

CBRNE-Terrorism Newsletter – 2014©

**March 2014**

**Website:** [www.cbrne-terrorism-newsletter.com](http://www.cbrne-terrorism-newsletter.com)

**Editor-in-Chief**

**BG (ret) Ioannis Galatas MD, MA, MC**

**PhD cand**

Consultant in Allergy & Clinical Immunology

Medical/Hospital CBRNE Planner

Senior Asymmetric Threats Analyst

CBRN Scientific Coordinator @ RIEAS

Athens, **Greece**

**⮊ Contact e-mail:** igalatas@yahoo.com

**Assistant Editor**

**Panagiotis Stavrakakis MEng, PhD, MBA, MSc**

Hellenic Navy Capt (ret)

Athens, **Greece**

**Co-Editors/Text Supervisors**

* **Steve Photiou**, **MD,** **MSc (Italy)**
* **Dr. Sarafis Pavlos, Captain RN(ret’d), PhD, MSc (Greece)**
* **Kiourktsoglou George, BSc, Dipl, MSc, MBA, PhD (cand) (UK)**

Advertise with us! (New price list)

CBRNE-Terrorism Newsletter is published on-line monthly and distributed free of charge. Starting from 2014 issue all advertisements will be charged as following:

**⦁ Full page (A4) 100€**

**⦁ Double pages (A4X2) 200€**

**EDITOR**

**Mendor Editions S.A.**

3 Selinountos Street

14231 Nea Ionia

Athens, Greece

Tel: +30 210 2723094/-5

Fax: +30 210 2723698

**Contact e-mail:** Valia Kalantzi [info@mendor.gr](mailto:info@mendor.gr)

DISCLAIMER: The CBRNE-Terrorism Newsletter® is a free online publication for the fellow civilian/military First Responders worldwide. The Newsletter is a collection of papers related to the stated thematology, relevant sources are provided and all info provided herein is from open Internet sources. Opinions and comments from the Editorial group or the authors publishing in the Newsletter do not necessarily represent those of the Publisher.

CBRNE-Terrorism Newsletter is:

* **Read by First Responders in more than 80 countries around the globe (below right: top-20 countries);**
* **Distributed to more than 700 institutions, organizations, state agencies, think tanks, defense companies, institutions and universities.**

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | |
|  |  | |
|  |  | |

Editorial

**BG (ret’d) Ioannis Galatas, MD, MA, MC**

*Editor-in-Chief*

CBRNE-Terrorism Newsletter

**Dear Colleagues,**

For sure, March 2014 was characterized by two events – one on going (Syria’s chemical weapons destruction) and one new (mystery of Malaysian flight MH370).

Syria’s CWAs stockpile destruction is processing slowly and deadlines are not followed. Perhaps the excuse of the on going civil war is a logic one – perhaps not. We have to consider the fact that without CWAs the regime would become totally vurnable and those who currently control it do not like this option. I am not sure if we really know what is happening in this country and the reasoning behind this. But this conflict will end one day and the big problem will follow: what will the unemployed fighters will do the day after? Especially those from foreign countries – European, American or Canadian (just to name a few). How can we keep an open eye on them the moment we really do not know who they are? Or do we know exactly who they are?

Then it is the MH370 incident. Lots of unanswered questions and most probably they will stay that way for a long time. Latest information indicate that it might shot down because it was considered as a “renegate” threat to Garcia Air Force Base (US on British territory). It could take pages of philosophical debate on ethical and unethical issues related to all sides involved. But the most important question wil remain a mystery: *Cui bono*? For whose benefit?

The al Qaeda-affiliated group, Jemaah Islamiyah, has a presence in Malaysia as well as in the Philippines and Indonesia. But the group has been under sustained law enforcement pressure for more than a decade after it bombed nightclubs on the Indonesian island of Bali in 2002, killing more than 200 people, mostly Western tourists. The group has also carried out bombings at the Australian Embassy in Indonesia and the JW Marriott and Ritz-Carlton Hotels in the Indonesian capital, Jakarta.

However, the capabilities of the once-potent Jemaah Islamiyah have eroded over time. And would Jemaah Islamiyah, an Islamist militant group, target for attack the air carrier of a majority Muslim country on which quite a number of Muslims were likely traveling? It is more plausible that the group would select a Western airline because Western embassies and Western brand-name hotels have been the focus of their previous attacks and plots.

A terrorist group that might have a motive is the East Turkestan Islamic Movement, a separatist group in China founded by Uighurs that has had some historical ties to al Qaeda and the Taliban. The Uighurs is an ethnic group in western China who are Muslim. The group has conducted a number of terrorist attacks in China. Uighur terrorists might have a motive to hijack the Malaysia Airlines flight as it was bound for Beijing and most of the passengers were Chinese. But Uighur militants have operated almost exclusively inside China. And when they have tried to mount hijackings in the past they have been complete flops. On March 9, 2008, a 19-year old Uighur woman attempted to set off some kind of explosive device on a flight from the Xinjiang Uighur region en route to Beijing. The flight crew detained the woman before she could detonate the device. Four year later, on June 29, 2012, half a dozen Uighur men attempted to take control of an aircraft flying in the Xinjiang Uighur region using pieces of a metal crutch that had been sharpened to make crude weapons. This plot was also foiled.

Beyond Uighur militants or operatives of Jemaah Islamiyah, might there be other terrorist groups with the motivation and capability of pulling off the hijacking of the Malaysia Airlines flight? It doesn't seem so. If this were a hijacking for political purposes, the hijacking would have been followed by an act designed to send a political message, such as the planes hijacked on 9/11 that were then flown into the World Trade Center and Pentagon. Based on the above shooting down this commercial flying bomb sounds like the most reasonable answer. It remains to be proved if and when remains will be recovered.

One might add a third important March event: the crisis in Crimea and the annexation to Russia revealing that Western intelligence services failed to forsee this development along with their inability to play high level strategic chess – a game that seems to be genetically integrated to Russian DNA.

Parenthesis: It seems that historically March is the month of major conflict events!

March was also a month full of activities for the Newsletter. Editor participated as a speaker to a course (Response to Chemical Disasters – Doha Regional Center for CBRN Training [NCPW]) Doha, Qatar and a conference (4th Annual Fire Safety Technology Forum – photo below) and a training course (for Police Supervisors) in Abu Dhabi, UAE. Sharing knowledge is always a pleasure and a good opportunity to learn from others. It is of interest that these countries are now discovering the new emerging threats potential and are willing to take pre-emptive measures to defend their citizens and their miracles build on the desert sand. There are many things to be done in the long run. But the most important of all is the change of mentality on the critical inherent attitude “it will no happen to us!” On the other hand there are many consultants packed in these countries offering expertise and training of low quality caring only for high salaries and compensations to provide nice certification ceremonies and diplomas. Local governments are beginning to recognize this and have started to centralize educational programs that should be focused on specific knowledge and training instead of generic topics such as generic emergency and response management. But still there are many things to be done – especially in the field of medical CBRNE preparedness and training.

Situation in Greece is fragilly stable… Our new toy is the coming elections and which part or party will prevail over others. The word “progress” is still absent from politicians’ vocabulary and the depression status of populace progressed from subclinical to clinical.

**The Editor-in-Chief**

****

Secondary Barrier to Cockpit Door Needed, FLEOA Says; Door can be Breached, Video Shows

Source: http://www.hstoday.us/single-article/secondary-barrier-to-cockpit-door-needed-fleoa-says-door-can-be-breached-video-shows/54217eed070d311217633ed9cba4e767.html

In the wake of what it calls “the alarming air travel safety issues [that are] depicted in” a 23-second video (.mov file) showing that the cockpit door of a passenger plane can still be breached, “despite the current airline security procedures,” the Federal Law Enforcement Officers Association (FLEOA) said it is urging lawmakers to pass the Saracini Aviation Safety Act of 2013.

The bill has languished in committees of the House and Senate since introduction in the two congressional chambers last year.

In the video, called "**Two Seconds to Breach**,” FLEOA said “a cockpit breach occurs in quick succession," and noted that “The breach occurs during the moment the cockpit door is opened for crew to transit to or from the cockpit. A flight attendant and beverage cart placed as on obstacle poses no challenge for the would‐be hijackers” setting close to the front of the plane.

“This is not what was promised post‐9/11, nor what the American people deserve,” the organization said Tuesday.

Pending in the House Subcommittee on Aviation, and the Senate Committee on Commerce, Science and Transportation, the legislation would direct the Federal Aviation Administration (FAA) administrator to issue an order that would require:

* Installation of secondary barriers, other than the cockpit door, to prevent access to the flight deck of each commercial aircraft;
* Barriers on an aircraft with a cockpit door remain locked while the aircraft is in flight and the cockpit door separating the flight deck and the passenger area is open; and
* Barriers on an aircraft without a cockpit door remain locked as determined by the pilot in command.

"This video makes clear that gaps in our airline security still exist, and we need to address this vulnerability,” said FLEOA National President Jon Adler. “Putting our flight attendants in harm’s way to repel trained homicidal maniacs is an unacceptable strategic failure."

"We need to remember that on September 11th, 2001, terrorists hijacked aircraft and used them  a weapon of mass destruction to kill 2,873 Americans,” Adler said, adding, “In its aftermath, we vowed as a nation to ‘never forget,’ yet it seems with distance, we are forgetting."

FLEOA said the organization “would hope this video prompts Congress to move forward on this commonsense legislation that would fulfill the promises those same officials made to the American people after the 9/11.”

"With the lack of movement with this bill and decreased funding for our Federal Air Marshals (FAMS), the flying public is still at risk due to complacency,” Adler concluded. “The 9/11 Commission cited a ‘failure of imagination’ as part of the reason 9/11/01 happened and yet some of our elected officials and those in the airline industry seem to be suffering from amnesia and not imagining that a breach could still happen."

The bill has stalled out largely because of industry trade groups who oppose the bill on the grounds that it will be cost prohibitive to install a secondary cockpit door barrier. In addition, according to Capitol Hill sources, congressional supporters of the groups opposing the bill set on committees with FAA and aviation security oversight authority.

|  |
| --- |
| The video shows one man pushing the cart and the stewardness while a second man enters the cockpit and locks the door. **All that in less than 2 min!** The video was created by **Ellen Saracini**, widow of United Airlines Flight 175 Capt. Victor Saracini, whose plane crashed into the south tower of the World Trade Center; she is pushing for added security.  ►**Watch the video at:** http://www.nydailynews.com/news/national/widow-9-11-pilot-pushes-improved-in-flight-security-shocking-video-article-1.1703512 |

# UAE Islamic affairs authority reaffirms fatwa on Muslims travelling to Mars

Source: http://www.thenational.ae/uae/science/uae-islamic-affairs-authority-reaffirms-fatwa-on-muslims-travelling-to-mars

The Fatwa Committee of the General Authority for Islamic Affairs and Endowments on Monday reaffirmed its fatwa against humans travelling to the Red Planet.

According to state news agency, Wam, the authority said it received a question “about the rule of humans travelling to Mars and never to return”.

***“Based on the texts, it is not permissible to travel to Mars and never to return if life is not possible there and the expectation of death is more than the possibility of life, due to this action exposing one to self-destruction,”*** the committee answered.

The Mars One space foundation has asked UAE Islamic authorities to cancel a fatwa warning Muslims not to travel to the planet.

