electronic noses capture chemical molecules, their oscillation frequency changes. The precise nature of the change is different for different substances. A further component in the system - the sensor's data fusion function - traces the explosive's path and ferrets out the carrier. A second sensor network is needed to track the route the individual takes; for this, the researchers have used laser scanners. "HAMLeT's real achievement is its ability to collate all the data and convert it into a clear and accurate overall picture," says Koch. The sensor data fusion process employs complex algorithms which allow HAMLeT to build up a precise image of pedestrian flows and connect a particular smell with a specific individual. In a trial involving the German Armed Forces, researchers at the FKIE proved the system's ability to track down five "terrorists" carrying hidden explosives. The scientists are now working to refine the prototype's algorithms in order to reduce the false alarm rate.

Sonic tweezers could be the future of bioterror analysis

Sonotweezers, a device being developed by a collaborative research team with partners from Bristol, Dundee, Southampton and Glasgow Universities, may soon allow first responders to detect bioterror agents with a tweezer-like device that utilizes ultrasonics. When a potential anthrax mix is placed inside the sonotweezers, an ultrasonic force field will be generated onto the sample by an array of piezoelectric transducers. Differences in compressibility and density would then allow security officials to detect anthrax. The researchers developing the sonotweezers received a $6.4 million grant from the U.K. Engineering and Physical Sciences Research Council to complete research into the device by 2013. It is believed that the

tweezers could provide a variety of uses for homeland security. The tweezers are based on a silicon chip with an integrated cavity filled with an array of piezoelectric transducers. When a sample is placed inside this cavity, integrated transducers with varying voltage levels, phase and pulse shape will generate an ultrasonic force field onto the sample. From that force field, anthrax would be detected based on compressibility and density. "The different compressibility of powder relative to the cell means the force is different so you are able to differentiate them," Bruce Drinkwater, professor of ultrasonics in the Department of Mechanical Engineering at Bristol and team leader for the project, told HomelandSecurityNewswire.com. New chamber built to simulate battlefield for chemical agent sensor tests

Chamber to test, under realistic battlefield conditions, the viability of sensors designed to detect chemical warfare agents

The Defense Department's Joint Program Executive Office for Chemical and Biological Defense asked APL in 2006 to design and build the chamber, which will be used to evaluate technologies and systems to aid in the detection, protection against and decontamination of chemical warfare agents. "Our military operates over a wide range of battlefield conditions, whether it be in the high mountains of Afghanistan, the deserts of Iraq or off ships at sea," Thomas Buckley, of APL's National Security Technology Department and the Laboratory's project manager for the chamber, told The JHU Gazette. "All of these are potential venues for adversary use of chemical warfare agents." The chamber's realistic testing conditions will allow APL to test how quickly its military detectors can pick up trace level amounts of chemical warfare agents. "It operates over a wide range of temperature, humidity and simulated altitude while exposing the chemical agent detectors to interferents such as dust, smoke and diesel exhaust," he says. "Its control systems will allow the monitoring, displaying and recording of data from the systems under test in conjunction with the DTC challenge conditions to allow analysis of the response of the SUT in real time." The chamber is also the first of its kind to give real time agent characterization for all test scenarios and make available feedback of additional system parameters.

US Nuclear Weapons Site in Europe Breached

A group of people last week managed to penetrate deep onto Kleine Brogel Air Base in Belgium where the U.S. Air Force currently deploys 10-20 nuclear bombs.
Fortunately, the people were not terrorists but peace activists from a group known as

Vredesactie, who managed to climb the outer base fence, walk cross the runway, breach a double-fenced security perimeter, and walk into the very center of the air base alongside the aircraft shelters where the nuclear bombs are thought to be stored in underground vaults. The activists penetrated nearly one kilometer onto the base over more than an hour before a single armed security guard appeared and asked what they were doing. Soon more arrived to arrest the activists, who later described: "The military blindfolded for hours, they forced us to kneel in the snow, arms outstretched at 90° and threatened us if we intend to return to the base in the months to come." The activists videotaped their entire walk across the base. The security personnel confiscated cameras, but the activists removed the memory card first and smuggled it out of the base. Ahem… In June 2008, I disclosed how an internal Air Force investigation had concluded that most nuclear weapons sites in Europe did not meet US security requirements. The Dutch government denied there was a problem, and an investigative team later sent by the US congress concluded that the security was fine. They might have to go back and check again. The nuclear bombs at Kleine Brogel are part of a stockpile of about 200 nuclear weapons left in Europe after the Cold War ended. Whereas nuclear weapons have otherwise been withdrawn to the United States and consolidated, the bombs in Europe are scattered across 62 aircraft shelters at six bases in five European countries. The 130-person US 701st Munitions Support Squadron (MUNSS) is based at Kleine Brogel to protect and service the nuclear bombs and facilities. The activists will likely be charged with trespassing a military base but they should actually get a medal for having exposed security problems at Kleine Brogel. And this follows two years of the Air Force creating new nuclear command structures and beefing up inspections and training to improve nuclear proficiency following the embarrassing incident at Minot Air Force Base in 2007. Despite that, the activists not only made their way deep into the nuclear base but also discovered that the double-fence around the nuclear storage area had a hole in it! "We're not the first," one of the activists said. NATO needs to get over its obsession with nuclear weapons and move out of the Cold War and the

Obama administration's upcoming Nuclear Posture Review needs to bring those weapons home before the wrong people try to do what the peace activists did.

Rings of Terror

While we will be entering a world where the al Qaeda organization will come to matter less, today it still remains as the central point of reference. A scan of the current jihadi landscape

reveals that there are roughly six degrees of al Qaeda affiliation, each of which poses its own threat and requires a different response.

1. Al Qaeda's original leadership. The first group is made up of al Qaeda's original leadership -- and it is shriveling up like the roster of the local VFW. This crew still has a few big names: still-at-large figures like Osama bin Laden, Ayman al-Zawahiri, and Abu Yahya al-Libi. But the original core of al Qaeda is shrinking fast. No one knows the exact composition of this highest-level group, nor its exact whereabouts. But the best intelligence suggests the members live somewhere in the vicinity of Pakistan.

2. Al Qaeda's regional subsidiaries. Next, there are members of al Qaeda's regional subsidiaries, local terrorist or insurgent groups that have declared allegiance to the group. This includes outfits such as al Qaeda in the Islamic Maghreb, al Qaeda in the Arabian Peninsula, Ansar al-Sunnah in Iraq, al-Shabab in Somalia, and segments of the Taliban. These organizations do not take operational direction from al Qaeda's core, but accept broad strategic guidance. They are often critical to al Qaeda's efforts to expand its jihad throughout the globe. Al Qaeda, in turn, exploits these proxy groups, often mired in regional conflicts, to co-opt nationalist struggles into its broader narrative. Often, the senior leaders of these regional insurgent-cum-terrorist groups are in contact with original senior al Qaeda leadership.

3. Associated free agents. Associated free agents are individuals who are not official members of any terrorist group, but still have a connection, such as the radicals who carried out the 2004 Madrid train bombing. Their exact relationship to al Qaeda is often the most difficult to pin down because their affiliation tends to be fluid. Two days after the Madrid attacks, investigators found a video recorded by a man named Abu Dujan al-Afghani, taking credit for the attack and claiming to be al Qaeda's "European military spokesman." But a two-year probe into the plot found little evidence that the Madrid bombers really had al Qaeda

support. Their exact relationship to al Qaeda remains clouded, though there is overwhelming circumstantial evidence.

4. Entrepreneurial jihadists. Next, there are groups of entrepreneurial jihadists: radicals from outside conflict zones who nurse simmering grievances and conceive small-bore plots, rather than attempting spectacular attacks. These groups exist mostly in Europe, but also in the United States, Canada, and Australia. Entrepreneurial jihadists do not form organizations out of shared conflict experience or with the help of an al Qaeda associate, though they might try to establish contact with al Qaeda for training and equipment. Virtually any British terrorist cell, the Toronto 18, and the Somali immigrants involved in the recent plot out of Australia can be considered entrepreneurial jihadists. Often, these entrepreneurial jihadists come into violence through gateway groups like Hizb ut-Tahrir or the Muslim Students Association. Former radical Islamist Ed Husain offers an excellent account of this dynamic in his memoir, The Islamist: Why I Became an Islamic Fundamentalist, What I Saw Inside, and Why I Left.

5. Lone wolves. Lone wolves are individuals who share al Qaeda's ideology but have no connection with al Qaeda or any terrorist organization for that matter. Nidal Hassan, the Fort Hood shooter, is a classic case of a lone wolf terrorist -- someone who was radicalized by jihadi ideology, but who did not take instructions from jihadists. Lone wolves develop their missions on their own; if they managed to connect with like-minded individuals, they could move up to the entrepreneurial jihadist category. Most often, their operations are limited in their scale, scope, and effectiveness.

6. "Armchair jihadists," or jihadist pundits. These individuals share al Qaeda's ideology, but have no operational role in the organization. Still, their threat is insidious; although these individuals do not conduct operations, their ideology is disseminated, often over the Internet, and helps to radicalize others. Radical Yemeni preacher Anwar al-Awlaki is a jihadist pundit who has been responsible for radicalizing not just Nidal Hassan, but others as well.

Visa security is critical to preventing terrorist attacks

Umar Farouk Abdulmutallab's failed attempt to bomb Northwest Airlines Flight 253 on Christmas Day is another reminder that a visa is priceless to a terrorist. It is the golden key that allows easy passage to the United States. If the intelligence on Abdulmutallab had been properly analyzed, his visa would have been quickly revoked and he would have been denied access to Flight 253. We must go back to basics and strengthen the role of the Homeland Security Department in visa issuance, review and security. Certainly, we must continue to improve methods and technologies for screening and detecting explosives carried by airline passengers, but our highest priority is to remember the lesson of the Sept. 11, 2001, terrorist attacks and the attempted Christmas Day bombing: Our first line of defense against terrorism is intelligence and visa security. Yes, visa security. It's not an easy, 30-second sound bite and it takes a little more explaining, but it might be our best defense. Without a valid visa, America's enemies will not be able to lawfully enter the United States at all. This does not mean we should in any