More than 200,000 people applied for the chance to be part of Earth’s first colony on another planet.

|  |
| --- |
| Dubai resident shortlisted from more than 200,000 people for Mars One mission Source:http://www.thenational.ae/uae/science/dubai-resident-shortlisted-from-more-than-200-000-people-for-mars -one-mission  The race is on to become the first person to go to Mars – and Khalid Al Jaaidi is well and truly on the starting line.  http://www.thenational.ae/storyimage/AB/20140105/ARTICLE/140109603/AR/0/AR-140109603.jpg&MaxW=460&MaxH=306The 21-year-old designer has been shortlisted along with 1,058 applicants for the Mars One mission. More than 200,000 people applied for the chance to be part of Earth’s first colony on another planet, and Khalid feels he was picked for his natural ability to adapt to different situations.  “I want to be part of this because it is the most interesting thing to happen to humankind since the moon landing,” said Khalid, who was born and brought up in Dubai. “It’s going to be very challenging and exciting.  “Many people don’t think it’s possible, but I think the programme has a very strong committee board and a good plan. I’ve put my trust in them.”  Khalid has a degree in visual communications, but he says the most important thing is having the right mindset.  “It is all about how resilient, creative, and determined you are. There are going to be good times and hard times, and you have to be ready to deal with the hard times.”  Since applying to the programme, Khalid has been trying to absorb as much information as he can about his potential future home.  “One of the most interesting things I learnt is that Canada was colder than Mars this winter.”  Khalid says the whole adventure has really changed the way he sees things.  “I have in the back of my mind the thought of how drastic the change will be. I’m not taking anything for granted any more. We will have to work hard to make it livable there; we have to grow our own food. No more biryanis.”  Khalid, the youngest of seven, didn’t tell his family about the project until after he learnt he had been shortlisted.  “They were happy at first until I told them it was a one-way trip. My father is supportive but he thinks it’s a programme for prisoners. My mum doesn’t believe it is possible and my siblings don’t take me very seriously. I don’t think it has sunk in yet.”  He said his friends had posted on social media calling the mission a “real camping trip”.  “One of my best friends doesn’t want me to go, every day he tells me don’t go to Mars and I’ll buy you all the Mars bars you want,” said Khalid.  He had planned his life differently before applying to the Mars One programme.  “My parents still ask me what about our grandchildren,” he said.  Should he make it to the final selection the first team are scheduled to blast off in 2023, but Khalid says getting married between now and then is out of the question.  “Who wants a husband with an expiration date?”  He admits the whole idea does scare him a little. “I am nervous; I’d be crazy if I wasn’t. But in a way you know when you’re about to go, so you can say your goodbyes.”  Khalid is now planning to get into physical shape. The next step is passing the medical test, and then a number of interviews with the committee, before the numbers are cut further. |

# Combating transnational organised crime fuelled by escalating instability across Africa

Source: http://www.defenceiq.com/naval-and-maritime-defence/articles/combating-transnational-orga-nised-crime-fuelled-by/

**Africa’s steady creep towards being the global hub for transnational organised crime and violent terrorism is becoming one of this decade’s key security concerns for international actors. The United Nations Office on Drugs and Crime (UNODC) estimates that 13 percent of global cocaine traffic moves through West Africa, meaning that in the past several years the region has become a crucial transit route for drug trafficking from the Americas.**

David M. Luna, Senior Director of the U.S. Department of State’s Bureau of International Narcotics and Law Enforcement Affairs spoke at the AFSEC 14 conference this morning (Feb 26), which is focusing on the importance of strengthening international cooperation on sea and on land to effectively disrupt and dismantle transnational organised crime, illicit flows, and terrorism across Africa.

“We must recognise that trans-regional illicit trafficking of drugs, arms, humans, and other illicit trade goods and services, are fuelling greater insecurity and instability across Africa, and in other parts of the world,” said Luna.

While West Africa is the focus of and location for the conference, the content of the presentations were all fixed within a global context. Luna made it clear that no one region is isolated from the security challenges of another that facilitates organised crime.

“Today’s reality is one in which we live in a world where there is no region, no country and no people who remain untouched by the destabilising effects and corruptive influence of transnational organised crime and violent terrorism.

“The United States, China, France, and other countries must work more closely with the international community to better coordinate efforts and resources, build Africa’s sustainable future and work together to combat the threats that undermine the capital and investments that are necessary to sustain economic prosperity throughout Africa.”

More specifically, the US Bureau of International Narcotics and Law Enforcement Affairs (INL) is undertaking a number of initiatives and programmes to undermine transnational criminal networks in West Africa and to reduce their ability to operate illicit criminal enterprises. **For example, a US government team has developed a plan called the West Africa Cooperative Security Initiative (WACSI), which is built around five objectives designed to respond to the underlying factors that allow transnational crime to flourish in West Africa. These are:**

1. Technical assistance and capacity building to help governments and civil societies develop the skills to combat impunity;
2. Technical assistance drafting anti-Trafficking and Organised Crime (anti-TOC) laws and policies, assisting in the process of getting these laws enacted, and creating awareness about the laws and policies on anti-TOC;
3. Investing in elite counternarcotics units, operational training and equipping of accountable institutions, and technical assistance to build basic law enforcement skills and institutional capacity;
4. Technical assistance to build the capacity of prosecutors and judges to prosecute and adjudicate complex TOC cases; and
5. Drug demand reduction and raising public awareness of TOC.

In 2011 and 2012, the U.S. government provided approximately $95 million for WACSI programmes. **The UN Office on Drugs and Crime (UNODC) estimates that terrorist financing, trafficking in arms, drugs, and people, and other transnational forms of organised crime generate approximately $3.34 billion per year.**  One of the critical challenges for the international community is to begin to close that gap, and working together to offer better options to those individuals who are so often pulled into the world of organised crime and extremist groups. The options of economic freedom, and sustainable futures.

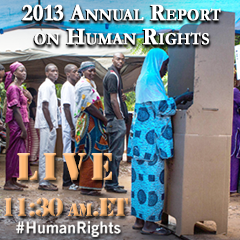
“To do this, we must support pragmatic partnerships and creative incentives that deter the recruitment of Africa’s marginalised youth and peoples, unemployed, and disenfranchised and invest in developing economic opportunities that help finance their education, health, and on agricultural technologies and other micro-business that augment market growth and investment strategies,” said Luna. “Reducing demand for increasingly available illicit drugs is a key part of this puzzle, if we are to give Africa’s youth a fighting chance at stopping the cycle of crime and corruption.

“We need to address underlying causes that are contributing to today’s conflicts in Africa: food and water security, poverty, economic integration and development, and other socio-economic areas that empower communities and nurture growth markets, investment frontiers, and resiliency.

“With careful, targeted assistance, and smart diplomatic engagement, together we can advance our common objectives and strategic interests.”

# State Department Report Details Suppression of Human Rights Abroad

Source: http://www.nytimes.com/2014/02/28/world/state-department-report-details-suppression-of-human-rights-abroad.html?\_r=0

The State Department reported Thursday that an increasing number of governments were suppressing political opponents and restricting the freedom of assembly.

In Russia, the State Department said in its annual human rights assessment, “the government continued its crackdown on dissent that began after Vladimir Putin’s return to the presidency.”

In Iran, there has been no measurable improvement in the bleak human rights situation there since Hassan Rouhani became president in August, the State Department said, and in Egypt, human rights abuses that were prevalent under President Mohamed Morsi have continued since he was deposed by Gen. Abdul-Fattah el-Sisi, now a field marshal.

The report is a sobering assessment of the prospects for the spread of democracy. “A growing number of countries are cracking down on civil society,” said Uzra Zeya, the senior State Department official who supervised the preparation of the report. “Evidence of this reality is apparent in every corner of the globe.”

Congress requires the State Department to prepare the report covering the United States’ partners as well as its enemies. The State Department’s briefing room was packed Thursday with foreign reporters and attachés from foreign embassies eager to learn what the assessment said about their countries.

In a briefing for reporters, Ms. Zeya said that 2013 was marked by “some of the most egregious atrocities in recent memory,” including the Aug. 21 chemical weapons attack in Syria that killed 1,429 people and what the State Department said were “rampant disappearances” in North Korea.

On a positive note, the report said that Myanmar had released more than 1,100 political prisoners and had allowed the International Committee of the Red Cross to visit all of its prison and labor camps. But the report noted that the government had done little to help members of an Islamic minority in Rakhine State who have been displaced by sectarian violence. Tens of thousands of them are still in camps, the State Department said.

The overall trend was not encouraging. Surveying the global situation, the report said that more than a third of the world’s people live in countries that are ruled by authoritarian governments, and that there was a widening gap between the rights that are guaranteed by international law and the “daily realities” around the world.

In Belarus, the report said, security forces beat protesters and imprisoned the government’s critics on politically motivated charges. In Cuba, the government organized mobs to assault peaceful demonstrators.

In China, “repression and coercion, particularly against organizations and individuals involved in rights advocacy and public interest issues, were routine.” In Sri Lanka, it said, attacks on activists have produced “an environment of fear and self-censorship.”

In South Sudan, government forces and rebel militias were both blamed for serious human rights abuses, including extrajudicial killings.

The report also included pointed assessments of some of the United States’ longstanding allies and negotiating partners. Secretary of State John Kerry stirred controversy in August when he said that the Egyptian military had been “restoring democracy” when it ousted Mr. Morsi.

But the State Department report cited “the removal of an elected civilian government” and “excessive use of force by security forces” as among the most significant human rights problems in Egypt.

And while the United States is involved in negotiations with Iran over its nuclear program, the report noted that there had been little progress on human rights under Mr. Rouhani.

“There have been some steps, as the release of some political prisoners last fall, but over all I would say the situation remains poor,” said Ms. Zeya, who added that among other abuses, the report detailed “allegations of torture, political imprisonment, executions in the absence of due process, which have gone up under this government, harassment of ethnic and religious minorities.”

Bahrain has been a touchy subject for the Obama administration: The United States Navy’s Fifth Fleet has its headquarters there. The country has a Sunni-led monarchy and a Shiite majority and has been rife with sectarian tensions.

“The most serious human rights problems included citizens’ inability to change their government peacefully; arrest and detention of protesters on vague charges, in some cases leading to their torture in detention; and lack of due process in trials of political and human rights activists,” the report stated.

Turkey, a NATO member and important American partner in the Syrian crisis and on other issues, was cited in the report for a number of abuses, including against the news media.

“Authorities imprisoned scores of journalists who remained incarcerated at year’s end, most charged under the antiterror law or for connections to an illegal organization,” the report said. “Of particular note, authorities used excessive force in response to the summer’s Gezi Park protests, leading to mass casualties (including seven deaths) and an overall diminution of freedom of expression and press.”

# And the response:

# Iran Reports on Human Rights Violations in the United States

Source: http://www.terrorismwatch.org/2014/02/iran-reports-on-human-rights-violations.html

Tired of being on the receiving end of human rights concerns by Washington, Iran has responded with its own scathing report on rights violations by the United States.

**A report by Iran’s Basij militia questions the United States’ role as the self-proclaimed defender of human rights, accusing Washington of a string of abuses.**

Death penalties, violation of prisoners’ rights, racial discriminations, breach of privacy rights, lack of free speech, and violation of the rights of indigenous populations are among the ways that Iran believes the United States breaches human rights.

The 30-page report accuses Washington of using human rights as a tool to wage war on other countries, while violating those same rights at home.

“Although the United States of America claims to be a protector of human rights around the world, and each year assesses the HR situation in each country, it remains to be asked where its own situation in terms of respecting and protecting Human Rights is,” says the report, published in English, Arabic and Farsi.

“As soon as we all hear the phrase ‘human rights,’ the painful memories of Abu Ghraib, Guantanamo, and Bagram prisons remind us of the human rights violations committed by the US government,” says the report, referring to US military scandals involving prisoners under its care.

The focus of the report, released in a ceremony at Tehran University, is on rights abuses in 2013.

Last week, the United Nations published a report on human rights violations in the Islamic Republic, which was immediately dismissed by the Iranian justice minister, Mostafa Pour-Mohammadi.

The Basij report refers to specific cases, including Edward Snowden’s, a former National Security Agency contractor who revealed top secret NSA documents to several media outlets.

“The American Civil Liberties Union documents show that... (US) security agencies widely intercepted American citizens’ phone calls in 2013. Many of these actions were carried out without a court order,” the report notes.

It also objects to a 35-year prison sentence given by a US military court to Bradley Manning, the young American soldier who was arrested in 2010 for revealing classified information to WikiLeaks, the online whistle blower.

Iran notes that rights watchdog Amnesty International has repeatedly asked for his release.

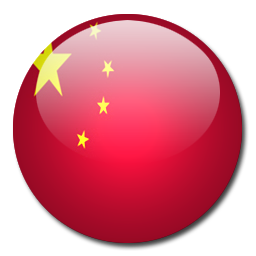
Privacy violations of Muslims by the New York Police Department (NYPD) and other law agencies is another topic of focus for Iran, which shows strong support for American Muslims whose anger it sees as justified.

“For over a decade, the NYPD's Intelligence Division has targeted Muslims for discriminatory surveillance based on nothing but their faith, spying on them in their places of worship, businesses, and even homes.” the Iranian report says.

“The NYPD's biased spying program constitutes a clear violation of the civil rights of innocent Muslims, who are viewed as suspect and stigmatized by the very authorities charged with protecting them,” it adds.

# China hits back at US in human rights report

Source: http://www.terrorismwatch.org/2014/02/china-hits-back-at-us-in-human-rights.html

China on Friday (Feb 28) issued a report on human rights in the US, denouncing it for foreign drone strikes, state-sponsored spying and "rampant" gun crime after Washington criticised its rights record.

Beijing said the US "concealed and avoided mentioning its own human rights problems", such as a government-run intelligence programme known as PRISM which it said "seriously infringes on human rights".   
The document came after the State Department issued its annual global human rights report Thursday.

China regularly produces a statement on the US in response. It does not release rights reports aimed at other countries.

The report, released by China's State Council, or cabinet, singled out the US for criticism for drone strikes in countries such as Pakistan, which it said have caused "heavy civilian casualties".

It also said the US suffers from "rampant gun violence", while its agricultural sector employs a "large amount of child labourers".

Washington's report released on Thursday praised China for some successes in human rights, such as the abolition of some labour camps and a change to the one-child policy.

But it added that "repression and coercion, particularly against organisations and individuals involved in civil and political rights advocacy... were routine".

It also noted Beijing's continued repression of ethnic Uighurs and Tibetans.

Human rights are a long-standing source of tensions between China and the US, which imposed sanctions on Beijing after the 1989 Tiananmen Square crackdown on pro-democracy protesters which left hundreds or thousands dead.

References in the Chinese document showed that much of it was sourced from US media reports.

China's ruling Communist Party tightly controls its own domestic media and has repeatedly imprisoned those who openly challenge its right to rule.

China often says that its rapid economic development in recent decades has lead to a greater respect for human rights, and that other countries are not entitled to criticise its record

.

# Designing in security for major sporting infrastructure

**By Roger Cumming**

Source: http://icss-journal.newsdeskmedia.com/Designing-in-security-for-major-sporting-infrastructure

**Roger Cumming** explores the challenges that designers of major sports venues and infrastructure face in unpredictable security threats and the importance of ensuring a positive spectator experience

In the summer of 480 BC, the Athenian Olympic Games celebration was disrupted by fears of a second invasion by the Persians, the first having been defeated at the Battle of Marathon, 10 years earlier. The Athenians consulted the Oracle of Delphi for guidance on how to defend themselves and were advised to place their trust in a “wall of wood”. Taking this to be a reference to ships, the Athenians prepared their fleet and subsequently used it to evacuate Athens and later defeat the Persians at sea.

The organisers of today’s major international sporting events do not need to rely on Delphic predictions for security advice; there are highly sophisticated systems available to assess and respond to immediate threats and well-developed levels of information sharing and international cooperation to support the host country.

**However, the infrastructure for the sporting event is likely to have been designed many years before the event takes place when it would have been impossible to know with any accuracy what kind of threats it would need to withstand.** This article looks at some of the challenges facing architects, designers and engineers to ensure that sporting events can take place safely and securely in a variety of threat environments.

**Strategic approach**

Infrastructure of any type, sporting or otherwise, takes a long time to plan and build, and will last even longer. At the sport security Experts’ Summit organised by the International Centre for Sport Security (ICSS) in April, participants observed that it takes an average of eight years from the decision to build a major piece of sporting infrastructure to its becoming operational. The prevailing threat that might bear upon that infrastructure when it is used will be impossible to predict accurately that far in the future. Furthermore, the threat can change much more quickly than any defensive posture arranged to protect it. An unexpected terrorist attack, for example, is likely to cause an abrupt re-assessment of the threat. New cyber threats and avenues of attack can appear very rapidly, a situation that is unlikely to diminish in the short term and may get significantly worse. If protective measures need to be added retrospectively, it is invariably at great expense in terms of time, money and disruption.  
How do those designing infrastructure and sports venues build in protection against threats that they cannot accurately predict? The answer is that by following a few strategic guidelines, it becomes possible to produce designs that not only satisfy the sporting requirements, but are safe and secure, aesthetically pleasing, and – importantly – capable of withstanding changes to the risk environment in a flexible and cost-effective way throughout any legacy use.

**The wider context**

The first guideline is for the design process to take account of the wider context – for example, a national security strategy or plan that is set by a higher authority (normally the national government). The security planning for most international sporting events will take place within the context of the host country’s strategic planning framework. This is likely to consider a range of risks to people, events, and physical and logical infrastructure. Underpinning this should be a comprehensive set of relationships between the event organisers and the government agencies, especially law enforcement, responsible for assessing security threats and disseminating advice about how to mitigate them. The organisers of a major sporting event must work with these agencies to address any issues relating to threats that might bear upon the event; they cannot reduce the threat by themselves. It is therefore important for them to understand the broader risk environment and how the national (and local) response machinery is organised. The way to achieve this is to establish long-term working relationships with the relevant organisations, which then can be utilised to respond to a particular event, from a one-off match to a major sporting event like the FIFA World Cup or the Olympics.

**Impact-driven design**

The second guideline is to focus the design on minimising the impact of a hostile event (for example a terrorist bomb or cyber attack). Designers and architects are very familiar with the need to ensure that sports stadia and other infrastructures are built to ensure the highest levels of safety at times of an emergency such as a fire. There is no reason why security should not figure as prominently in their considerations. There is a considerable body of knowledge about how to protect against the effects of a blast from a terrorist bomb (whether carried in a vehicle or on a person) or against shots from a weapon. There is a similar wealth of knowledge about how to defend against cyber attacks. It is essential, therefore, that designers and architects engage early with security practitioners to understand the impact that a catastrophic event might have on the sporting venue and its occupants. However, all too often, designers focus on the likelihood of an attack, rather than on what impact it would have. A mindset that considers impact ahead of likelihood will produce a design that is capable of withstanding a variety of threat scenarios, including new ones and those that may change in nature over the lifetime of the infrastructure.

To achieve this, the designer should have a clear understanding of what is critical to the functioning of the infrastructure and venue. Some of this may emerge naturally from consideration of the safety aspects (for example having multiple entrances and exits that can be used in the case of a fire), but others may not be so evident. **Sometimes, good design and good security design may not be the same thing.** For example, placing the back-up to a critical system alongside its master may be elegant in design terms and cheap to implement, but a bomb designed to damage one may take out the back-up as well. The designer needs also to place critical systems as far away as possible from the public domain to minimise the chances that intruders can quickly penetrate a protective perimeter and cause damage.  
Good physical security need not detract from the aesthetic impact of the venue. Planned in advance, it can be built into the fabric of the venue and its surroundings in such a way as to be pleasing to the eye, discreet and highly effective. The challenge for the designer is to use the natural lie of the land, and existing geographical features, to avoid the need to construct defences that might present a more stark appearance. A stream or ditch might easily be adapted to control the flow of vehicles or block potentially hostile ones. Earth banks planted with attractive foliage can protect buildings from the effects of a blast. Where defensive structures need to be built, they should be merged into the surrounding ‘streetscape’ as much as possible. Raised flower planters, bicycle racks and street lighting fixtures might all be adapted to act as hostile vehicle mitigation of some form. A major north London football club has some of its hostile vehicle mitigation measures constructed in the form of giant letters of the club’s name. Other barriers might be hidden behind stone balustrades or constructed from materials that blend in with the surrounding architecture and heritage of the site. **All that is required is for the designer to engage early with the security professionals so that the artistry of the former blends with the requirements of the latter in as attractive a way as possible.**

**Taking an holistic approach**

Acquiring a comprehensive understanding of what is critical to the functioning of a venue leads to the third of the strategic guidelines – taking an holistic approach. The complex nature of modern communications and control systems leads to myriad interdependencies between the physical and logical elements in a modern stadium. Entry gates, CCTV monitors, public-address system and display screens will all be controlled across communications networks, which themselves are based on internet protocols (IP). Such networks will be flexible and able to adapt to changing requirements, but unless they are properly protected, they also will be vulnerable to cyber attack. This could result in sound physical protection measures being compromised in some way. Any holistic approach must also include the people who operate the physical and cyber measures at a venue.

However, an holistic approach means much more than just considering physical, cyber and personnel risks together in some way. Security functions that are organised in silos are inefficient and obstruct the identification and mitigation of risk. It is important that the governance of the various security functions is structured in such a way as to support an holistic approach. Having different reporting or line management chains for these functions will stretch channels of communication and introduce potential gaps from which greater risk is likely to emerge. In our follow-up article in the next edition of this journal, it will also become clear why it is important to embed this holistic approach throughout the supply chain for both the build and operation of an event.

Effective security starts at the top of the organisation and should be embedded throughout it by a culture in which the everyday attitudes of staff contribute effortlessly towards an organisation’s protective security regime. It is vital that event organisers work to achieve such a positive culture and one that takes an holistic, not siloed, approach to security – designed to minimise physical, information and personnel risks and protect spectators and staff.

The cyber threat to a venue will manifest itself in many ways, not just in relation to the operation of physical elements. Information in many forms will be vital to the successful design, construction and operation of any sporting venue, not only for its immediate use, but also possibly for many years of legacy beyond that. Authorities need to take action in a number of areas, including:

* Protection of documents relating to the design and construction of the venues. Inappropriate disclosure could allow the identification of weak points or vulnerabilities in the construction that could be exploited.
* Protection of documents relating to the operation of the venues, especially during sporting events when the risks are greatest. Inappropriate disclosure could allow security regimes to be subverted or compromised.
* Protection of information in all media. While the majority of information will be carried via electronic systems and networks, the use of paper will still be necessary in certain cases. It is important that the information protection plan encompasses both mediums and enables venues to be confident that portable media (paper, memory sticks, CDs and so on) is protected as effectively as that carried on the many (cyber) networks that will be necessary to support events.
* Identification of new threats as they emerge. The rapid development of cyber threats is unlikely to diminish in the short term and may get significantly worse. It will be particularly important for sporting venues to have confidence that appropriate protection is in place to counter the most sophisticated of these.

The last point underlines why it is so important to adopt an impact-driven approach to the security of cyber infrastructures in particular. Focusing on a threat that can change so rapidly and far more quickly than defences can be reconfigured will not lead to a secure cyber infrastructure that will remain resilient in the face of uncertainty. However, by understanding what is critical to its operations, a venue can start to build a cyber system that can deter, detect and defend against the inevitable attempts to compromise its operations.

An effective and holistic security risk-management regime will therefore have a number of components, including: senior management support; capable people; efficient processes; and the selection of appropriate physical and technical controls. Each component should interact with and support others in a holistic manner. It is important to seek a balance between these components as the model is compromised if any one component is deficient or fails. Organisers should understand that technology is just one piece of a complex jigsaw that will eventually deliver a safe and secure celebration of sport. A multidisciplinary team is needed to ensure that physical assets and information are safeguarded appropriately and a positive security culture is fostered among staff.

At this stage, it will also be necessary to consider any legal and compliance issues set by a higher authority, for example regional or national government. There are numerous relevant national and international industry standards that might be adopted. However, it will be important for the leadership of the venue to ensure that the focus remains on effective and proportionate risk management and not just slavish obedience to a particular standard. The danger of adopting standards is that the focus of management effort switches to achieving compliance with the standard rather than holistic management of the risk.

**Getting there**

The three guiding principles – considering a wider context, being impact driven and taking an holistic approach – may be easy to say, but are much more difficult to achieve. It is vital to get things right from the very start and have security considered at the beginning of the design stage, not as a post-build ‘add-on’. **Early engagement between security professionals, designers and architects is essential.** This can save money in the long term and produce a design that enhances the spectator experience by inducing a greater feeling of safety and security.

Achieving this requires good communication skills and the ability to keep the communication going throughout the design and build of a project and its subsequent operation. But that is easier to say than do as personal relationships, group dynamics and overarching governance structures can all interfere in the process and allow differing elements to drift off in their own directions. So often, security is considered well after the start of the design process when changing plans becomes expensive and time consuming. While getting it right at the start is vital, so is the ability to keep that level of engagement going. This requires continuing commitment and leadership from the management and an engaged as well as supportive workforce, ready to embed the security objectives into their everyday actions.

As we will consider in part two of this article, it becomes even more important to achieve this once the design phase is over and construction begins. As the real venues start to emerge and the number of people involved in the project rises, different challenges emerge. However, by following a simple set of guidelines, it is possible to achieve a safe, secure and highly enjoyable celebration of sport – and provide a lasting legacy for generations to come, whatever the prevailing threats of the time.