way diminish America's role as a gateway to visitors from around the world. Common-sense security measures and an open and welcoming culture are not mutually exclusive. Revoking Abdulmutallab's visa would have done nothing to interfere with the travel plans of any other passenger boarding a flight to America. When it was initially revealed that the United States granted visas to the Sept. 11 terrorists, Congress wisely directed the new Homeland Security Department to take a larger role in visa security. Prior to that, the State Department had exercised a historically lax approach to visa security. As DHS' first undersecretary for border and transportation security, it was my responsibility to fulfill the congressional mandate to establish a visa security office, deploy visa security agents to priority and at-risk embassies, and identify visa seekers who might pose a risk to the United States. Before DHS was created, visa security checks were limited. Consular officers would interview visa applicants at U.S. embassies worldwide, they would conduct automated name checks against watch lists of known terrorists, and they would obtain the applicants' fingerprints and a digital photograph. Now a visa security agent complements the State Department's efforts, applying a keen law enforcement perspective to further check applicants who are either "not yet known" or flagged, to stop them from reaching the United States. The DHS visa security office's deployment of agents to embassies has been limited due to resistance from the State Department and a lack of funding. State contends its employees do the job adequately and that visa security agents can do their work remotely in Washington. Clearly the former is inaccurate; the Christmas Day bombing attempt is a case in point. But what of the latter assertion? The DHS inspector general has found that the successful vetting of visas requires a hands-on presence at the embassy. On the ground, visa security agents can better connect local intelligence (such as that given by Abdulmutallab's father to the U.S. embassy in Nigeria). They also can re-interview applicants if necessary, applying trained law enforcement and security perspectives the State Department simply does not offer. In one instance cited by the IG in a July 2008 report, an applicant applied for a student visa at an overseas embassy. Based on available information, the consular officer initially approved the application. The visa security agent further vetted the applicant and produced information revealing that the applicant's uncle was the subject of a terrorism investigation. Because of the agent's work, additional information was provided to the FBI about the uncle and, based on the agent's recommendation, the consular officer denied the student visa. In 2007 alone, DHS visa agents recommended denials due to security concerns for more than 700 visa applicants. Regrettably, agents are posted in fewer than 15 embassies, which is less than 10 percent of all U.S. embassies and consulates. This needs to change immediately. Logic suggests that if hundreds in high-risk areas have been denied visas, other locations might also require a close look. What is more, America's enemies are smart and resourceful. Soon they will figure out where their chances of obtaining a U.S. visa are greatest, if they haven't done so already. There is another advantage to the role of Homeland Security deploying visa security agents, and that is another avenue of redress in the event an error is made and a legitimate traveler is wrongly denied a visa. A visa security agent can review the intelligence and provide checks and balances for an imperfect human system. Congress must place a priority on funding these critical visa security positions. The Obama administration needs to make sure the State and Homeland Security departments are working together on this important mission because, as it is, nearly a decade after the Sept. 11 attacks, terrorists still are arriving on planes. As President Obama said, this is "totally unacceptable."

Asa Hutchinson, president and chief executive officer of Hutchinson Group consulting in Little Rock, Ark., is former undersecretary for border and transportation security at DHS.

An American suicide bomber?

"As for the Taliban fighters, they not only don't cherish life, they expend it freely in suicide bombings. It's difficult to imagine an American suicide bomber," Washington Post pundit Richard Cohen opined in a recent column. A few columns later Cohen returned to this theme, which clearly matters considerably to him: "There is really no such thing as an American suicide bomber. We don't extol the bomber and parade his or her children before the TV cameras so that other children will envy them for the death of a parent. This is odd to us. This is chilling to us. This is downright repugnant." Cohen added, "Maybe we have come to cherish life too much." The Cold War turned the entire United States into a suicide bomber rehearsing obsessively for the moment when we would 'push the button' and take down millions of our enemies with us. Seen in this light, Americans trained for the biggest suicide bombing mission of all." Reading Cohen's words made me recall a passage written by the anthropologist Renato Rosaldo, my graduate adviser. Rosaldo was classified 1-A for the draft during the Vietnam War while he was doing fieldwork with the Ilongot headhunters of the Philippines. "[The Ilongot] immediately told me not to fight in Vietnam, and they offered to conceal me in their homes. . . . Unthinkingly, I had supposed that headhunters would see my reluctance to serve in the armed forces as a form of cowardice. Instead, they told me that soldiers are men who sell their bodies. Pointedly, they interrogated me: 'How can a man do as soldiers do and command others to move into the line of fire?' This act of ordering one's own men (one's 'brothers') to risk their lives was utterly beyond their moral comprehension." Rosaldo's story reminds us that judgments of what is "repugnant" when it comes to war may vary across cultures and that, while Cohen worries that "we cherish life too much," the U.S. way of war may seem abhorrent and unnatural in other parts of the world. Thus, the proverbial anthropologist from Mars might wonder, along with British psychoanalyst Jacqueline Rose, why it is, when it comes to judging suicide bombers, that "dropping cluster bombs from the air is not only less repugnant: it is somehow deemed, by Western leaders at least, to be morally superior." Wondering why suicide bombers attract such scorn in the West, Rose can only say, "Why dying with your victim should be seen as a greater sin than saving yourself is unclear." She wonders if it has to do with "the unbearable intimacy shared in their final moments by the suicide bomber and her or his victims." That anthropologist from Mars might note that many people in the Middle East feel about U.S. drone attacks the way Richard Cohen feels toward suicide bombers. The drone attacks are widely perceived in the Middle East as cowardly, because the drone pilot is killing people on the ground from the safety of an air-conditioned pod in Nevada, where there is no chance that he can be killed by those he is attacking. He has turned combat into hunting. In this regard, the drone is the culmination of a long tradition of colonial war-fighting technologies--going back at least to the machine guns with which British and French colonial soldiers mowed down spear-carrying Africans--that ensure that the "natives" die, in an unfair fight, in considerably larger numbers than the colonial soldiers. The drone operator is also a mirror image of the suicide bomber in that he too deviates, albeit in the opposite direction, from our paradigmatic image of combat as an encounter between warriors who meet as equals risking the wounding or killing of their own bodies while trying to wound or kill the others' bodies. The honorable drama of combat lies in the symmetrical willingness of warriors to wager their bodies against each other for a cause. But now, in the words of the anthropologist Talal Asad,

in his book On Suicide Bombing, U.S. "soldiers need no longer go to war expecting to die, but only to kill. In itself, this destabilizes the conventional understanding of war as an activity in which human dying and killing are exchanged." (Asad's words clearly apply more to drone operators than to foot soldiers on patrol in Afghanistan). While it takes a lot more courage--or desperation--to be a suicide bomber than a drone pilot, suicide bombers and drone pilots each undercut the normative script of combat by depriving their enemies of the chance to kill them in return. (As Asad points out, the state will intervene to prevent a condemned person from committing suicide so that they can be executed instead. It's somehow essential to the order of things that a person's body be destroyed by legitimate authority, not by their own hand.) Just war theory and the laws of war have little to say about either suicide bombers or drone operators. They focus on the proportionality and legality of the means of violence and on the legitimacy of the targets, not on whether the person pushing the button is near or far from his targets or whether he deliberately perishes with them. Thus, while we may feel a visceral revulsion toward suicide bombers, according to just war theory, the main question in judging them is whether they have acted in a just cause, whether they have used a legitimate technology of violence (bombs, good; gas, bad), and whether they have primarily targeted soldiers or civilians. And so, just war theorists would presumably condemn a suicide bomber who blew herself up on a bus in Jerusalem, but not the suicide bomber who killed seven people at a CIA base in Afghanistan. And, Richard Cohen's own words notwithstanding, it isn't too hard to imagine him writing a future column extolling the noble sacrifice and just cause of an American who penetrated Al Qaeda and got close enough to Osama bin Laden to give him a taste of his own kamikaze medicine. Yet we don't have to imagine hypothetical future scenarios of suicide attacks on bin Laden to see that Cohen is already wrong when he writes, "There is really no such thing as an American suicide bomber." Leaving aside the epidemic of U.S. "suicide shooters" such as Eric Harris and Dylan Klebold at Columbine High School in Colorado and Nidal Hasan at Fort Hood in Texas, who shoot others and either kill themselves or expect to be shot, there remains the question of America's suicidal dance with the biggest bomb of all--the atomic bomb. For decades loyal U.S. soldiers in nuclear missile silos have trained to launch their weapons in the expectation that they would be killed almost immediately afterwards in the ensuing nuclear war. I once interviewed a former special-forces officer who was trained to hike behind enemy lines with a tactical nuclear weapon on his back and place it near an important target. Although the weapon had a timer, he expected to die at ground zero. If such men were the elite nuclear suicide bombers whose mission was prepared but never carried out, the Cold War turned the whole country into a suicide bomber rehearsing obsessively for the moment when we would "push the button" and take down millions of our enemies with us. Seen in this light, Americans trained for the biggest suicide bombing mission of all. David Rohde of the New York Times reports that the Taliban have a song with the lyrics, "The Americans have the atomic bomb; we have suicide bombers." The Taliban presumably mean by this that suicide bombers are their greatest military asset, one that strikes fear into the hearts of their enemies. But there are other points of comparison between suicide bombers and atomic bombs as well and, while the Taliban presumably don't intend the comparison to call into question the legitimacy of suicide bombing, their lyric surely invites us to take a fresh look at our military and to ask ourselves, in a way that our mainstream pundits have failed to do, how much the U.S. way of war is built upon a concern to "cherish life," both our own and others'.

Is the cyber threat a weapon of mass destruction?

Google's surprise announcement of "a highly sophisticated and targeted attack" on its systems--a case of computer-aided espionage--has also raised the specter of offensive warfare. Defense News quotes Adm. Robert Willard of U.S. Pacific Command as declaring that "the skills being demonstrated" by Chinese hackers in the service of "exfiltrating data"--a fancy way of saying "spying"--are also relevant to "wartime computer network attacks." If that's not alarming enough, last week, Gerald Posner added a new entry in the annals of hype

in a piece he wrote for the Daily Beast: "While Google weighs exiting China, a classified FBI report says [Beijing] has already developed a massive cyber army [that is] attacking the U.S. with 'WMD-like' destruction capabilities." In the last few years, it's become almost a rite of

passage among federal employees to have their computer networks partially shut down for days or weeks after an intrusion, usually (but not always) attributed to China." Posner's assessment is clearly excessive. But recent years have seen a growing tendency to treat "the cyber threat" as a "strategic" problem, sparking an interest in "cyber deterrence." U.S. Strategic Command even appears to have incorporated computer network attacks into the existing U.S. nuclear declaratory policy, based on the idea of "calculated ambiguity." Last May, Gen. Kevin Chilton of STRATCOM told journalists, including the Global Security Newswire's Elaine Grossman, "You don't take any response options off the table from an attack on the United States of America," including a cyber attack. When "cyber attack" means a form of spying, General Chilton's statement will come across as extreme. But it's certainly possible that the ability to compromise computers will play a role in future war-fighting. (Aaron Mannes and James Hendler identified some realistic possibilities in a Washington Times op-ed last August.) Still, let's keep the matter in perspective: If the United States were ever to get into a shooting war with another nuclear weapon state, cyber attacks would be the least of anyone's worries. The Google Affair underscores that there is a different sort of "strategic" cyber threat. Today's issues of global concern hinge in large part on the state of U.S.-Chinese relations: stabilizing the world economy in the wake of the fiscal crisis, shoring up the nuclear nonproliferation regime, and achieving effective cooperation to forestall the worst effects of climate change, to name the most salient issues. And let's be blunt: Pervasive spying via the internet is harming China's relations with the United States. In the last few years, it's become almost a rite of passage among federal employees to have their computer networks partially shut down for days or weeks after an intrusion, usually (but not always) attributed to China. Everyone from the Office of the Secretary of Defense to the Commerce Department has been a target. And in certain circles, there are few computing experiences more familiar and less delightful than receiving the dreaded socially engineered e-mail attack--an authentic-looking message, seemingly from a known person, but with a nasty PDF attachment. In other words, not every intrusion of this type is as systematic and well-planned as the December 2009 raid on Google, Adobe, and other U.S. firms. Any American who works on Asia-Pacific security issues or has an interest in human rights in China has probably been aware of the problem for some time. If they haven't received an e-mail probe personally,

chances are good they will know someone who has. The damage to goodwill has been considerable. It isn't shocking that one major power spies on another, or necessarily even intolerable. As the saying goes, "It's all in the game." But the game has never been friendly, and there's something breathtakingly crude about how it's being played today. The attempt to capture as many computers as possible is aggressive and indiscriminate, reaching into the lives of private citizens in the United States and beyond. In a particularly insidious turn, the spies have been known to take advantage of professional contacts between Americans and Chinese in order to assemble convincingly spoofed messages and to mine e-mail address books for targets. All of this effort is aimed at getting the targets to open the attachments. No serious attempt is made to cloak where the attacks are coming from, should a fake message be spotted. That's especially striking in contrast to the technical and social sophistication of the probes. These practices are, quite frankly, abusive and uncivilized. And the mechanical denials of Chinese officials do as much harm to the country's image as the scattershot spying itself, if that's possible. As it happens, spying is not the same as warfare. But it does harm regardless.