**Getting the security requirement right**

Architects and designers of sporting infrastructure should seek to build security features into the very fabric of the structures themselves. The best security is usually the most discreet, but there will also be occasions when more overt measures will provide a deterrent to those with malicious intent, as well as reassurance and comfort to competitors and spectators. Further, there will also be times when security features separate from a main building will be necessary. The most obvious example of this is a perimeter fence.

All stadium systems should be designed and installed in a way that maximises through-life flexibility to support both changing operational needs and emerging technology. To achieve this, it is important that all relevant stakeholders agree on a structured mechanism to capture requirements for the functioning of system components.

The temptation at this stage is to think in terms of solutions rather than requirements, but this is a false economy. Take the simple example of a perimeter fence. The designer may ask for a fence of a certain height; but on what is that decision based? Is it just because a similar stadium had a fence of a certain height surrounding it, or was that fence the most prominent in a catalogue? It is important that rigour is applied to the specification of security components based on what they are seeking to achieve in the environment in which they will operate.

The generally agreed best approach to this issue is through the drafting of an Operational Requirement (OR) for a security component. This is a statement of need based upon a thorough and systematic assessment of the problem to be solved and the hoped for solutions. A structured process for the development and agreement of ORs has been successfully used to deliver the security systems for numerous parts of the UK’s infrastructures and many permanent and temporary sporting venues.

Among the questions to be answered during the preparation of an OR are: what is the output desired of the system/component? For example, in general terms **‘a fence’** is a solution rather than a requirement. Is the objective to demarcate aparticular area from another; to give one area more protection than another; or to channel people in a certain direction? All of these aims could be solved in a number of differing ways. It is also worth remembering that it is a mistaken belief that fences will keep people out of a certain area. While this is true for most law-abiding people, the same does not apply for those determined to enter a restricted area. In this case, the fence will only delay their entry (as it is climbed, burrowed under or cut through), although sensors will be able to detect this activity and alarms will be raised. If the fence was required for surveillance, was this for constant coverage of a particular area, or only at certain times?

The next question is: what are the options by which the output could be achieved? For example, fences come in all shapes and sizes. Some are hard to climb; others difficult to cut. Sensors to detect this activity can be discreet (sounding silent alarms) or noisy (triggering klaxons and spotlights). Also, surveillance can be achieved through the deployment of people, technology or a mixture of the two.

Another key consideration is the environmental and technical requirements for system components. Harsh environmental conditions will affect the materials that a security component is made from, especially if it is part of a permanent structure. CCTV cameras are particularly sensitive to the weather – those designed to function well in wet or damp conditions may not perform so well in hot and sandy conditions, and the reverse is also true.

The residual risks and weaknesses in the proposed solutions should then be considered. A fence might have sensors to detect when someone has cut it or is scaling it, but what happens then? How are resources mobilised to respond to the intrusion and how quickly will they arrive? In the case of surveillance, the effectiveness of this could be reduced during heavy rain, fog, snow and sand storms.

The next question is: what are the interdependencies between various system elements? This is a simple question, but the answers might be complex and take a long time to work out. This article is not long enough to tackle this in anything other than superficial detail, but as an example, the level of security a fence provides needs to be matched to the response time of the manned guarding. The shorter the delay the fence can provide, the faster the manned guarding needs to respond. This may require more guards at shorter distances from the perimeter.

It is important that rigour is applied to the specification of ORs and the focus is not allowed to drift back to thinking in terms of solutions. It is unlikely that the fundamental requirement for a security feature will change much (if at all) over the lifetime of the infrastructure, whereas the technologies that might be employed to achieve a particular outcome could change considerably. It is important that the replacement technologies do not weaken the overall security stance or remove features that were present in the original build. The best way to achieve this is by focusing on the requirement rather than the solution.

**Designing for the future**

Once the ORs and interdependencies of security-system components are understood and agreed, the system can be designed and installed. However, remembering that any form of permanent sporting infrastructure will last a considerable number of years, it is necessary to adopt a strategy that seeks to maximise the capabilities of new technologies as they emerge and minimise the disruption and change required to embrace them. Such a strategy is likely to include the following principles:

* Modularity – systems will be specified and delivered in a way that makes it easy to upgrade one element without changing numerous other components.
* Internet Protocol (IP) based – the historical separation between the physical and logical worlds is no longer applicable as so many of the physical entities in a stadium (including entry gates, CCTV monitors, public address system and display screens) will all be controlled across communications networks based on IP.Modern stadia can all be flood-wired with IP networks to achieve this. Such networks will be flexible and able to adapt to changing requirements of the terminating equipment. However, care needs to be applied in the way in which such networks are configured and protected to prevent them becoming a weakness that can be exploited via cyberattack, rather than a strength that delivers flexibility and adaptability.
* Based on open protocols – wherever possible, system components will be specified to use open, rather than manufacturer-proprietary, protocols for interfaces and data transfer. This will be particularly important for the control of numerous physical entities, as discussed above. It is inevitable that the degree to which a cyber environment is used to control physical entities will only increase over time. Similarly, the number of manufacturers offering products in this area will also increase.
* Flexible at the security-management system level – this is the point at which the inputs from the various systems are combined and then presented to the system operators.

Ongoing operator training is an important element of the process that is often forgotten or minimised after system commissioning has been completed. Ongoing refresher training programmes need to be planned and executed in order to ensure that operators remain conversant with the latest aspects of the system. These programmes will also be the best route through which to introduce new capabilities.

Designers of security systems need to devote time to keeping themselves up to date with developments in the technology market through a mixture of:

* attendance at trade shows, exhibitions and conferences;
* ongoing dialogue with suppliers and manufacturers in order to understand new uses, improvements to existing as well as new products, and capabilities that are in development; and
* regular engagement with relevant government or national bodies responsible for research and applied science and technology – each national government will have slightly different structures and processes to cover this. In the United Kingdom, the Home Office’s Centre for Applied Science and Technology is responsible for testing and assessing security equipment. The Centre for the Protection of National Infrastructure (CPNI), part of MI5, provides advice to the companies that run the UK’s infrastructure on how to protect themselves from national security threats
* This engagement will allow the designers of sports infrastructure to understand the strengths and weaknesses of products as assessed by independent experts, as well as aiding the implementation of current best practice. This will enable a judgement to be made as to whether an emerging capability offers a significant improvement (both technically and financially) over those currently proposed. This kind of activity could be swept up in the design-integration meetings that often take place in major projects when each engineering discipline determines how it is affected by security requirements and vice versa.

**A structured approach**

It is during the design and construction phases that the layers of security for venues will be specified and installed. Once this phase starts and the number of people involved in the project begins to rise significantly, it is important that a structured approach to the handling of information is introduced. The importance of this was highlighted in part one of this article. Information in many forms will be vital to the successful design, construction and operation of all major sporting venues for the many years of their legacy use. The protection of information will normally be achieved by the definition and implementation of an Information Security Policy (ISP) that needs to be written in collaboration with all relevant stakeholders. This should be designed to ensure that sufficient information relating to security systems is incorporated into master designs, but that sensitive information (for example, camera fields of view) is only released on a need-to-know basis.

To facilitate this process, a single authority should be established with the responsibility for writing the ISP and also deciding the relative sensitivity of information to be disseminated. This authority should specify how sensitive information will be marked, stored, transmitted and handled by users. Different countries will have their own established processes for this, such as some form of national protective marking scheme for sensitive documents (for example, restricted or confidential).

The ISP needs to cover appropriate elements of the supply chain. **The challenge here is to ensure that information is appropriately cascaded down the chain to facilitate the purchase of the right goods and services, but without exposing the overall security posture of the venue.** This will be particularly tricky when dealing with overseas suppliers or organisations with an unknown or weak cyber-security posture. This is a new area that may require the venue designers and builders to seek specialist advice to ensure that they can balance the advantage of going to the market for goods and services against the exposure of potentially sensitive information through the same route.

It is important that the ISP covers the protection of the numerous industrial-control systems that are necessary for the operation of physical systems at the venues, or that a separate policy is written to address these risks. A modern venue will have innumerable systems – including those for crowd access, lighting, air-conditioning, display screens and many aspects of security (command and control rooms, CCTV networks) – which will be controlled via data networks and electronic infrastructures. Complete or partial loss of control of any of these systems would result in serious consequences for the safe and secure operation of the venue.

The challenges of securing these systems from cyberthreats are brought into sharp focus when considering the projected life of the control units that turn cyber commands into real action on the ground. On average, an item of corporate IT equipment (such as a desk computer) will have a refresh or replacement rate of about four to five years. A typical industrial control unit may have a refresh rate of 20 to 25 years. The cost of replacing the remote control units and the disruption to essential services while this happens are among the reasons for this sharp difference in refresh rates. Over that period of time, it is impossible to predict what cyberthreats may emerge.

This is why it is important to adopt an impact-driven approach to security as described in part one. Focusing on a threat that cannot be judged so far in advance may ultimately lead to an inaccurate assessment of the risks, resulting in either inadequate or over-specified security features.

It is certain that those who wish to compromise information assets belonging to a sporting venue will be imaginative in their approach. In response, it is necessary to understand the threat to assets and build solid defences against incidents that could ultimately impact the security of venues and/or supporting infrastructures. In particular, the ISP needs to have a flexible response that adapts to changing technologies and attack methodologies. The pace of change in information systems is such that it will be necessary to keep the designs flexible and able to integrate appropriate new technologies as they emerge. But new threats also emerge at a significant rate. The ISP should ensure that venue owners can be confident they are able to manage their risks effectively throughout the lifetime of the venues. This reinforces the need to adopt an impact-focused, risk-based approach that will build the appropriate information security controls (for cyber and other mediums) into the fabric of the venue. This will ensure that it is capable of deterring, detecting and defending against the inevitable attempts to compromise its operations. It is impossible to prevent all compromises from internal and external threats, but an effective ISP will: support a security architecture necessary to create a resilient operation; respond to incidents effectively; learn from security breaches; and, most importantly, manage risk within proportionate tolerance levels.

**Information security standards**

There are numerous internationally recognised information security standards and frameworks that could be adopted. These include the standards set by the Geneva-based International Organization for Standardization – ISO 27001and ISO 27002 – and the 800 series from the United States’ National Institute of Standards and Technology (NIST), in particular NIST 800-53 and 800-82 for industrial control systems. There may also be applicable standards from the US-based International Society of Automation (ISA) and others, such as ISA 62443, which covers the protection of plant networks. Most national governments also provide protective security advice through specialist organisations.

**The engagement of security specialists as part of the multi-disciplinary design team will ensure that all the physical infrastructures are inherently secure and resilient, and make it relatively easy to search for suspect devices prior to the public being admitted.** Once construction of the infrastructure is under way, it is important that there is a controlled process to review proposed design changes from a security perspective. This process needs to encompass both substantive changes to the building’s construction (for example, the redesign of a layout), and changes to elements such as the cladding to be applied to a wall. Such cladding could easily be seen as ‘cosmetic’, but might have been selected for the way it resists explosive blast. However, this is unlikely to be known to the supply chain, who might propose a similar-looking material that is less resistant to blast.

During the construction phase it is important that: the site is physically segregated from the wider world; the workforce has been vetted prior to being allowed on site; goods and materials are screened prior to site admission; and frequent verification visits are undertaken. There are a number of models that could be adopted to achieve this, one of which is described below.

An appropriate perimeter barrier, with supporting technology, will be specified to separate the construction site from the surrounding areas. A typical set-up for a major sporting venue or site would consist of a perimeter fence, supported by CCTV, lighting, perimeter intrusion and an operational guard force around the whole of the construction site. Individual areas within that, for example the main stadium, would have their own construction site boundaries. A central construction command-and-control location should be specified to be responsible for monitoring installed systems (for example, CCTV and intrusion detection) and managing the guard force. If deemed necessary by a threat assessment, measures to guard against vehicle attack will be installed to protect the construction site. However, such measures need to be considered carefully to ensure that the barriers are suitable for that environment and their installation will not impede the required flow of construction vehicles.

Deliveries of construction plant and materials should be controlled through the use of a delivery management system to record details of loads, delivery vehicles and their drivers. To minimise risk to the construction site, one or more off-site centres should be used to process and check vehicles, drivers and their loads before they are sealed for final delivery to the site.

Checks on vehicles should then be undertaken at the boundary to the construction site. For vehicles entering the site, the checks should confirm that the vehicle and occupant details are as expected and that the load has not been tampered with since the off-site checks. For vehicles leaving the site, the checks should confirm that no unauthorised goods are being removed.