Hand-held Detection Devices

Sometime this year, the U.S. Army plans to provide troops in Afghanistan with hand-held sensors that can peer through walls, detect buried explosives and spot enemy fighters hiding behind vegetation or sneaking through underground tunnels. The devices use low-power ultra-wideband radio-frequency - or RF - waves to produce images of what's concealed by wood, stone, brick, concrete and dirt. The Army's Expeditionary Warrior Experiments program hopes that these small RF imagers will help U.S. forces counter the war zone's most deadly threat: buried roadside bombs. The devices can produce clear images of objects by penetrating "any non-metal structure," including "walls, glass, floors, concrete, ground, culverts, etc., up to six feet depth," an Army document says. The sensors' creator, TiaLinx, Newport Beach, Calif., says some of the sensors can see through more than 10 feet of earth. TiaLinx has developed three models, said Fred Mohamadi, the company's chief executive. Two are designated as Eagle5s, the other is the Eagle60.

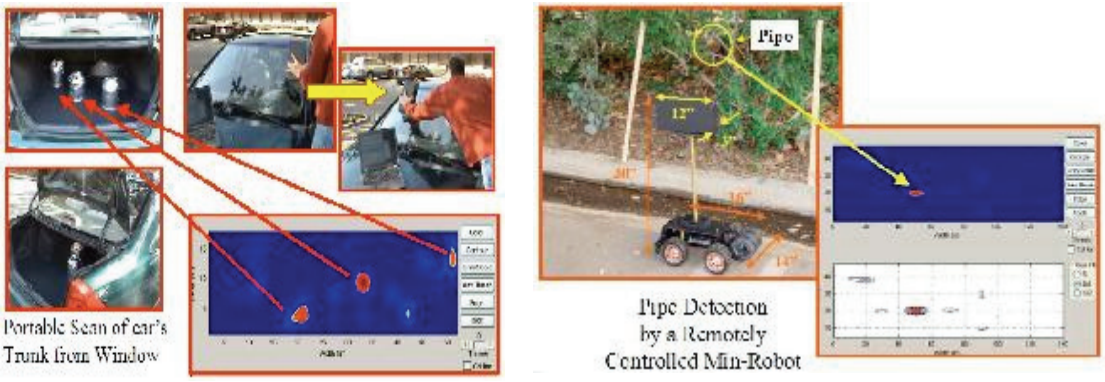
The **Eagle5 scanners** - an M model and a P model - pump out radio waves at 5 gigahertz, a frequency that gives them substantial penetrating capability even at extremely low power.
The M model is designed to detect motion, including movements as small as a heartbeat or breathing. Tialinx says the device can detect people or animals farther than 20 feet behind an 8-inch-thick concrete slab.
The P model is designed to penetrate the ground and can locate tunnels, people in tunnels and buried objects at depths greater than 10 feet, the company says. Both of the Eagle5 models can also be used as motion sensors for stand-off surveillance of buildings, trails and other areas.

The **Eagle60** operates in the V-band, a higher frequency that enables it to produce sharper images. But the clearer picture comes at a price. The Eagle60 cannot penetrate as deeply as the lower-frequency Eagle5-P.

"That's the nature of radio frequency," Mohamadi explained. "As the frequency goes higher, the extent of penetration reduces because of attenuation." That is, the higher-frequency signal diminishes faster as it moves out from its source.

A Better View Than Radar

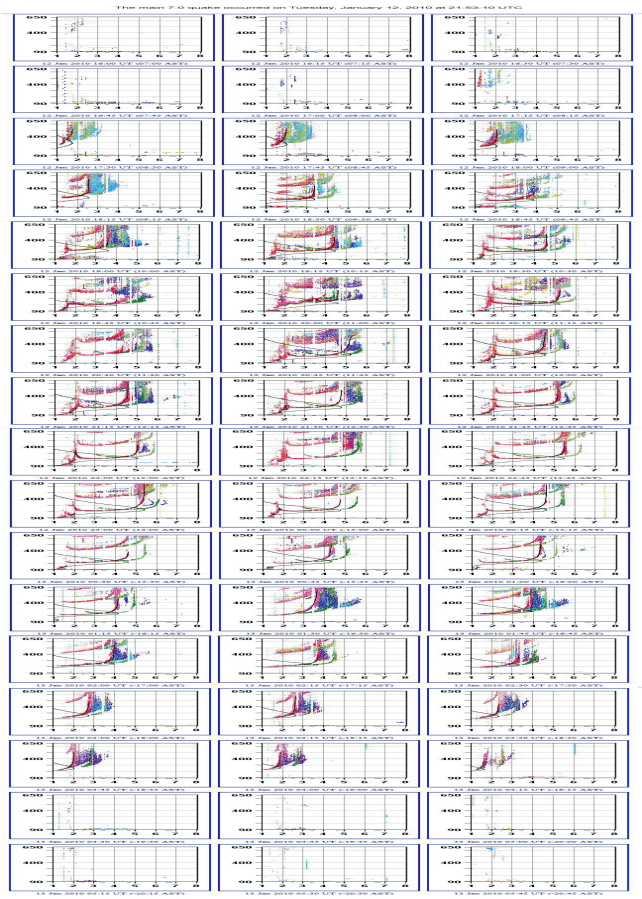
The Eagle imagers offer the U.S. military an alternative technology to ground-penetrating radar. And Mohamadi said his company's imagers are superior for several reasons. One is that they transmit ultra-wideband signals. In a sense, that enables the Eagle sensors to get a more complete view of hidden objects. Most ground-penetrating radars use a narrow band of signals and offer a more limited view, and are more prone to producing false readings, Mohamadi said. Ultra-wideband signals are also less affected by environmental factors such as rain, snow and fog that degrade the performance of many radars, he said. Ultra-wideband sensors also consume much less power. "The energy we transmit is a fraction of that that is used by a cell phone," Mohamadi said. Thus, ultra-wideband sensors can be made smaller and lighter, and they require less support in the field. The Eagle5s look something like a cross between a video game controller and an oversized cell phone. Each weighs 3.5 pounds. The ground-penetrating 5-P is about a foot long, 8 inches wide and 3 inches thick. The motion-detecting 5-M is about half that size. The higher-frequency Eagle60 weighs about 6 pounds and is roughly the size of the 5-P. The devices run on batteries and can operate for about four hours between recharges. In each case, the sensors have an antenna that sends radio-frequency pulses toward a target and a receiver that detects the pulses that bounce back. A signal processor built into the device analyzes the returned pulses, and a complex algorithm turns them into an image of the object they bounced back from. The image is displayed on a small screen on the Eagle device and can be transmitted wirelessly to a nearby computer to be



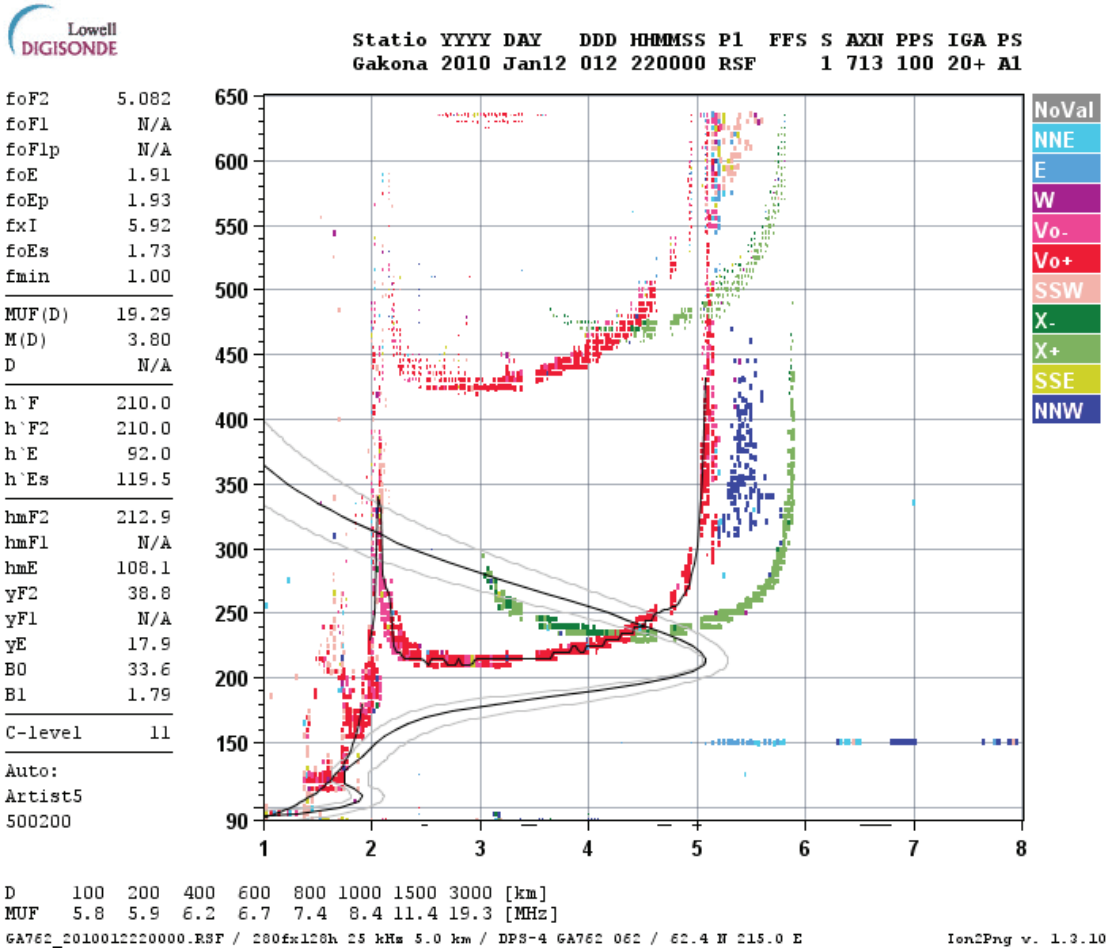
further analyzed and displayed. Their wireless capability also means that the devices can be mounted on ground-crawling robots or small unmanned aerial vehicles to search areas that are considered too dangerous or inaccessible to humans. They can report their findings instantly from as far as 300 feet away. The Expeditionary Warrior Experiments program describes the RF imagers as "user friendly" in a catalog of emerging technologies it says show promise for use on the battlefield. Simply "turn on, calibrate, then point and scan," the Army says, noting that the imagers show promise for use against buried improvised explosive devices. Funding to develop even more advanced versions has been provided by the Office of Naval Research, the Air Force Research Laboratory and the Defense Advanced Research Projects Agency, TiaLinx said. But the military is not the only potential customer, Mohamadi said. The Department of Homeland Security, the Justice Department, intelligence agencies, police departments and utility companies all might have uses for the Eagle sensors, he said. The ground-penetrating Eagle5-P could be used to find broken underground pipelines, to find victims in collapsed buildings and hostages in locked rooms, to locate water or oil leaks underground, to find smugglers' tunnels along the U.S. border or to detect activity in tunnels and underground bunkers, he said.