Throughout construction, verification and assurance visits should be undertaken to confirm that potential issues are identified early and addressed quickly. This will include a process for certifying that voids are in fact empty before they are sealed.

It should now be obvious that the number of people working on the project, either in offices or on site, has risen dramatically from the levels involved at the pure design stage. This means more people have access to information (some of which may be sensitive) and more people have access to sites and systems that may be vulnerable to malicious activity. It is therefore necessary to consider carefully the personnel aspects of the overarching security strategy. This is very often overlooked, with attention being focused on the physical and cyber elements, while the people who operate both are forgotten. It is wrong at this stage to suggest that all staff need to go through comprehensive vetting in order to establish their good faith and levels of integrity. That is unnecessary and too time-consuming and expensive. However, care should be devoted to ensuring that, as a very minimum, the true identities of all staff and contractors are fully established, and that they all have the appropriate right to work from the host country. Some staff and contractors will require extra clearance if they are to have access to more sensitive data.

This is an area where the importance of taking a holistic approach and not operating in silos cannot be overstated. The venue’s security professionals should take an active interest in this area and not simply leave the matter to the human resources or personnel department. High-quality leadership from the organisation’s top management layers will be necessary in order to articulate a vision of how the everyday actions of all staff involved in infrastructure and delivery contribute to the overall security of the event. If the leaders are clear about the type of event they want to achieve, then it is much easier for the staff to understand what they need to do. So often, weak or absent leadership will be filled by staff doing what they feel is right. Quite often, they will get the tone wrong and this could adversely impact the overall security stance, or inhibit the spectator experience.

**Let the games begin**

Security does not end when the building phase is over. Towards the end of this, and prior to the venues being used, there needs to be a final process of assurance to test whether the various security infrastructures and systems are fit for purpose. This is when their operation is tested against the original OR. The quality of finish should also be examined. If the processes described here were followed, there should be minimal need for remedial action or reconstruction, but this is not always the case.

If security has been integrated into the very fabric of the building then it will also support the handling ofincidents or emergencies. An integrated design will enable the event organisers, police, emergency services and others to respond to security incidents, disruptions and threats. The way that security is designed into the structure should aid this and produce an integrated response to a wide range of circumstances, for example, through the careful location and functioning of control rooms. This is the point at which people, processes and technology should all come together in perfect harmony.

Very often, security is considered as an afterthought – something to be applied once the design is complete. Not only can this be expensive, but frequently it will fail produce the desired levels of protection. By considering security aspects at the beginning of the design process, taking a holistic approach, thinking in terms of impact and involving relevant experts throughout both the design and building phases, it is possible to take discreet yet effective security measures at reasonable cost. This can deliver high levels of assurance to event organisers, and others, that the competitors, spectators and the venue itself will be protected against malicious activity.

Adopting the approach outlined in this article takes dynamic leadership from general management, supported by appropriate security professionals. By working together from the very beginning of a project, they can ensure that security enhances a sporting event, rather than being seen as a tax upon it.

***Roger Cumming is the Technical Director of Atkins’ security business. Atkins, an international design, engineering and project management consultancy, was heavily involved in the design of the infrastructure for the Olympic Park and temporary venues for London 2012.***

|  |
| --- |
| EDITOR’S COMMENT: This is a very informative article written by a person with inside knowledge of mega events infrastructure. I think that the most important conclusion is that designers must have a close collaboration with security experts when designing or hardening sports facilities – especially those meant to be used for mega events. Although the author focus extensively in practical security (i.e. fencing) and cyber threats he omitted a line or two on new emerging threats such as C(B)R that are on the top three of the threats’ list in all major events involving mass international gathering of spectators. You might argue that such an attack never happened in the past. But it seems you forget that the unexpected always happens and millions are spent for this reason (after 9/11 or the 2004 Olympic Games in Athens – the first summer Olympiad after the US bloodshed). Since one my small dreams in life is to be involved in the designing process of critical or mega events infrastructure I tried to contact mega designers in the area of new hospitals – especially in the Middle East (UAE and Qatar). I got zero replies – not even the polite “*thank you for your email*”; one exeption was from a Danish company replying that “these issues are taken care of by local authorities”. When I comment on this, I got no further reply. This attitude reflects lack of knowledge and absence of security experts so strongly indicated in this article. On the other hand in a recent training course I participated as an instructor (held in Doha, Qatar), one of the table-top exercises was based on a scenario involving spraying a 50,000 stadium with lewisite-mustard contaminating 70% of those watching the soccer game… And this reveals a second layer of responsibility – that of the organizers that should provide valid and accurate threat analysis to the designers and demand solutions covering all aspects of old and new threats that might emerge during the specific event. In that respect change of mentality should be added to the above chapter “Designing for the future”. |

|  |
| --- |
| **SPACE QUESTION**  http://www.newinspirationnetwork.com/wp-content/uploads/2012/10/astronaut.png  Will Russian-USA “cold” confrontation affect the return of American austonaut Mike Hopkins (and his two Russian colleagues) from International Space Station with space vehicle Soyuz? |

## Muslims in Ukraine: A Small Problem Amid a Larger One

**By J. Millard Burr**

Source: http://acdemocracy.org/muslims-in-ukraine-a-small-problem-amid-a-larger-one/#sthash.f7ahfL 1R.dpbs

“Crimean Tatars and Pro-Russian activists clashed outside a local parliament building in Ukraine’s Crimean peninsula.” (Washington Post, 26 February 2014)

In a long and detailed article on recent events in the Ukraine the Washington Post provided a tantalizing snippet, noted above, and then provided no further comment on an incident pitting Ukraine’s Muslim and ethnic Russian communities.

With the exit of President Viktor Yanukovych, observers are left to speculate what will become of the Ukraine.  In that nation there exists a plethora of political parties, and thus the election for President and to the 450-member unicameral legislature (the Verkhovna Rada) has in the past been subject to much horse-trading.  Still, if simplification is demanded, it can be said that as of this moment the Ukraine is divided between the Russophiles found east of the Dneiper River and in the Crimea, and the Russophobes to the west.

A second question should be, what will happen in the Ukraine’s Crimean Peninsula?  If the Russophobes in Kiev retain the power they have won, will the emerging Russophobia lead Russia’s President Vladimir Putin to seize the Crimea where ethnic Russians comprise about sixty percent of that region’s population?  Most importantly, as Sevastapol serves as a singularly important Russian naval base and is home to Russia’s Black Sea fleet, the possibility that Russia will move against Kiev to protect its interest is all too real.

Previously a part of Russia, in 1954 Soviet leader Nikita Khrushchev, “gifted” Crimea to Ukraine as a gesture of goodwill to mark the 300th anniversary of Ukraine’s merger with tsarist Russia. At the time, it did not occur to anyone to think the unthinkable: that one day the Soviet Union might collapse and the Ukraine might become an independent country.

Today, the Ukraine is a Republic composed of twenty-four provinces (oblasts) and the self-governing republic of Crimea. The Crimea itself is found on the northern coast of the Black Sea where Russia’s massive Black Sea Fleet is stationed at Sevastopol.  Russia is the beneficiary of a lease agreement with Ukraine that allows its fleet “to remain at Sevastopol until 2042.”  As a result, the Russian base in Sevastopol is home to an estimated 26,000 military, while the some 60 percent of the region’s population is ethnic Russian.  Recent news reports from Moscow indicate that Russia is prepared to fight, (i.e., occupy) the Crimea if the Ukrainian nationalists threaten ethnic Russian dominance.  ”This viewpoint seems to reflect Kremlin thinking,” and it is recalled that at a 2008 meeting with U.S. President George W. Bush, Putin reportedly told Bush that “Ukraine was an accident of history.” (Josh Cohen, “Will Putin Seize Crimea,” The Moscow Times, 24 February 2014) And Europeans are reminded that in a similar circumstance Russia invaded Geogria in 2008 when Moscow’s hold on the Caucasus was threatened in South Ossetia and Abkhazia.

Other questions remain: If the Crimea seceeds, will Ukraine’s Russophile oblasts located east of the Dneiper River (which divides the country in half) follow suit?  Finally, what will happen to the Ukraine’s Muslim minority, which fears a return of the Russians and of Russian Orthodoxy championed by Putin himself.

**Tension in the Crimea**

Well prior to recent events in the Ukraine, in 2008 an expert on Islam in the Ukraine–and the Crimea in particular–was asked to comment on the trouble brewing between the dominant Russian population in the Crimea and that region’s Muslim minority, the Crimean Tatars. Recent clashes had resulted from questions of land ownership and the economic marginalization of the Tatars.  The expert claimed:

“Tensions in Crimea only take on a front of religion. Conflicts in Crimea are periodically used by Russian nationalists for political means, in portraying a weak Ukrainian government incapable of managing the Crimean situation. I think that Russian nationalists would not necessarily mind a deteriorating situation in Crimea if it in fact de-legitimizes Kiev. The situation in Crimea is an opportunity for Russian nationalists to instigate conflict. Even though Russian nationalists represent the fringe among ethnic Russians in Crimea, the question remains whether they are indeed on the margins. (“Islamic Organizations and Challenges in Crimea: An Interview with Dr. Alexander Bogomolov,” Laryssa Chomiak and Waleed Ziad, International Committee for Crimea, updated 18 April 2008.)

When Dr. Bogomolov was asked to comment on recent trends in Muslim political activity he stressed that substantial participation was occurring thanks to umbrella organizations “found primarily in Kiev, the autonomous republic of Crimea, and the Donbass region.”  Still, just how extensive was the growth of the worrisome Islamist movement seemed to be anyone’s guess.  (This has been the case since the author of this piece began following events in the Crimea in the 1990s).

Bogomolov has noted that, in estimating mosque participation, the number of Muslims in Ukraine totals approximately 439,000 people, which includes both Ukrainian citizens and non-citizens. He feels the estimate provides a “more realistic count” than the common estimate of two million Muslims that was used shortly after Ukraine achieved independence.  While mosque participation may not be the best method to judge the extent of the Muslim community, it still makes up a very small percentage of Ukraine’s population of some 45 million souls.

**The growth of Muslim communities**

Despite the difficulty in estimating the Muslim population, it is certainly true that its organization has increased substantially in the years following the independence of the Ukraine and its membership in the Commonwealth of Independent States (CIS)–the organization founded in December 1991 by the Ukraine, along with the Republic of Belarus, and the Russian Federation, and later joined by nine former Soviet Republics.

Among the CIS states of predominantly non-Muslim population, Ukraine deserves special attention. First, beginning with the collapse of the Soviet Union, there soon emerged a number of nationalist-qua-separatist organizations in the Crimea. According to Russian reports the Crimea was then in the process of creating “bases of Wahhabism”, i.e., Islamist nodes fostered and financed by Saudi Arabia.  As Moscow saw it, the Saudis were clearing a fertile field for an Islamic outreach (dawaa) program that would reach the more than two million Ukrainian Muslims, a majority of whom lived in what Islam traditionally called the Tatar territory of the Crimea.

Shortly after gaining independence on 24 August 1991 the nascent republic was warned by Moscow that certain Ukrainian “radicals” had begun to form ties with the emerging Islamist movement in Chechnya. It was next claimed that “Wahhabite gangs” formed in the Crimea were taking part in the jihad intended to separate Muslim Chechnya from Russia. And the Kavkaz center, based in Lvov, was providing the Internet service used by “Ukranian legionnaires” involved in the Muslim struggle that aimed to incorporate once and for all the Caucasus in the Dar-al-Islam (the House of Islam).

In the Ukraine itself, the first Islamic community was founded in Kiev’s Shevchenko district in 1991.  It was at about the same time that members of the International Muslim Brotherhood (the Ikhwan al-Muslimun) began to make an appearance.  Their effort was soon noted in the creation of Muslim youth camps, the crucible used by the Ikhwan elsewhere to mold future leadership.

In August 1992 the General Administration of Muslims of Ukraine was founded and its leader, Sheikh Ahmed Tamim, urged enjoined Muslims, actual and lapsed, to begin the study of the Koran. He founded a madrassah for that purpose later that year.  In September 1993 the organization was renamed the Spiritual Administration of Muslims of Ukraine (DUMA). It was determined to unite the nation’s Muslims and provide religious training.  Later that year the Islamic Institute of Kiev opened its doors.