Αϊτη-Ο σεισμός προκλήθηκε από δοκιμή νέου αμερικανικού υπερόπλου?

Πληροφορία που προήλθε από τον ρωσικό στόλο, αναφέρει ότι ο σεισμός της Αϊτής προκλήθηκε από δοκιμή νέου αμερικανικού «σεισμικού όπλου», το οποίο δοκιμάστηκε με το ενδεχόμενο να χρησιμοποιηθεί εναντίον του Ιράν. Παρόμοια αποκάλυψη έκανε και ο πρόεδρος της Βενεζουέλα Ούγκο Τσάβεζ, υποστηρίζοντας ότι πρόκειται για υπόγεια αμερικανική δοκιμή ενόψει του πολέμου με το Ιράν. Πληροφορία του τηλεοπτικού σταθμού Russia Today, αναφέρει ότι και η Μόσχα έχει κατηγορηθεί για την κατοχή και χρήση



παρόμοιου όπλου. Το 2002 ηγέτης πολιτικού κόμματος στη Γεωργία είχε κατηγορήσει τη Ρωσία ότι επίτηδες προκάλεσε σεισμική δόνηση στη Γεωργία. Ανεπιβεβαίωτες πληροφορίες αναφέρουν ότι τον προηγούμενο μήνα ανάλογη «σεισμική δοκιμή» είχαν πραγματοποιήσει οι ΗΠΑ και στον Ειρηνικό, με αποτέλεσμα να προκληθεί σεισμική δόνηση μεγέθους 6.5 Ρίχτερ, που έγινε αισθητή και στην πόλη Εύρηκα της Καλιφόρνια. Με τον τρόπο αυτό επιβεβαιώνεται η υποψία πως "κάτι γνώριζαν οι ΗΠΑ" και για το λόγο αυτό είχαν "προτοποθετήσει" στο νησί τον υποδιοικητή του Νότιου Στόλου ναύαρχο P. K. Keen. Για να βρίσκεται εκεί και να επιβλέψει στην διακίνηση της βοήθειας που "αν χρειαζόταν" θα έστελνα εκεί οι ΗΠΑ. Οι δοκιμές αυτές εντάσσονται στο πρόγραμμα High Frequency Active Auroral Research Program (HAARP), που μπορεί να προκαλέσει καιρικές ανωμαλίες, όπως πλημμύρες, ξηρασίες και τυφώνες. Μελετητές, έχουν συνδέσει το πρόγραμμα αυτό με το ενδεχόμενο να είχε δοκιμαστεί και στην πρόκληση του σεισμού 7,8 Ρίχτερ που είχε σημειωθεί στην κινεζική πόλη Sichuan στις 12 Μαΐου 2008. Το πρόγραμμα αυτό δοκιμάζεται στις ΗΠΑ από το 1970 και αρχικά είχε επικεντρωθεί στη δημιουργία "shockwave bombs". Η Ρωσία είχε ήδη καταγγείλει τον αμερικανικό στρατό ότι χρησιμοποιεί παρόμοια όπλα και ότι τα είχε χρησιμοποιήσει πτοκαλώντας τον φονικό σεισμό των 7,2 Ρίχτερ στο Αφγανιστάν, το Μάρτιο του 2002. Στα μέσα του 1990 στην Κρατική Δούμα της Ρωσίας είχε γίνει επερώτηση από 90 βουλευτές που υποστήριζαν ότι οι ΗΠΑ δημιουργούν ένα νέο γεωφυσικό όπλο που μπορεί να προκαλέσει αναταράξεις στον φλοιό της Γης με υψηλής συχνότητας ραδιοκύματα".



Airliner C4 Threat

Homeland security people are concerned (due to intel intercepts and interrogations) about al Qaeda bringing bombs aboard airliners that do not look like bombs. They are worried that moldable C4 is going to be fashioned into objects that appear harmless (like statuettes, knickknacks, etc.) and carried onto airliners or placed in checked baggage. The puffers (if the explosive was on someone's person) and swab-style mass spectrometers (4 types) would detect these explosives, but only a tiny percentage get this treatment. They are also worried that C4 could be perfectly molded into the inside of things like personal DVD players and go right through scanners without being detected. If they device is not swabbed, it could go right through with no problem. For example, you could cut the tops off of batteries, remove the guts, replace the guts with C4, replace and fasten the battery tops, and place the batteries in electronic devices and get them right aboard. Be on the lookout for closer TSA scrutiny being applied to electronic devices.

Somali Pirates and Ammonium Nitrate

Al Shabab, Somalia's al Qaeda franchise that controls part of the country's pirate industry, is hopefully being heavily monitored with various US intel assets in part because several of the ships they have seized are/were carrying ammonium nitrate (AN), a very powerful high explosive when properly mixed and rigged (Tim McVeigh used AN in OKC and the US Embassies in Nairobi and Dar es Salaam were destroyed with AN IEDs). In November 2009, that other terrorist (also Shabab) flying from Mogadishu to Dubai was caught with an explosive whose primary ingredient was ammonium nitrate (NOT PETN). Shabab has been

offloading some of the AN from seized vessels with the intent to use it against US and other Western targets in Africa, Yemen, the Middle East and elsewhere. Do not be surprised if we have been trying like mad to observe the offloading and follow the AN as it gets moved by truck and dhow (mostly), and considerable assets have been assigned to track the stuff. Very serious warnings have been issued regarding this threat. Expect the DoD and CIA's SAD to have both trained for missions to seize pirated vessels carrying AN that are anchored off Somalia. Also, we have the ability (obviously) to use air strikes to hit vehicles and dhows carrying AN away from its original vessel. More than one high-ranking DoD official in the decision/recommendation loop has said we should consider sinking pirated AN vessels while at anchor.

Bioterrorism And Disaster Preparedness

According to a study in a special issue of Medical Decision Making, a large-scale, covert anthrax attack on a large city would overwhelm hospital resources even with an extremely effective public health response, primarily because of expected delays in detecting the attack and initiating a response to it. The article "Predicting Hospital Surge after a Large-Scale Anthrax Attack: A Model-Based Analysis of CDC's Cities Readiness Initiative Prophylaxis Recommendations," examines one of the CDC's principal bioterrorism-response programs, the Cities Readiness Initiative (CRI), a program that recommends the medical countermeasures necessary to minimize the hospital surge resulting from anthrax-related illness and response in the first two days after a major bioterrorism attack. The researchers found that a CRI-compliant prophylaxis campaign starting two days after exposure would protect as many as 86% of exposed individuals from illness. However, each additional day needed to complete the campaign would result in as much as 3% more hospitalizations in the exposed population. Unsustainable levels of hospitalizations would result from delays in detecting and initiating response to large-scale, covert aerosol anthrax releases in a major city, even with highly effective mass prophylaxis campaigns. The article, written by Nathaniel Hupert, incorporates some of the latest type of modeling techniques scientists use in the disaster preparedness.field. Such models have become increasingly important to public health officials and hospital administrators. To improve the consistency and quality of these models, the Society for Medical Decision Making convened experts to recommend best practices for modeling the public health response to a terror attack. Their article, also published in the current issue of Medical Decision Making, is entitled "Recommendations for Modeling Disaster Responses in Public Health and Medicine: A Position Paper of the Society for Medical Decision Making." The authors examined a large selection of published mathematical and simulation health sector disaster response models to generate a set of best practice guidelines. They made several recommendations, including striking the appropriate balance between simplicity and complexity, designing a plan to evaluate the many uncertainties inherent in disaster response, and good model reporting of the disaster response. in the article, "Evaluating the Capability and Cost of a Mass Influenza and Pneumococcal Vaccination Clinic via Computer Simulation" researchers set out to determine the best way a clinic could vaccinate as many as 15,000 clients in 17 hours, including such factors as how to best configure the personnel to maximize the number of clients vaccinated; and to estimate the costs and revenue of such an undertaking. The researchers found that it was possible for

the clinic to reach its target and that using a computer simulation could help them determine the most efficient use of staff, machinery, supplies, and time. "How hospitals and public health agencies are prepared for an attack--and how they respond to the surge in patients seeking care—will determine our success in containing an attack if one happens."" said Mark Helfand, editor of Medical Decision Making.

Russia destroys first ton of war gas sarin

"The first ton of the warfare gas sarin was destroyed at the chemical weapons destruction facility Maradykovsky in the Kirov region. The destruction of this substance, which is a nerve agent, was launched on July 27, and more than 1,100 kilograms of sarin has already been destroyed so far," chief of the regional department for conventional problems Mikhail Manin told Itar-Tass on Wednesday. […] Sarin was destroyed in 26 warheads at 9 a.m. Moscow time on Wednesday, after that their hulls were decontaminated and exposed to thermal processing. […] Manin also noted that inspectors of the Organisation for the Prohibition of Chemical Weapons, representatives from the working group of the Federal Agency for Safe Storage and Destruction of Chemical Weapons and the regional ecological monitoring center are monitoring round-the-clock the sarin destruction process. […] The Maradykovsky chemical weapons destruction facility is planning to destroy 231 tons and 119 kilograms of sarin by the year end. Some 4,833 aviation bombs and warheads of chemical missiles contain the foresaid war gas. Maradykovsky is the third Russian complex, which had launched the full-scale destruction of chemical weapons since September 2006. Since 1953 the complex has stockpiled more than 40,000 aviation bombs and warheads of chemical missiles staffed with the mixture of nerve agents. […] The Maradykovsky destruction facility is planning to launch the destruction of one more toxic agent - soman as of 2010. Russia will have destroyed the whole stock of toxic agents under Russia's international liabilities and the federal program for the destruction of chemical weapons in Russia by 2012."