Fortunately for the Ukraine, Sheikh Ahmed Tamim, the Grand Mufti of Ukrainian Muslims, took a cautious approach in what was then an emerging Muslim community that was finally free of the Soviet yoke. Tamim did not disguise his concern that the entry of Ikhwan and their “wahhabite ideas” was counterproductive.  Thus, he urged Ukranian authorities to “take drastic steps for strengthening their control over the activity of organizations and movements nominally related to Islam.” Tamim warned that Wahhabi “propaganda literature” enjoyed an “uncontrolled diffusion in the Ukrainian regions.”  The propaganda with which the Grand Mufti was concerned was being printed in the Ukraine in both Arabic and Ukrainian. Material was being sent from the Ukraine to the Caucasus and into nearby Belarus.  Its production was being financed by Saudi Arabia’s very Islamist World Assembly of Muslim Youth, an organization penetrated throughout by the International Muslim Brotherhood. It followed that in Kiev a Department of Religious Affairs was created which served under the Minister of Justice at the national level. Regionally, the Crimean Council of Ministers was responsible for giving legal recognition to Muslim communities.

**Ar-Riad and the Muslim Brotherhood**

It was debatable how much influence Sheikh Tamim himself had in Crimea because a Crimean Tatar Mejlis (organization) emerged and seemingly operated independently of Kiev.  A Crimean Tatar Muftiyat soon emerged which united in a single body the mufti responsible for the organizing of mosque communities. The Tatar Mejlis emerged as the nation’s best organized Muslim political association.  However, it was soon under attack following the arrival of Ar-Riad (The Association of Social Organizations in Ukraine), an Arab-sponsored Islamic dawaa movement founded in 1997 and funded by Saudi Arabia. Other smaller organizations included the Hizb al-Tahrir (established in 2003, and an Islamist organization often criticized in the West), and a few “Salafi (Wahhabi) groups, which were in the main based in the Crimea. Politically, an Islamic Party of Ukraine was founded, but has had little impact. (Parties must achieve 4% of the vote to gain representation in parliament.  Thus it is only by forming blocs that the smaller parties are represented.)

The Ar-Riad united the many clandestine efforts of Muslim students (especially those that had been involved in the convening of youth camps) in a single organization. It was led by one Abu Obeid, who would shortly afterward be denied entrance to Ukraine. Internationally, it was a participant in the World Association of Muslim Youth, and it was funded from Saudi Arabia.  Throughout, it was an Ikhwan operation.  The same year it was founded, Ar-Riad organized a summer camp that brought Muslim youth leaders from all parts of the Ukraine. The training program involved lectures, group discussions, and other elements devoted to the propagation of dawaa.  In addition, Ar-Riad opened a book publishing house in Odessa in 1998 (its opening coincided with the opening of three new mosques in the Crimea).  Later that year the movement began the publication of its Ar-Riad newspaper, which included articles by or on Ikhwan ideologues including Banna, Qutb, and Qaradawi.

By the new millennium the Muslim Brotherhood, though limited in membership (approximately 300 senior members, with 30 cells in Crimea alone), was the most active Muslim spearhead operating in the Ukraine. Its Ar-Raid, for years led by Ismail Qadhi, remains to the present a member in good standing of the Ikhwan-dominated Federation of Islamic Organizations in Europe (FIOE). Ar-Riad takes part in numerous activities “in the administrative, religious, cultural, educational, charity, public relations, media, and civilizational communication fields,” as well as outreach (dawaa). The organization, composed of “anywhere from 9-13 chapters,” includes those in Kiev, Crimea, Donetsk, Kharkiv and Odessa. It has recently been claimed that Ar-Riad is funded by the Saudi Islamic Development Bank.

In the Ukraine the Al-Raid reportedly has developed a large clientele and a network of regional branches.  While these groups do receive funding from Saudi Arabia and the Gulf states and is a member in global Islamic networks, Muslim activity has in large part been devoted to building local communities. There are no recent reports that Ukrainian Muslims may have been enticed to join jihadists in the Caucasus, Syria or the Maghreb.  One indication of how closely the movement is watched was the treatment given to the chairman of Ar-Riad in April 2000.  Following a trip to Egypt, he was denied re-entry to the Ukraine. Still, the government has done nothing to halt the entry of young Egyptian and Gulf Arabs from participating in summer dawaa.

**The Russian response**

In the Crimea it has been claimed that the ethnic-Russian majority actually assists the Ar-Riad.  It does so in order to weaken the local Crimean Mejlis subservient to Kiev and to its Muslim hierarchy involved with the Department of Religious Affairs.  While the Mejlis has received de facto acknowledgement from the Ukrainian government, that status has been disputed by Russian nationalists. The result has been reports of “significant disagreements” between the Crimean Mejlis and its Muftiyat, which has been penetrated throughout by the “Wahhabis.” As far as the Muslim leadership in Kiev was concerned, the Wahhabis are attempting to introduce a foreign ideology that conflicts with the Tatar traditional way of life.

In opposition to the growing radicalism in the Crimea, the relationship between the government and the Crimean Mejlis was strengthened with the creation of a Crimean Tatar advisory board that advised President Kuchma.  A seemingly competitive “Council of Crimean Tatars” was then chosen by Prime Minister Yanukovich.

The relationship between the Mejlis and the Rukh (center right, western Ukraine) Party precedes that of the creation of the Republic. It is based on arrangements made by “dissident Ukrainian nationalists (i.e., Tetyana Chernovil) and Crimean Tatars (especially Mustafa Jemilev) in Soviet prisons.” The Rukh then assisted the Crimean Tatars “to establish a voice within the national Ukrainian political landscape in the early years of Ukrainian independence. Early on, the Rukh Party viewed Crimean Tatars as natural allies in a Russian-dominated Crimea.”  And if the Crimean Tatars and other Ukrainian Muslims have support today, it still comes from center-right allies in Kiev and western Ukraine.

**The Al-Rakhma Mosque as symbol**

The Al-Rakhma (mercy) mosque, which opened in Kiev in December 2011 in the former Muslim quarter of Tatarka, was the first to be built in Kiev since the independence of the Ukraine. Tatarka was the site where Muslims of many nationalities, “but mostly Tatars,” congregated in the 19th century.

In 1987 a small prayer house was opened to serve some 500 Muslims. The Muslim community was officially registered in Kiev in 1991, and in 1994 began the construction of the copper-domed Al-Rakhma mosque completed two decades later. Its opening was welcomed by the same Grand Mufti of Ukraine Sheikh Ahmad Tamim, the leader who had first warned of Wahhabi penetration.

Included in the mosque complex reportedly financed by the local community, there has been built an administrative building, a publishing house, a madrassah, a wedding hall, and space for an incipient Muslim university.  Although there is a minaret, the cautious Sheikh Tamim, still waging a battle with extremists, stated that a muezzin would not be calling people to pray because, “We are trying to take into consideration the environment we live in and the interests of the people around us, and as we strive for peace and mutual understanding, the minaret only remains a symbol.”

The effort to maintain a peaceful coexistence was welcomed. It has been 18 years since the All-Ukrainian Council of Churches and Religious Organizations was formed, which has since its founding in 1995 included a Religious Department for Muslims of Ukraine.  And Bishop Yevstratii, Kiev Patriarch of the Ukrainian Orthodox Church, added, “The new mosque is situated in a district called Tatarka, which signifies that Tatars began to settle in Kyiv quite a long while ago. So, the relations between Christian and Muslim Ukrainians have a long history; it was not easy, but it is shared by all of us. It is obvious that in the conditions of the modern globalized world there are representatives of practically all world religions in any big European city, and they require a place to gather and pray. That is why it is good that Kyiv Muslims will have a place like this.”

It is ironic that Ali Khamzin, the head of the foreign relations department of the Mejlis of the Crimean Tatar people, was somewhat more cautious.  He noted that the year 2011 had been, “a year of good hopes for the Ukrainian Muslims because in March, after long-lasting protests of Crimean Tatars and court cases on this matter, Crimean Muslims finally managed to legally obtain an official order to build a mosque-cathedral Buyuk Juma Jami in Simferopol.”  He did see the construction of a mosque in Kiev and the approval of one for Simferopol was “an important step of Ukraine’s government, Ukrainian society and the nation towards the Muslims in the country, their rights and expectations.”  He added, “Nowadays there are many questions concerning relations within the Muslim community of Ukraine as well as its relations with the government. But the main issues should be settled in an unbiased dialog between the Muslim community and the government. We have a lot of examples of such relations which usually have [a] positive outcome.”

It was likely that still fresh in Khamzin’s memory were the recent clashes that occurred in the Crimea.  Crimean Tatars maintain a list of places over which they claim historical, cultural and religious ownership, including the Aziz in Bakhchisaray, Crimea.  This Muslim cemetery and pilgrimage site was demolished by the Soviets and a market was built on top of it.  It remains today a point of conflict between Russian nationalists and ethnic Tatars.  When Tatars began in August 2006 to move to take back the site, they were met by strong local resistance.  To at least one observer, “it was clear that the so-called Russian ‘Cossacks’ were the main culprits.”  The explosive situation was ended with the arrival of security forces, armored vehicles, and by the Tatar Mejlis effort to arbitrate the dispute.

As it now stands, the Tatars have no better ally than the western Ukrainians.  Should the Crimea fall to the Russians, the general freedom that the Tatar have enjoyed will almost surely be ended.  For there is one thing that is certain, the Russian government hates the Ikhwan.  For more than two decades it has attacked the organization in words whenever and wherever it could, and it holds the Ikwhan-qua-”Wahhabi” responsible for prolonging the jihad in the Caucasus. Given free rein in the east, a Russian invasion would almost assuredly put an end to the Ikhwan, to dawaa, and to the Tatar Mejlis.

***J. Millard Burr*** *is a Senior Fellow with the American Center for Democracy.*

Elbit Keeps Eye On Carnival Crowds

Source: http://www.hstoday.us/single-article/elbit-keeps-eye-on-carnival-crowds/f7b55ad0fe786be59edb 92c6314e4db3.html

**Elbit Systems has used the Carnival in São Salvador da Bahia, Brazil as the launch pad for its new wide-area persistent surveillance ground system which generates real time intelligence imagery.**

GroundEye’s high resolution images are assisting security forces to ensure the safety and security of the thousands of people who are participating in the Carnival celebrations that began on February 27 and end March 5.

Elbit said it developed the system to meet the growing demand of security forces and decision makers to achieve continuous intelligence imagery covering a wide area of interest in high resolution and in real time for situational awareness purposes, especially during large scale events.

With GroundEye, security forces can monitor and deal with multiple events simultaneously in real time, or, if missed in real time, as soon as an operator is available. **GroundEye retains in its memory both the area and time dimensions in their entirety, allowing precise comprehension of activities in the area and generation of high-quality and comprehensive intelligence data. In addition, the system detects and issues alerts upon the occurrence of pre-programmed events.**

The system used during the Salvador Carnival is designed for both civilian and military applications, including border protection, perimeter control of infrastructure and critical sites, military operations, safe city programs and large scale events.

**GroundEye’s main components are a mast-top, non-rotating panoramic sensor head, a processing and storage unit and several operator stations. It can be operated either in a stand-alone mode or in a command and control (C&C) network integrated mode, meshing with the customer’s existing command and control networks.**

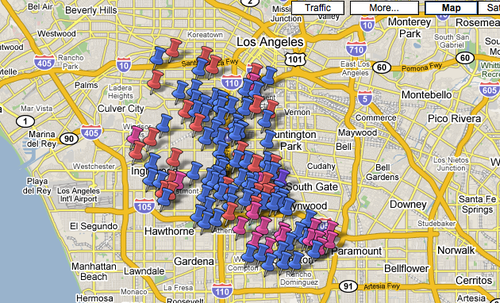
GroundEye employs several high resolution sensors which operate in parallel, coupled with fast and parallel specialized electronics/ software, for processing and controlling the imagery. Located at the foot of the mast is a large storage device used to store the volume of imagery flowing from the mast-top sensors, at the same time it is being viewed.