New Mobile Trailer CBRN Detection Unit

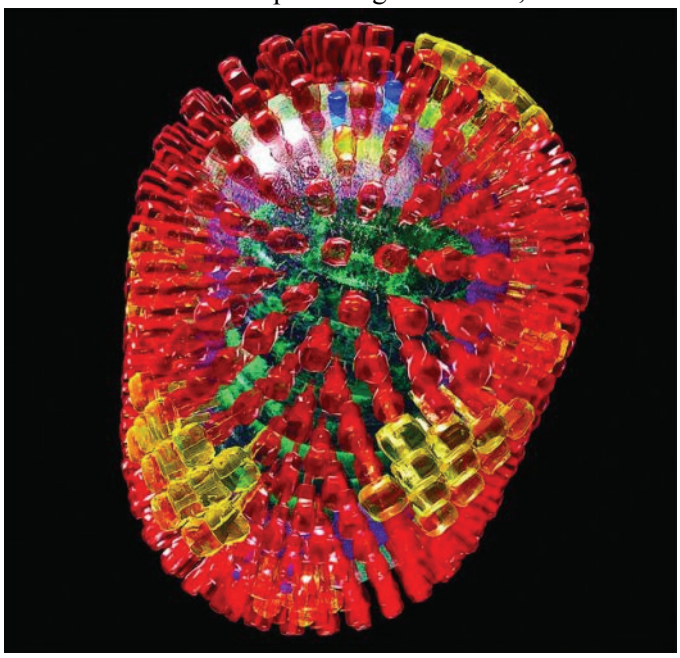
Building Protection Systems, Inc. (BPSI), the developers of the first complete building protection system to actively and reliably protect buildings and their occupants from airborne toxins, announced today that it has completed testing and is ready to deliver its new mobile trailer CBRN detection system. The Mobile Sentry One solution was developed at the request of various law enforcement agencies for the protection of VIPs at events while in their cities. "This mobile CBRN detection system solves a real protection problem when talking special security events," said Greg Eiler, CEO of BPSI. "Simply put, law enforcement would not know of an airborne toxic chemical attack or a dirty bomb release until it is too late. Now the Mobile Sentry One provides reliable, real-time information wherever it is needed." The Mobile Sentry One is based on the same reliable technology as BPSI's Building

Sentry One, which has been protecting Fortune 100 office buildings for more than 18 months in the absence of false alarms, an unheard of feat in the detection industry. Mounted inside a lightweight 4'w x 6'l x 5'h trailer, the rugged, shock resistant Mobile Sentry One system can be transported anywhere it can roll. The 120v hook-up allows for unlimited detection run time while the onboard battery power supply provides up to four hours of back-up operation. Optional solar and generator power supplies are also available. Each Mobile Sentry One trailer can be easily networked to other Mobile Sentry One trailers, providing complete perimeter protection from an airborne release or targeted attack. "BPSI's ability to transfer its reliable building protection system to a mobile platform further expands the level of protection it affords citizens from airborne toxins," said Tom Ridge, former U.S. Secretary of Homeland Security and head of Ridge Global, a strategic advisor to BPSI.

How it works, briefly
BPSI's Mobile Sentry One is the first trailer-mounted system that incorporates proven chemical and radiological (optional biological detection is available) sensor technology with proprietary firmware and software to reliably detect and identify an airborne toxic attack within seconds. In real time, the Mobile Sentry One communicates with the security command center providing toxin and location data and has the ability to automatically activate predetermined desirable protocols to mitigate the effects of the dangerous toxins.

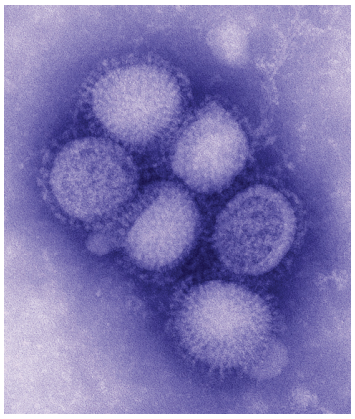
New Flu Treatment Outsmarts Mutations

Before swine flu swept through the U.S., the virus had bounced around South America undetected for years. The H1N1 strain caught scientists by surprise, and without a vaccine. But a few weeks before the first North American case popped up, researchers successfully tested a therapy that could knock out almost any flu, and possibly any virus. Conventional vaccines packed with inert versions of a flu strain give your immune system the chance to develop antibodies. These identify that strain's particular version of hemagglutinin, a lollipop-shaped protein on its surface, so your body knows what to kill if infected. Every strain's hemagglutinin has a slightly different head, so Robert Liddington, a biologist at the Burnham Institute for Medical Research in California, went after its stalk. "The lollipop head changes quite easily from generation to generation, but the stalk remains stable," he says. "It's the flu's Achilles' heel." His team found a rare antibody that targets it, injected it into mice, and exposed them to 10 times the lethal dose of several seasonal flu strains, the H5N1 bird flu and the pandemic-causing 1918 Spanish flu. The drug staved off serious infection in each case, even if administered 72 hours after the initial exposure. Liddington says the trick might work on viruses with similar proteins, such as HIV, but he is fast-tracking the flu drug, wrapping up tests in ferrets before handing it to the Centers for Disease Control and Prevention to oversee human trials. "Considering the recent outbreaks, expedience is the rule."



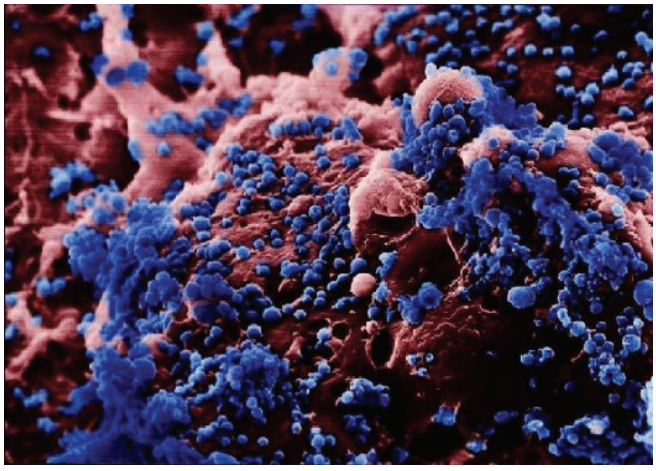
Swine Flu Consistent with Other Pandemic Strains

The Star of the Show : This virus is ready for it's close up courtesy of the Center for Disease



Control and Prevention. I know, I know. You had moved on. It was fun while it lasted, but you sent H1N1 your breakup mix tape, gave it back the underwear it left in your apartment, and now you've started a new relationship happily reading about the new BMW 7-series or possible Supreme Court nominees. Well, unfortunately, swine flu is still out there, and swine flu news wants to get back together. This time, we can make it work. Yes, despite the feeling that the swine flu story is SO April, there has actually been some important news as of late. The most important news came from a paper published online in Science yesterday. Researchers have completed their first analysis of the outbreak, and the report has some good news and some bad news. The good news is that that the virus isn't nearly as deadly as the 1918/1919 H1N1 pandemic flu or the H5N1 bird flu. The bad news is that, based on the spreading patterns so far, the outbreak will almost certainly reach a pandemic level. This quote from Nature News wraps it up nicely: "It's a virus that almost certainly will cause a global epidemic," says study author Neil Ferguson, an epidemiologist at Imperial College London. "But it's not the catastrophic scenario people were fearing for bird flu." The study concluded that if the virus sticks around for flu season in the Northern Hemisphere, about 20 to 30 percent of people will get the flu, up from around the 10 percent infection rate seen in the normal seasonal flu. Of course, like all models, the mathematical model that produced that 20-30 percent prediction relies on a number of assumptions about very complex systems. Over at Seed, Effect Measure takes a look at those assumptions and breaks down some of the questions in the model. While Seed and Nature News focus on the future of the outbreak, the Washington Post takes a look at the past of the swine flu. In this article, writer David Brown follows swine flu's family in Kansas, its hardscrabble climb to the big time in the 70s, its problems with drugs, and finally its big 2009 comeback tour. And Boing Boing highlights an educational video from the performance troupe The Art of Bleeding. It uses sexily-dressed nurses and a guy in a gorilla suit to answer all your swine flu questions. Frankly, I don't think its fair. They get to use revealing vinyl outfits and a dude dressed like a monkey to talk about swine flu, and all I get is a blue stained picture from a microscope.

A Cure for the Uncommon Flu



Ninety years ago the Spanish flu swept across the globe, killing between 50 and 100 million people in only a few months. Since then, the specter of another flu pandemic dealing death and woe around the world has periodically terrified the medical and popular communities. But scientists searching for ways to prevent a similar outbreak in the form of the H5N1 bird flu have found a cure for the deadliest flu in the most unlikely place: nonagenarian immune systems. A new paper in the journal Nature confirms that a team of doctors has succeeded in isolating pandemic-flu killing antibodies from 90+ year old survivors of the Spanish flu outbreak. To

test whether or not the antibodies still worked, the doctors injected the immune cells into mice, and then dosed the mice with preserved copies of the 1918 flu recovered from frozen victims of the Spanish flu that had been buried in Alaskan permafrost. Within those mice, the antibodies and the virus renewed a microscopic battle that had lain dormant for almost a century. The mice that received a high dose of the antibodies lived, while mice that received a low dose of antibody, or none at all, died as expected. While the authors of the paper indicated that understanding the immune system's ability to "remember" infections for so long could be useful in studying all manner of viral infection, it is unlikely that antibodies synthesized from survivors would be able to immediately help in a future bird flu pandemic. The 1918 Spanish flu and the modern Asian bird flu are different species, and the antibodies are probably not compatible. Rather, by understanding how the body produces and preserves flu antibodies over a lifetime doctors hope to be able to develop more effective vaccines specific to viruses like the bird flu. Currently, the common flu kills 30,000 Americans a year, so developing effective vaccines is important even without an outbreak of the more deadly pandemic strain of the disease.

Pandemics That Were And Weren't

1956/1958- The Asian Flu: Far less deadly than the Spanish flu, the Asian flu of 1956-1958 killed about 70,000 Americans. The strain mutated from an earlier H2N2 flu that had originated in Russia and gone pandemic in 1889. With its relatively low death rate and long duration, the Asian Flu perfectly exemplifies how most pandemics don't threaten the collapse of civilizations, but merely exacerbate the problems already caused by seasonal flu. A girl gargling broth in Sagamihara Hospital, Japan, during the 1957 flu outbreak, courtesy of the National Museum of Health and Medicine, via Flickr.com

More often than not, it's the newer diseases, like HIV or Ebola, that grab all the headlines. But those Johnny-come-lately microbes have nothing on one of the most dangerous, and most ancient, viruses that afflicts mankind: influenza. Medicine has grappled with the deadly influenza virus since the time of Hypocrites, and some historians have identified flu epidemics as far back as ancient Rome. In a regular year, the Center for Disease Control and Prevention estimates that 36,000 Americans die from the seasonal flu, while the virus costs the nation between $71 and $160 billion. That's ten times the death toll of 9/11 and double the cost of Hurricane Katrina, but it's far less noticeable, as the virus mainly kills the very old and very young, and the cost is spread out over the entire year in question. Every few decades, though, the virus mutates into a particularly virulent strain, and spreads across the globe as a pandemic. While only the 1919 flu pandemic managed to create scenes reminiscent of the Decameron, the other pandemics have pried at the chinks in society, negatively impacting the economy and boosting the already high mortality rates for influenza. At the same time, some flu strains that were predicted to cause a pandemic never became as deadly as they were expected to, leading to accusations from the public that the media "hyped" virus' threat level. With the current swine flu epidemic continuing to expand, PopSci.com takes a look back at notable flu pandemics, as well as some threats that never materialized.