This multiple random-read access, allows several users to examine, in parallel, several events which occurred at different times and in different locations.

|  |
| --- |
| EDITOR’S COMMENT: Cutting edge technology works best in an overall technologically advanced security environment. If not then it just might multiply the possibility of been unable to “connect the dots” and come to solid conclusions regarding imminent threats. Mega events are a good environment to test and sell new technologies but cannot fix the unorthodoxus shift that these events follow. They are supposed to be happy mass gatherings either for fun or for sports. Instead they become a good excuse for new arms sales and spending of extraordinary amounts of money – especially in a big country where the equilibrium between upper and lower classes has been lost for good. |

## Gangbangin' in Syria: Two L.A. gang members in Syria to defend Assad regime

Source: http://www.homelandsecuritynewswire.com/dr20140307-gangbangin-in-syria-two-l-a-gang-members-in-syria-to-defend-assad-regime

About a hundred Americans have gone to Syria to take part in the war, all of them — with the apparent exception of two L.A. gang members named “Creeper” and “Wino” — to fight on the side of the Sunni rebels against the Alawite Assad regime. In a video recently posted on YouTube, the two are shown brandishing AK-47s and firing at an unseen enemy. **Their tattoos identify one of them as a member of Sureños-13, which is affiliated with the Mexican mafia, and the other as a member of Westside Armenian Power gang.** They tell the camera they are “in Syria, gangbangin’.”

Two Los Angeles gang members are taking part in the Syria’s civil war, raising security worries on the West Coast.

ABC News reports that a video posted recently on YouTube shows two gang-tattooed and camouflaged men, who call themselves “Creeper” and “Wino,” holding AK-47s and saying that they are “in Syria, gangbangin’.”

The video has been posted online a few days ago, but the LAPD says they learnt about the two LA gang members in Syria five weeks ago.

Deputy Chief for Counterterrorism Mike Downing told ABC News Sunday that “My organized crime and gang investigators found it online and on Facebook,” Downing said. “We’re kind of concerned about their recruitment and whatever other associates they have here… We predicted this would happen — the [organized crime and terrorism] convergence. What we’re worried about is the ones we don’t know about here or coming back to the U.S.”

Downing said the two men — one Armenian and the other Latino, neither one a U.S. citizen — are members of a local gang, not radicalized Islamist jihadists. In fact, the two men are fighting as part of a Hezbollah formation to defend the regime of President Bashar al-Assad.

Downing said that one, perhaps even both, were deported from the United States some time ago, a fact mentioned on the gangsters’ public social networking posts.

In the video, Wino is shown firing his AK-47 at unseen enemies (or “enemigas,” as he calls them) through a hole in the wall of a destroyed building. Between rounds, he turns to the camera and says: “We’re on the f—king frontline, homie. Front-f—king-line, homie. We don’t give a f—k, dawg.”

Close to a hundred Americans went to Syria to take part in the war, all of them – with the apparent exception of the two L.A. gang members – to fight on the side of the Sunni rebels against the Alawite Assad regime.

About fifty of them have already returned to the United States, where they are under FBI monitoring. Some have been questioned, and others are under surveillance.

FBI director James Comey and Director of National Intelligence James Clapper told lawmakers that U.S. authorities are concerned that these individuals were radical enough to risk their lives in Syria, where they have also picked up useful training in terrorism tradecraft from the al-Qaeda-affiliated jihadist groups.

All fifty returnees have had combat experience in Syria.

ABC News notes that on Facebook, a man calling himself Wino Ayee Peeyakan, who looks to be the same man as in the YouTube video, has posted dozens of photos from Syria displaying his “APX3” gang tattoos, indicating he belongs to the Westside Armenian Power gang, and admits he was deported from the United States several years ago, leaving behind a child in Los Angeles.

“Man im come back thru Mexico turn my self in do couple of yers and get out [sic],” Peeyakan commented a year ago on a photo of his daughter.

The other gang member appearing with Peeyakan in photos and the video calls himself “Creeper.” He displays tattoos for Sureños-13, which is affiliated with the Mexican mafia.

“Tell the homies in f—king Middle East, homie, still gangbanging, homie, putting that s—t down for the big Sur-13 gang,” Creeper says in the video.

|  |
| --- |
| EDITOR’S COMMENT: I recall a paper I read some time ago writing that US gang members join the military to acquire specialized knowledge on fire arms, explosives, communications etc. Perhaps now gang members adapt in the new security environment and go to war zones for more effective street fighting “methodologies”! |

# Surveillance Balloons

Source: http://i-hls.com/2014/03/israeli-tech-aerostats-worldwide/



SPEED-A camera on the Skystar aerostat

Static surveillance balloons or blimps are considered almost standard equipment for monitoring borders, facilities, areas and army bases. Similar to unmanned aerial vehicles, modern aerostats carry advanced payloads, with cutting edge cameras and sensors. They provide real time intelligence essential for defending bases, facilities and borders and for carrying out tactical operations.

Clients in Israel, the Canadian Army and Europe use advanced, combat-proven Israeli payloads on board their aerostats.

The Israeli payload includes the advanced thermal camera SPEED-A. This multi-mission, gimballed system features a continuous optical zoom lens, allowing for constant coverage of targets even in harsh conditions. The payload can also be fitted with an optional laser range finder. It weighs 23 kilograms and is especially suited for aerostats, providing long range surveillance capabilities and high-resolution images. The SPEED-A is manufactured by the Israeli CONTROP.

## High level of “brain waste” among highly educated immigrants

Source: http://www.homelandsecuritynewswire.com/dr20140310-high-level-of-brain-waste-among-highly-educated-immigrants

Many highly educated immigrants coming to the United States without a job lined up have been unable to find work at their level of education, leading to considerable “brain waste,” Purdue University researchers have found.

Agricultural economics professors Brigitte Waldorf and Raymond Florax were on a team of researchers who analyzed data from the U.S. Census Bureau and its American Community Survey to determine the prevalence and persistence of job-education mismatch among male immigrants in the United States from 1980 to 2009.

“Overeducation is more of a reality for people who come to the United States to be with family,” said Waldorf, co-author of the research. “They have not been recruited by a specific employer, and they often do not find a job that matches their education.”

A Purdue University release reports that the researchers found that, throughout the period, the level of education of nearly half of immigrants was above the education requirements for their job, compared with one fourth of men born and living in the United States. **The prevalence of such “brain waste” exceeded 40 percent for immigrants with a bachelor’s degree, 50 percent for those with a doctoral or professional degree, and 75 percent for those with a master’s degree. The overeducation prevalence for U.S. natives was 10-20 percentage points lower.** Over time, immigrants find suitable jobs, but not to the extent of U.S. natives.

Waldorf noted that prevailing thinking assumes that highly educated immigrants are a significant gain for the U.S. economy and society. The researchers said, however, that “given the abundance of foreign and domestic talent in the United States, with much of it being poorly matched in the labor market, a policy shift toward attracting even more global talent may actually be backfiring.”

One possible consequence of large numbers of highly educated immigrants is that some Americans might look for opportunities abroad to find a job that better matches their education.

Similarly, immigrants who are highly skilled and highly educated may become more likely to return to their home country or move to a third country because they are unable to get a suitable job in the United States, at least initially.

“In anticipation of being overeducated in the United States, migrants from other countries may also simply not choose the United States in the first place,” the researchers said.

The study also identified circumstances influencing the risk of immigrants being overeducated for the jobs they got. One key finding was that assimilation — integrating into U.S. society such as by learning the English language — helped highly educated immigrants find a job that adequately matched their education level. Conversely, lack of proficiency in English “was the most powerful predictor” of immigrants unable to get a suitable job, the researchers concluded.

Policymakers should put greater emphasis on measures that foster the assimilation and integration of newcomers when considering a shift toward increasing immigration to attract specific skills, the researchers said. Possible strategies include English language classes and extending work permits to family members.

The study was published in the Journal of Regional Science.

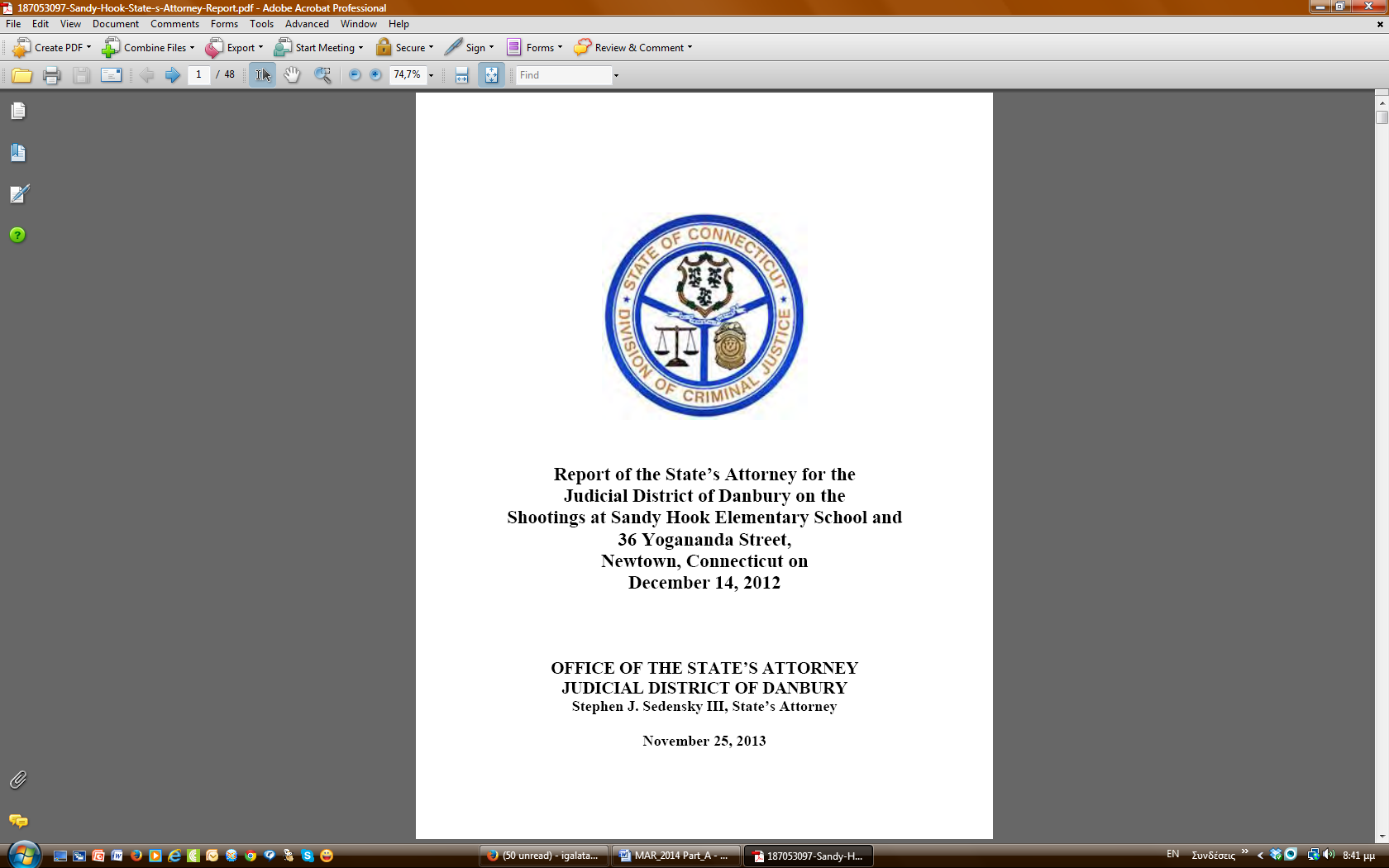
The release notes that women were not included in the study because women often had complex labor market careers, especially during the 1980s and 1990s, which included stints of part-time employment or temporarily dropping out of the labor force from having children.

*— Read more in Julia Beckhusen et al., “Attracting Global Talent and Then What? Overeducated Immigrants in the United States,”* Journal of Regional Science *53, no. 5 (December 2013): 834–54*

|  |
| --- |
| EDITOR’S COMMENT: An interesting article that brought back memories from my 2013 adventure in Houston, TX… |

### Shootings at Sandy Hook elementary State Attorney's Office repor

**Executive summary**

The purpose of this report is to identify the person or persons criminally responsible for the twenty-seven homicides that occurred in Newtown, Connecticut, on the morning of December 14, 2012, to determine what crimes were committed, and to indicate if there will be any state prosecutions as a result of the incident.

The State’s Attorney for the Judicial District of Danbury is charged, pursuant to Article IV, Section 27 of the Constitution of the State of Connecticut and Connecticut General Statutes (C.G.S.) Sec. 51-276   *et seq.*, with the investigation and prosecution of all criminal offenses occurring  within  the  Judicial  District  of  Danbury.  The Connecticut State Police have  the responsibility to prevent and detect violations of the law and this State’s Attorney has worked with and relied upon the Connecticut State Police since the incident occurred.