Scientists successfully isolate Marburg virus from African fruit bats link

A team of scientists reported today the successful isolation of genetically diverse Marburg viruses from a common species of African fruit bat (Egyptian fruit bat, Rousettus aegyptiacus). A paper published in the open-access science journal PLoS Pathogens provides new insight into the identity of the natural host of this deadly disease, a puzzle that has long baffled scientists. Infection with Marburg virus and the related Ebola virus can produce severe disease in people, with fever and bleeding. During outbreaks, as many as 90 percent of those infected have died. The natural reservoir for Marburg virus, and its cousin Ebola virus, has been the subject of much speculation and scientific investigation. The study provides the strongest evidence to date of the species' capacity to host Marburg virus. While previous investigations have found antibodies to Marburg virus and virus genetic fragments in bats, the recent study goes significantly further by isolating actual infectious virus directly from bat tissues. The new study shows unambiguously that this bat species can carry live Marburg virus. In addition, this study identifies a genetic link between the viruses carried in bats and those found circulating in humans working near them, suggesting that these bats were the source of the outbreak. Genetic sequences of Marburg viruses obtained from the infected bats exhibit broad genetic diversity, suggesting that Marburg infection in Egyptian fruit bats is not a recent phenomenon. R. aegyptiacus isgenerally cave-dwelling and widely distributed across sub-Saharan Africa. Many caves and mines are inhabited by large populations of R. aegyptiacus. Caves, as popular tourist attractions, and active mines can invite potential close contact between bats and humans. By identifying the natural source of this virus, appropriate public health resources can be directed to prevent future outbreaks. Additionally, the study takes scientists one step closer to identifying the reservoir host for Ebola virus.

A Novel H3N2 Influenza A Variant Emerges

While the pandemic 2009 H1N1 influenza A virus continues to spread globally, it may not be the only significant influenza challenge we face this year. A new H3N2 variant has emerged that may be poorly matched to the 2009 seasonal influenza vaccine. This could pose a risk to the older population and to those who have been vaccinated against the pandemic strain. Since 1968, H3N2 has been the dominant strain in most influenza seasons. It has been implicated in more severe annual flu outbreaks than seasonal H1N1, and it harbors almost universal resistance to the adamantane class of drugs. Over the past few months, the H3N2 virus has been accumulating genetic changes that may diminish the protectiveness of the seasonal influenza vaccine.

Antigenic Drift Found in H3N2

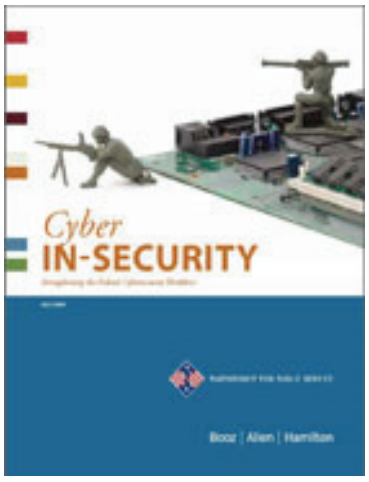
A genetically drifted variant of the H3N2 strain of virus was uncovered in March. The mutated virus was first discovered in samples taken from an influenza outbreak within a nursing facility. It was found to have 3 mutations at 2 different antigenic sites when compared to the vaccine strain A/Brisbane/10/07 (H3N2), which was included in the current season's vaccine for both hemispheres. It is also to be included in the 2009-2010 vaccine. The virus has been found to represent a minority of isolates in the current Southern Hemisphere flu season but has been deemed capable of becoming the dominant strain of H3N2. The WHO has been unable to assess the full potential of this new variant due to strain on resources from the concomitant H1N1 pandemic.

The New Strain Could Complicate and Worsen the Flu Epidemic

While information on the clinical illness caused by the H3N2 variant and the amount of protection conferred by the seasonal vaccine is not yet available, the fact that a vaccine mismatch might exist is worrisome. While a mismatch to a single component of the trivalent influenza vaccine is not uncommon, for this coming season, it could mean a substantial

increase in the number of flu victims. This is because H3N2 viruses have a penchant for disproportionately affecting the elderly, who have been largely spared by the pandemic strain now circulating. Also susceptible to the variant H3N2 virus would be those vaccinated against the pandemic strain. As a result, the coming flu season could be driven by a combination of these two viruses and could afflict a greater proportion of the population than would be vulnerable to either the novel H1N1 influenza A virus alone or to the seasonal flu alone. The emergence of this drifted variant of H3N2 underscores the vital need for continual surveillance of influenza isolates of all subtypes, as the propensity for this virus to alter its genetic components will also pose an obstacle to crafting efficacious vaccines.

Report Finds Inadequate Federal Cybersecurity Workforce

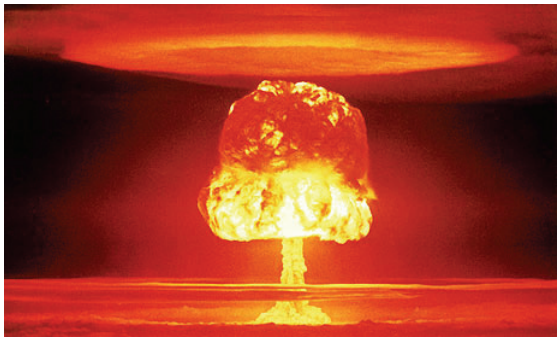


"Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce," a report by the Partnership for Public Service and Booz Allen Hamilton, produced **four major findings:**

- ✓ The pipeline of potential new talent is inadequate.
- ✓ Fragmented governance and uncoordinated leadership hinders the ability to meet federal cybersecurity workforce needs.
- ✓ Complicated processes and rules hamper recruiting and retention efforts.
- ✓ There is a disconnect between frontline hiring managers and government's human resources specialists.

Terrorists could use internet to launch nuclear attack: report

Terrorists groups could soon use the internet to help set off a devastating nuclear attack, according to new research. The claims come in a study commissioned by the International Commission on Nuclear Non-proliferation and Disarmament (ICNND), which suggests that under the right circumstances, terrorists could break into computer systems and launch an attack on a nuclear state – triggering a catastrophic chain of events that would have a global impact. Without better protection of computer and information systems, the paper suggests, governments around the world are leaving open the possibility that a well-coordinated cyberwar could quickly elevate to nuclear levels. In fact, says the study, "this may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves". Though the paper admits that the media and entertainment industries often confuse and exaggerate the risk of cyberterrorism, it also outlines a number of potential threats and situations in which dedicated hackers could use information warfare techniques to make a nuclear attack more likely. While the possibility of a radical group gaining access to actual launch systems is remote, the study suggests that hackers could focus on feeding in false information further down the chain – or spreading fake information to officials in a carefully orchestrated strike. "Despite claims that nuclear launch orders can only come from the highest authorities, numerous examples point towards an ability to sidestep the chain of command and insert orders at lower levels," said Jason Fritz, the author of the paper. "Cyber-terrorists



could also provoke a nuclear launch by spoofing early warning and identification systems or by degrading communications networks." Since these systems are not as well-protected as those used to launch an attack, they may prove more vulnerable to attackers who wish to tempt another nation into a nuclear response. Governments around the world have recently stepped up their commitment to increasing cyber-defence, after a number of high-profile incidents in which hackers launched attacks on foreign nations. Recent online conflicts, as well as reported attacks on government computer systems in the US, UK and elsewhere have increased the stakes. In Britain, Gordon Brown recently announced plans to step up online intelligence operations – while in the US, President Obama has said he intends to appoint a cyber-security tsar to ensure that protecting America's computer systems "will be a national security priority". "Cyberspace is real, and so is the risk that comes with it," he said in May, adding that online attacks are "one of the most serious economic and national security challenges we face". However, the study suggests that although governments are increasingly aware of the threat of cyberwar with other nations, action to bolster those defences does not alleviate the threat of a rogue group that circumvented the expected strategies for online warfare. "Just as the 9/11 attacks were an unprecedented attack with unconventional weapons, so too could a major cyber attack," it says.

Securing Serbia´s Nuclear Legacy

A soft summer rain falls on a decrepit, rusting warehouse in the suburbs of Belgrade, Serbia. From the outside, all appears normal, nothing more than a shabby storehouse set against a small patch of trees. But inside, a pile of decades-old radioactive waste in deplorable condition has sat for decades, posing a threat to the health and safety of people and the environment. More than a thousand sealed radioactive sources remain inside - a half-century´s stock of radioactive refuse from the former Yugoslavia and Serbia. But the full picture of what´s inside this radioactive storehouse is a mystery, since precise records haven´t been kept. Such is the scene at the Vinča Institute of Nuclear Sciences, a large research campus that served as the nerve center for former Yugoslavia´s nuclear research activities since the late 1940s. Just a few kilometres from the Danube, the site has endured different periods of upheaval and influence, including varying degrees of Cold War-era intervention by the US and the Soviet Union. In 1959, the USSR supplied Vinča with the nuclear fuel and technical assistance to construct Vinča´s "RA" reactor, a 6.5 megawatt, heavy-water moderated research reactor capable of using fuel highly enriched in U235. The RA reactor was actually the second to operate at Vinča, and was preceded by the country´s first nuclear reactor, a heavy-water zero-power critical assembly (which is still in operation). There has been much speculation as to the original intentions for the facility under Yugoslavia´s then-leader Josip Broz Tito, and some research seems to indicate that a modicum of weapons research may have been conducted at Vinča in its early days. Changes in government, the breakup of Yugoslavia, and the NATO bombing campaign in 1999 are all factors that conspired to keep Vinča´s management, direction, and focus in a constant state of flux. These dynamics brought Vinča to where it is today; and serve as a prime example of capable scientists and sophisticated equipment falling prey to political winds of change. Concerns about Vinča on the part of the international community grew in the mid-1990s, when IAEA teams were dispatched upon Serbian request to inspect the site. These visits were instrumental in alerting the outside world about the state of the nuclear fuel on site, and the inherent risk to health and safety of those around Vinča. As part of the IAEA

and global community´s push to support reduced enrichment for research and test reactors, along with concerted efforts to return highly enriched uranium (HEU) fuel to the country of origin, an extraordinary level of international cooperation has coalesced to clean up Vinča. The first major step in the Vinča project took place earlier this decade, when the most urgent threat to proliferation was dealt with. In 2002, an international operation to return 48 kilograms of unirradiated HEU fuel of Soviet-origin came about after protracted negotiations between then-Yugoslavia, the US, Russia, the IAEA, and other parties. The transport of the fuel was conducted amid intense security, with over 1200 armed guards ushering a convoy of trucks to the Belgrade airport for a flight to Russia, where the HEU would then be down-blended to a low-enriched form. IAEA safeguards inspectors watched over the procedure by gauging the fissile material, inspecting records, and applying seals to the shipping containers.

Current Workload

Since return of the unirradiated HEU, the foremost priority has been to deal with two-and-a-half tons of Russian-origin irradiated, spent nuclear fuel elements, which were initially used in the RA reactor. As the reactor last went critical in 1984, the SNF has been stored for decades in aluminium barrels in an adjoining spent fuel pool. However, the pool´s water chemistry has been poorly maintained, leading to corrosion of the fuel element´s aluminium cladding and leakage of fission products into the storage pool, though not into the environment. The water´s condition is further degraded by an accumulation of sludge, increasing the pool´s turbidity and lending it an inky black colour. So the push is now on to repackage and repatriates the spent fuel for return to Russia, and the strong support and involvement of the Serbian Government has been instrumental in moving this project forward. An agreement between Serbia and Russia that governs the transfer of the fuel was signed this past June, and work is set to begin in autumn. Yet the task is fraught with complexities, and long lists of preparatory steps need to be taken to facilitate the fuel repacking and removal work. IAEA Director General Mohamed ElBaradei visited the facility in early July 2009, to assess the progress at Vinča. "The unused nuclear waste is in poor condition and needs to be moved as soon as possible. The situation is under control for now, but it could be very dangerous from a safety and security point of view," he commented. To remove, characterize, and repackage Vinča´s spent fuel, technologically unique operations will have to be performed. Sludge in the pool needs to be removed, custom fuel handling equipment needs to be designed and fabricated, and enhanced radioactivity monitoring systems need to be installed before repackaging begins. The fuel also needs to be stabilized and undergo thorough analysis before it can be removed. Finally, roads leading to the spent fuel storage room need to be reinforced to increase loading capacity and access for the trucks, cranes, and steel casks that will be used in the operation. Over 50 experts and technicians have been assigned for the task ahead. A target date of the end of 2010 has been set for the shipment, and work is set to begin in autumn 2009 to begin the fuel repackaging portion of the project. "For the Vinča project, we´ve needed access to huge, expensive technologies to move this massive amount of fuel back to Russia," said John Kelly, the IAEA Special Programme Manager tasked with coordinating the Agency´s work.

Radioactive Waste

Yet another important dimension to the Vinča clean-up effort that the IAEA and the international community are helping Serbia with is the construction of new facilities to deal with the legacy of radioactive waste at Vinča. Two hangars chock-full of more than 1000 disused radioactive sealed sources and other radioactive waste have sat for decades in degraded condition. The sealed sources and waste need to be removed from the two aging hangars and conditioned for secure and safe storage in new long-term storage facilities. All told, the waste will be dealt with by a waste storage facility, a secure storage bunker, and a waste processing facility. These three systems are in various stages of development, but the IAEA has committed to working with Vinča and Serbian regulators to commission these new installations. A sealed source conditioning facility is also on the near horizon. The support to the radioactive waste management improvements includes safety and security assistance,

training and experts, facility upgrades, regulatory assistance, and equipment donations. Much like the spent fuel repatriation, the radwaste management project is expected to take several years to complete.

Importance of Success

Logistically and financially speaking, the Vinča Institute Nuclear Decommissioning (VIND) project is the largest Technical Cooperation programme in the Agency´s history. Several divisions within the IAEA have deployed technical officers to work on the project, which involves the Departments of Safety and Security, Nuclear Energy, Safeguards, Legal Affairs, Procurement Services and Technical Cooperation. The funding aspect has been particularly challenging and given the complexity of the operation, it is little wonder that the price tag is expected to be $47.5 million for the full spent fuel repackaging and repatriation portion. The VIND programme in total is projected to reach roughly $75 million. To date, Serbia, the EU, the Czech Republic, Russia, Slovenia, Italy, UK, USA and the Nuclear Threat Initiative (a non-government donor) have made contributions to the project. The IAEA has also provided support through deployment of equipment, experts, and other assistance. "With the vast amount of funding needed for the VIND project, pulling together such a disparate donor pool has been nothing short of miraculous," explained Kelly. "But momentum has been the key driver in making progress towards donations - when donors see you actually making progress, then they want to participate. Donors want to invest in success." VIND highlights the IAEA´s unique role and importance in collaborating with and coaxing financial assistance from a diverse donor pool. "We´re working closely with the Serbian government and our goals are identical," said ElBaradei. "We must ensure that there are no similar risks either here in Vinča or elsewhere in Serbia." Though undoubtedly an expensive venture, the work is necessary, as leaving the site in its current condition is not an option. The VIND project is a prime example of the international community coming together through the IAEA to solve an important and complex safety and security challenge. -- Dana Sacchetti, IAEA Press and Public Information Officer, Division of Public Information

Όπλο EMP εξουδετερώνει τις μηχανές αυτοκινήτων στα 200 μέτρα.

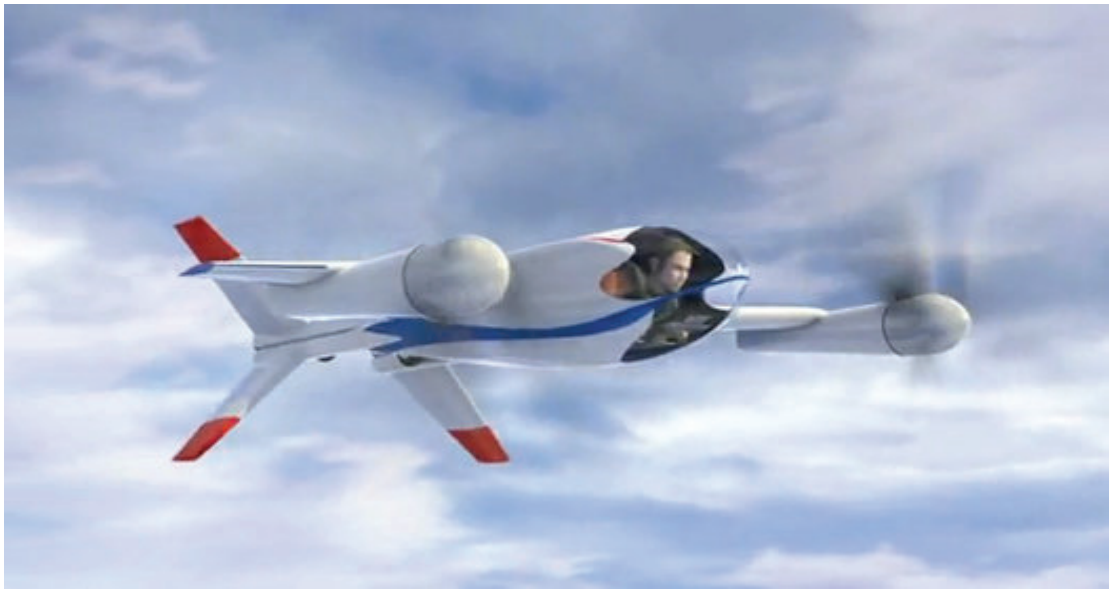
Μια καναδική εταιρεία προϊόντων υψηλής τεχνολογίας η Eureka Aerospace ισχυρίζεται πως έχει δημιουργήσει ένα όπλο ηλεκτρομαγνητικών παλμών με δυνατότητα να εξουδετερώνει τις μηχανές των αυτοκινήτων. Προς το παρών το όπλο που έχει επιδειχθεί είναι αρκετά μεγάλο

για να είναι μετακινούμενο, στα αμέσως όμως προσεχή χρόνια η Eureka Aerospace θεωρεί πως αυτό μπορεί να σμικρυνθεί σε σημείο που να ζυγίζει 50 έως 55 λίβρες έχοντας μια ακτίνα εξουδετέρωσης στα 700 πόδια απόστασης (230 μέτρα). Βασικός σκοπός της δημιουργίας του όπλου αυτού, σύμφωνα με την εταιρεία είναι η παροχή δυνατότητας στην αστυνομία να σταματά μια καταδίωξη υψηλής ταχύτητας κατά βούληση, αποτρέποντας έτσι την πιθανότητα αναστάτωσης

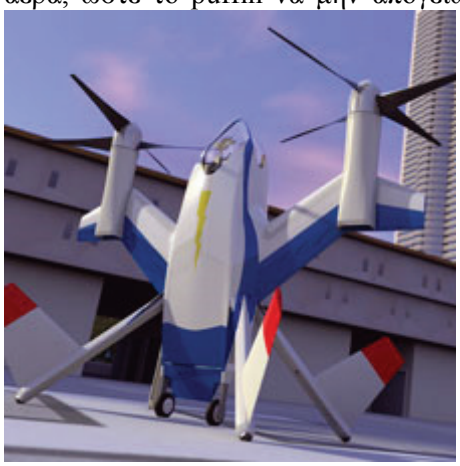
στους δρόμους των αμερικανικών πόλεων αλλά και της πρόκλησης ζημιών και αθώων θυμάτων. Πάντως το όπλο αυτό έχει επίδραση μόνο στα σύγχρονα αυτοκίνητα που χρησιμοποιούν ηλεκτρονικά συστήματα για τον έλεγχο λειτουργίας της μηχανής και μικροεπεξεργαστές και όχι στα παλαιότερης τεχνολογίας ιδίως αυτά που κατασκευάζονταν έως και τα μέσα της δεκαετίας του ΄70. Το όπλο ονομάζεται High Power Electromagnetic System (HPMES) και σύμφωνα με πληροφορίες έχει συγκεντρώσει το ενδιαφέρον του Σώματος Των Αμερικανών Πεζοναυτών αλλά και της Αμερικανικής Αεροπορίας η οποία έχει ζητήσει τη δημιουργία μιας αερομεταφερόμενης έκδοσης του όπλου από ελικόπτερα. Τόσο οι Πεζοναύτες όσο και η Αεροπορία αν και σκεπτικοί ακόμη απέναντι στις πραγματικές δυνατότητες του HPMES θεωρούν πως τόσο το Ιράκ όσο και το Αφγανιστάν θα μπορούσαν να αποτελέσουν κατεξοχήν πεδία δοκιμών του συστήματος.

Electric Icarus: Ηλεκτροκίνητο αεροσκάφος για ειδικές επιχειρήσεις

Ένα υπερβολικά ήσυχο με ικανότητα αιώρησης ηλεκτροκίνητο αεροσκάφος σχεδιάζει η NASA τον «Ηλεκτρικό Ίκαρο» προσπαθώντας να φέρει τις μετακινήσεις μέσω αέρος προσιτές στον καθένα. Το puffin (θαλάσσιος παπαγάλος) όπως είναι η ανεπίσημη ονομασία



του, όσο είναι στο έδαφος είναι σε κάθετη στάση στηριζόμενο σε τέσσερα πόδια που έχουν το χαρακτήρα του συστήματος προσγείωσης. Όσο οι δύο ηλεκτροκινητήρες του λειτουργούν όσο είναι στο έδαφος ειδικά πτερύγια καμπυλότητας σε εκταμένη θέση εκτρέπουν το ρεύμα αέρα, ώστε το puffin να μην απογειωθεί αλλά μόλις αυτοί είναι έτοιμοι τότε τα πτερύγια



μαζεύονται και το αεροσκάφος απογειώνεται, για να μετατρέψει την κάθετη του πτήση σε οριζόντια σε λιγότερο από ένα λεπτό. Το σκάφος είναι κατασκευασμένο από ανθρακονήματα έχει καθαρό βάρος μόλις 135 χλγ. και 180 χλγ. μαζί με τους συσσωρευτές λιθίου που διαθέτει για την κίνηση των ηλεκτροκινητήρων. Το puffin μπορεί να αναπτύξει ταχύτητα οικονομική 240 χαω, αλλά μπορεί να φτάσει μέχρι και τα 480 χαω. Το μέγιστο επιχειρησιακό ύψος θεωρητικά μπορεί να φτάσει τα 9150 μέτρα πριν οι συσσωρευτές εξαντλήσουν το δυναμικό τους, ενώ η εμβέλειά του με τις σημερινές τεχνολογίες μπορεί να φτάσει τα 80 χλμ. οι επιστήμονες όμως της NASA θεωρούν πως μέχρι το

2017 με τις τεχνολογίες που πρόκειται να αναπτυχθούν για τους συσσωρευτές η εμβέλεια θα μπορεί να φτάσει έως και τα 320 χλμ. Το συγκεκριμένο σχέδιο έχει προσελκύσει και το ενδιαφέρον του αμερικανικού στρατού καθώς ένα τέτοιο σύστημα θα μπορεί να χρησιμοποιηθεί για διεισδύσεις ομάδων ειδικών επιχειρήσεων με απόλυτη μυστικότητα καθώς το σύστημα πρακτικά δεν παράγει θόρυβο

Moving Through Time

Although we can't technically travel through time (yet), when we think of the past or the future we engage in a sort of mental time travel. This uniquely human ability to psychologically travel through time arguably sets us apart from other species. Researchers have recently looked at how mental time travel is represented in the sensorimotor systems that regulate human movement. It turns out our perceptions of space and time are tightly coupled. University of Aberdeen psychological scientists Lynden Miles, Louise Nind and Neil Macrae conducted a study to measure this in the lab. They fitted participants with a motion sensor while they imagined either future or past events. The researchers found that thinking about past or future events can literally move us: Engaging in mental time travel (a.k.a. chronesthesia) resulted in physical movements corresponding to the metaphorical direction of time. Those who thought of the past swayed backward while those who thought of the future moved forward. These findings reported online in Psychological Science, a journal of the Association for Psychological Science, suggest that chronesthesia may be grounded in processes that link spatial and temporal metaphors (e.g., future= forward, past= backward) to our systems of perception and action. "The embodiment of time and space yields an overt behavioral marker of an otherwise invisible mental operation," explains Miles and colleagues.

Llama Proteins Could Play a Vital Role in the War on Terror

Scientists at the Southwest Foundation for Biomedical Research (SFBR) in San Antonio have for the first time developed a highly sensitive means of detecting the seven types of botulinum neurotoxins (BoNTs) simultaneously. The finding may lead to improved techniques for testing water and food supplies should BoNTs be used as a bioterrorism weapon. The BoNT- detecting substances are antibodies --proteins made by the body to fight diseases--found in llamas. BoNT are about 100 billion times more toxic than cyanide, and collectively, they are the only toxins in the federal Centers for Disease Control and Prevention (CDC) 'category A' list of potential bioterror threats alongside anthrax, Ebolavirus and other infectious agents.

The llama antibodies, called single domain antibodies (sdAb) or "nanobodies," are molecularly flexible, unlike conventional antibodies. "As such, sdAb may allow biosensors to be regenerable and used over and over without loss of activity. Also, for some types of BoNT, conventional antibodies are not generally available and we are filling this biosecurity gap," said Andrew Hayhurst, Ph.D., an SFBR virologist. Since some sdAb have been shown to have inhibitory activity and can block toxin function, they may play a role as part of a future anti-botulism treatment. The new work, funded by the Defense Department's Defense Threat Reduction Agency Medical Diagnostics Program, is described in the Jan. 21 issue of the journal PLoS ONE. BoNTs are made by specific strains of the bacterium Clostridium, which are widely distributed in soils and aquatic sediments. Most cases of botulism are the result of improperly stored foods, which can encourage growth of Clostridia and production of toxin, which is then ingested. BoNTs are extremely potent and target the nervous system, resulting in paralysis that can be so severe as to require life support on a mechanical ventilator for weeks to months. Countermeasures to prevent and treat botulism, such as vaccines and therapeutics, are

extremely limited. Consequently, the ability to detect these toxins in the environment is critically important. “We not only aim to use the antibodies in BoNT detection tests, but also to understand how they bind and inhibit these fascinating molecules,” Hayhurst said. “We are also striving to improve our test by making it more sensitive such that one day it may be able to detect much smaller amount of toxins found in patients’ blood. Since BoNT also have therapeutic applications with carefully controlled preparations and dosing regimens, there is also an increasing need to monitor BoNT levels in these treatments.” In the new study, a llama was immunized with harmless versions of seven types of BoNT, blood taken to provide antibody producing cells. Using bioengineering techniques, the antibody genes were cloned and the resulting antibodies were tested for their ability to detect BoNT in a selection of drinks, including milk. Hayhurst and his team are continuing to study the molecular interactions of the llama antibodies to find out why they are so specific and why some of them inhibit toxins. The laboratory capabilities of SFBR enabled this research to be performed according to all applicable federal guidelines of biosafety and biosecurity under the CDC Select Agent Program. SFBR is one of the world's leading independent biomedical research institutions dedicated to advancing health worldwide through innovative biomedical research. Located on a 200-acre campus on the northwest side of San Antonio, Texas, SFBR partners with hundreds of researchers and institutions around the world, targeting advances in the fight against bioterror, cardiovascular disease, diabetes, obesity, cancer, psychiatric disorders, problems of pregnancy, AIDS, hepatitis, malaria, parasitic infections and a host of other infectious diseases.

US State Dept: Drug trade enabling WMD acquisitions

The explosion in the narcotics trade has provided drug cartels with the capability of acquiring radioactive material, chemical weapons and other WMD technologies, a top US State Department official warned Tuesday. "The sums of money involved are growing in extraordinary amounts, and that raises the possibility, because of the sums and the areas in which these groups have begun to operate, for that opportunity to be exploited," said David Johnson, assistant secretary of state for the Bureau of International Narcotics and Law Enforcement Affairs. "Some of these criminal syndicates have the organizational and financial wherewithal that could potentially allow them to acquire and sell radioactive material, biological and chemical weapons, and technologies used for weapons of mass destruction." Johnson, who was speaking at the Washington Institute of Near East Affairs, attributed the massive growth in drug profits to increasing demand and supply in the worldwide market. "The supply particularly of heroin is growing in ways that are hard to fathom," he said. When it comes to the Middle East, however, Johnson said that most of the major terror organizations get their funding from state sponsors rather than drugs and other criminal activities. "If you're looking at the areas around Israel, you're talking about state sponsors driving the organizations and this being more opportunistic rather than a direct impact on what they're doing," Johnson assessed, calculating that even the drugs grown in the Beqaa Valley in Lebanon are not a major source of income for Hezbollah. "It's more the case of criminal groups producing products and providing services that are quite useful to these groups that are engaged in even more nefarious activities," he said, pointing specifically to

smuggling and border crossing as a useful form of support criminal groups provide. He also spoke of the nexus of contraband and terror activity running through the tunnels Hamas has dug from Gaza into Egypt. In the West Bank, Johnson noted that the US has been helping train security forces there to deal with narcotics and other types of law enforcement and praised the efforts to date. "We're quite pleased with that program. The quality and capability of the individuals who came into it was significant," he said of the force assembled under American General Keith Dayton. He pointed to the crowd control the Palestinian police exerted during Israel's strikes on Gaza last winter as "extremely effective." He said that, "The Palestinians were able to exercise their constitutional right to protest, but they did so in a manner which you wouldn't have contemplated before."

"Eagle Eyes" program

Top leaders at West Coast Marine Corps installations have instituted a program to encourage all military and civilian personnel to keep a watchful eye for potential attacks - from biological to chemical to nuclear. The program, dubbed "Eagle Eyes," involves the safety and security programs of Marine Corps Installations West and the I Marine Expeditionary Force to enable all military and civilian personnel to aid base law enforcement and security authorities in preventing terrorist acts. “The motivation behind (Eagle Eyes) inception is the necessity to maintain a constant and increased vigilance because of terrorist threats to the United States,” Chief Warrant Officer 3 Jeffrey Frenchlujan, chemical, biological, radiological and nuclear defense officer, Mission Assurance, MCI-West, told Scout North County News. “With the recent terrorist incidents, we are reminded these threats still exist and this program is needed.” All bases and air stations in California and Arizona will take part in the Eagle Eyes program as well as several East Coast Marine Corps installations. The goal of the program is to allow individuals to take an active role in deterring, detecting and defeating terrorist crimes. The program asks personnel to keep a watchful eye for surveillance practices, suspicious questioning, tests of security, supply acquisition, suspicious persons, dry runs and asset deployments.

France creates new unit to deal with terror attacks

France yesterday created a specialised unit to deal with the threat of nuclear, biological or chemical (NBC) terror attacks. The unit "specialised in the fight against terrorist threats of a nuclear, radiological, biological or chemical nature", according to a prime ministerial decree, will come under the authority of the interior ministry. Co-ordinating the work of other similar units within the French police forces, it will intervene "whenever a device might release nuclear energy or contain NBC material or agents dangerous to people, goods or the environment". The new unit's chief will be named shortly, the decree said.

England reveals increased monitoring for dirty bombs, bioweapons

Major British ports have had high-tech machines installed to detect any materials that could potentially be used to build "dirty bombs," it has been revealed. Lord Alan West, speaking to The Sun, revealed the covert operation, telling them, "There is no doubt that terrorists still want to go for the big spectaculars - things like aircraft and dirty bombs. We have put in a whole range of measures to stop them but cannot be complacent. We have to be vigilant." The covert Project Cyclamen set up security portals that monitored substances coming into the United Kingdom. The project paid special attention to biological, chemical, radiological and nuclear materials that could effectively be used to make dirty bombs with an emphasis on stopping them from being brought into the country. "The portals enable us to see when a lorry

or a container comes through whether it is has any of this kind of material on board. When the portals detect radiological and nuclear materials we can take whatever action is necessary," West told The Sun. "They are already in a number of ports and other places and will be going into more. This has been highly complex because the technology is very difficult but I believe we have a world-beater." The search for any weapon, be it a biological attack or traditional radioactive attack, is of great importance as a single attack in London's Trafalgar Square, according to a 2003 BBC2 program, could leave London a barren wasteland.

Anthrax Cases among Heroin Users in Europe Illustrate Novel Risk

Bacillus anthracis, a ubiquitous but deadly pathogen found in soil, has been primarily an occupational disease. Notable exceptions include cases caused by the Amerithrax attacks and by exposure through animal drum skins. However, recent cases of anthrax, some fatal, in Scotland and Germany highlight a new risk—recreational heroin use. Only 1 prior case of anthrax infection in a heroin user has been reported: in 2000, a team in Norway described a fatal case in a user who had "skin-popped" the drug. No contamination source was ever elucidated.

Eight Deaths To Date

Since December 16, 2009, 8 heroin users have died from anthrax (7 in Scotland; 1 in Germany). In Scotland, 7 known nonfatal cases also have occurred. All patients were heroin users who presented with soft tissue infections, and all injected heroin subcutaneously or intramuscularly and/or smoked or snorted it. Severe cases have progressed to septic shock and meningitis. Treatment regimens have included antibiotics and anthrax immunoglobulin.

Speculation on the Source

The source of anthrax contamination is believed to be animal products that may have been present in cutting agents used to dilute the heroin. Early speculation has focused on bone meal, a known source of anthrax contamination, particularly in heroin from anthrax endemic regions such as Afghanistan—a major exporter of heroin to the UK. Contamination in the purification of heroin could also have occurred if it was done in proximity to animal products.

More Cases Expected

Because of the black market-like nature of drug distribution networks, it will be difficult to anticipate future cases caused by contaminated heroin. Details of the case of the deceased German patient, who had no travel to Scotland, may indicate the risk of infection outside of Scotland and the point of origin of contamination (source, dealer, etc.). Heroin users in the U.S. are at much lower risk of anthrax given that most heroin in this country originates in South America and Mexico, neither of which have a rate of anthrax endemicity as great as that of Afghanistan.

More Details Sought

Several pieces of information that may solve the epidemiological puzzles posed by these cases have not been but should be made available, including:

- results of any investigation into cutting agents present in the case patients' heroin supply;
- details on the local and international supply chain known for the case patients' heroin; and
- serotype of the anthrax strains isolated from the patients.

END OF PART 1