Since December 14, 2012, the Connecticut State Police and the State’s Attorney’s Office have worked  with  the  federal  authorities  sharing  responsibilities  for  various  aspects  of  this investigation. Numerous other municipal, state and federal agencies assisted in the investigation. The investigation materials reflect thousands of law enforcement and prosecutor hours. Apart from physical evidence, the materials consist of more than seven-hundred individual files that include reports, statements, interviews, videos,  laboratory  tests  and  results,  photographs, diagrams, search warrants and returns, as well as evaluations of those items.

 In the course of the investigation, both state and federal law enforcement personnel received a large number of contacts purporting to provide information on the shootings and the shooter. Although  many times  these “leads”  would  go  nowhere,  each  one was  evaluated  and  often required substantial law enforcement time to pursue. An abundance of caution was used during the investigation to ensure that all leads were looked into, despite the fact that more than 40 such “leads” proved, after investigation, to be unsubstantiated. Information that was substantiated and relevant was made part of the investigation.

It  is  not  the  intent  of  this  report  to  convey  every  piece  of  information  contained  in  the voluminous investigation materials developed by the Connecticut State Police and other law enforcement agencies, but to provide information relevant to the purposes of this report. While no report is statutorily required of the State’s Attorney once an investigation is complete, it has been the practice of State’s Attorneys to issue reports on criminal investigations where there is no arrest and prosecution if the State’s Attorney determines that some type of public statement is necessary. Given the gravity of the crimes committed on December 14, 2012, a report is in order.

On the morning of December 14, 2012, the shooter, age 20, heavily armed, went to Sandy Hook Elementary School (SHES) in Newtown, where he shot his way into the locked school building with a Bushmaster Model XM15-E2S rifle. He then shot and killed the principal and school psychologist as they were in the north hallway of the school responding to the noise of the shooter coming into the school. The shooter also shot and injured two other staff members who were also in the hallway.

The shooter then went into the main office, apparently did not see the staff who were hiding there, and returned to the hallway.

After leaving the main office, the shooter then went down the same hallway in which he had just killed two people and entered first grade classrooms 8 and 10, the order in which is unknown. While in those rooms he killed the two adults in each room, fifteen children in classroom 8 and five in classroom 10.  All of the killings were done with the Bushmaster rifle.

He then took his own life with a single shot from a Glock 20, 10 mm pistol in classroom 10.

Prior to going to the school, the shooter used a .22 caliber Savage Mark II rifle to shoot and kill his mother in her bed at the home where they lived at 36 Yogananda Street in Newtown.

The response to these crimes began unfolding at 9:35:39 a.m. when the first 911 call was received by the Newtown Police Department. With the receipt of that call, the dispatching and the arrival of the police, the law enforcement response to the shootings began. It was fewer than four minutes from the time the first 911 call was received until the first police officer arrived at the school. It was fewer than five minutes from the first 911 call, and one minute after the arrival of the first officer, that the shooter killed himself. It was fewer than six minutes from the time the first police officer arrived on SHES property to the time the first police officer entered the school building. In fewer than 11 minutes twenty first-grade pupils and six adults had lost their lives.

The following weapons were recovered in the course of this investigation: (1) a Bushmaster Model XM15-E2S semi-automatic rifle, found in the same classroom as the shooter’s body. All of the 5.56 mm shell casings from the school that were tested were found to have been fired from this rifle. (2) a Glock 20, 10 mm semi-automatic pistol found near the shooter’s body and determined to have been the source of the self-inflicted gunshot wound by which he took his own life. (3) a Sig Sauer P226, 9 mm semi-automatic pistol found on the shooter’s person. There is no evidence this weapon had been fired. (4)  a Izhmash Saiga-12, 12 gauge semi-automatic shotgun found in the shooter’s car in the parking lot outside the school, and which was secured in the vehicle’s trunk by police responding to the scene. There is no evidence this weapon had been fired. (5) a Savage Mark II rifle found at 36 Yogananda Street on the floor of the master bedroom near the bed where the body of the shooter’s mother was found. This rifle also was found to have fired the four bullets recovered during the autopsy of the shooter’s mother.

All of the firearms were legally purchased by the shooter’s mother. Additionally, ammunition of the types found had been purchased by the mother in the past, and there is no evidence that the ammunition was purchased by anyone else, including the shooter.

At the date of this writing, there is no evidence to suggest that anyone other than the shooter was aware of or involved in the planning and execution of the crimes that were committed on December 14, 2012, at Sandy Hook Elementary School and 36 Yogananda Street. From the time an unknown male was encountered by the Newtown police outside of the school during the initial response, until well after the staff and children had been evacuated, the thought that there may have been more than one shooter was a condition all responding law enforcement worked under as they cleared the school. Individuals located in the wooded areas surrounding the school as the searches and evacuations were taking place were initially treated as suspect and handled accordingly (including  being  handcuffed)  until  their  identity  could  be  determined.  The circumstances surrounding  all  of  these  individuals  were  fully investigated  and  revealed  no additional shooters. DNA testing of evidence recovered from both the school and 36 Yogananda Street also revealed no potential accessories or co-conspirators.

It is the conclusion of this State’s Attorney that the shooter acted alone and was solely criminally responsible for his  actions  of that  day.  Moreover, none of the evidence developed to  date demonstrates probable cause to believe that any other person conspired with the shooter to commit these crimes or aided and abetted him in doing so.

Unless additional – and at this time unanticipated – evidence is developed, there will be no state criminal prosecution as result of these crimes. With the issuance of this report, the investigation is closed. Should additional reliable information related to the existence of accessories or co- conspirators come to the attention of the investigators, the investigation will be reopened.2

 In the course of his rampage the shooter committed a number of crimes in violation of our Connecticut Penal Code.  The most significant are those where lives were taken and people were physically injured.  In  Sandy Hook  Elementary  School,  the  crime  of Murder  under  Special Circumstances,  in  violation  of  C.G.S.  Sec.  53a-54b,  was  committed  twenty-six  times  and Attempted Murder under Special Circumstances in violation of C.G.S. Secs. 53a-49 and 53a-54b was committed twice as it relates to the two individuals who were shot by the shooter and survived. The crime of Murder in violation of C.G.S. Sec. 53a-54 was committed by the shooter in killing his mother.

The  obvious  question  that  remains  is:  “Why  did  the  shooter  murder  twenty-seven  people, including twenty children?” Unfortunately, that question may never be answered conclusively, despite the collection of extensive background information on the shooter through a multitude of interviews and other sources. The evidence clearly shows that the shooter planned his actions, including the taking of his own life, but there is no clear indication why he did so, or why he targeted Sandy Hook Elementary School.

 It is known that the shooter had significant mental health issues that affected his ability to live a normal life and to interact with others, even those to whom he should have been close. As an adult he did not recognize or help himself deal with those issues. What contribution this made to the shootings, if any, is unknown as those mental health professionals who saw him did not see anything that would have predicted his future behavior. He had a familiarity with and access to firearms and ammunition and an obsession with mass murders, in particular the April 1999 shootings at Columbine High School in Colorado. Investigators however, have not discovered any evidence that the shooter voiced or gave any indication to others that he intended to commit such a crime himself.

This State’s Attorney expresses his sincere sympathy and condolences to the victims of the incident of December 14, 2012, and to their families. He also expresses his appreciation for their continued patience and understanding during the course of the investigation and preparation of this report. He acknowledges and thanks law enforcement, which responded to Sandy Hook Elementary School in minutes and entered the building believing someone could be there ready to take *their* lives as well. He also acknowledges and thanks the staff of the Sandy Hook Elementary School who acted heroically.  The combination saved many children’s lives.

This report would not have been possible if not for the assistance and cooperation of numerous agencies at the state, local and federal levels of government. The State’s Attorney expresses his sincere gratitude and appreciation to all of these agencies and to all of the men and women who contributed  so  much  to  this  investigation.  The  assistance  of  federal  authorities  has  been invaluable. Particularly worthy of special note are the men and women of the Connecticut State Police, and in particular, the Western District  Major Crime Squad.   The thoroughness  and sensitivity with which they conducted their investigation is unmatched in my experience.

# Touching moment giraffe says goodbye to dying zoo worker

Source: http://www.express.co.uk/news/world/466101/Touching-moment-giraffe-says-goodbye-with-a-kiss-to-dying-worker-in-Holland-zoo

|  |  |  |
| --- | --- | --- |
|  |  |  |

March 21 – The 54 year-old maintenance worker, known only as Mario, had his last wish granted as he was taken to the zoo on his hospital bed to say farewell to the animals.

And one of the giraffes, apparently sensing that the man was unwell, came over and nuzzled him.

Mario has spent his entire adult life cleaning the animal enclosures at the Diergaarde Blijdorp zoo in Rotterdam.

And, when he was diagnosed with a terminal illness, his last wish was to pay a final visit to his former workplace.

Kees Veldboer, founder of the Ambulance Wish Foundation - which took Mario to the zoo - said that the animals also wanted to say goodbye to Mario.

He said: "These animals recognised him, and felt that things aren’t going well with him.

"It was very nice that we were able to work on the last wish of this man."

He described the encounter with the giraffe as "a very special moment", adding: "You saw him beaming."

The Ambulance Wish Foundation is a charity which helps terminally ill patients with mobility issues to fulfil their dying wishes.

Giraffes are non-territorial animals who travel in social groups.

Recent research has shown that they form special bonds with other animals in their herd.

|  |
| --- |
| EDITOR’S COMMENT: Just a reminder of the recent giraffes’ slaughter in Danish Zoos… Giraffes’ also have feelings and souls; I am not sure about many people in our civilized societies… |

# Are Income Taxes Political Weapons Of Mass Destruction?

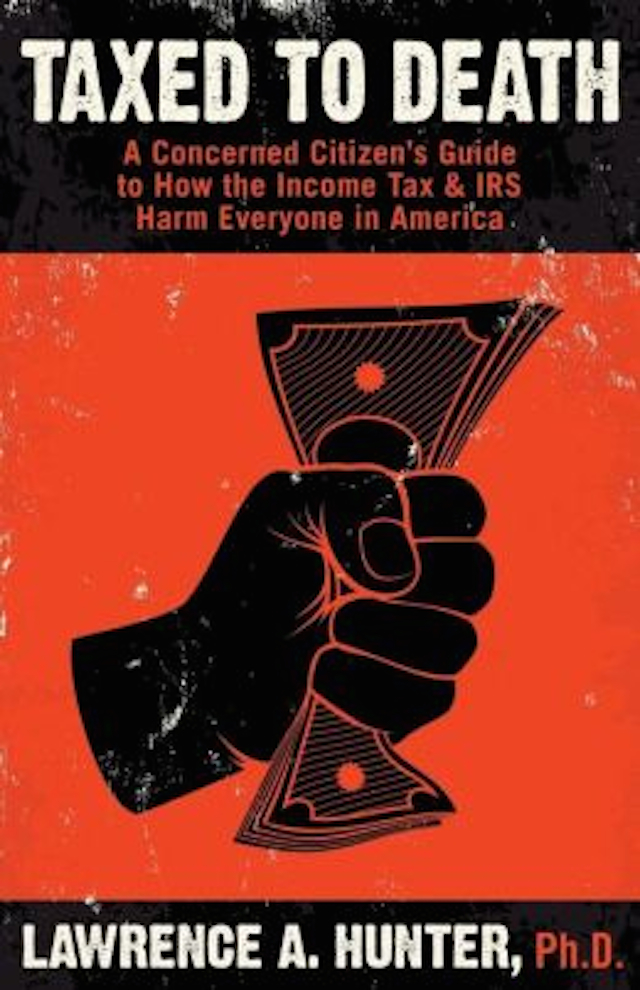
**By John Tamny** (Forbes Staff)

Source: http://www.forbes.com/sites/johntamny/2014/03/21/are-income-taxes-political-weapons-of-mass -destruction/

I was first introduced to Larry Hunter back in 2008 by a mutual friend. It was amid the banking implosion, and Larry and I were somewhat alone in saying the bailouts were a terrible idea that would rob the economy of a natural recovery.

Since then I’ve at times served as Hunter’s editor, and have learned a lot from him. Most important there has been his energetic support for scrapping the tax code in favor of a simple consumption tax.

The latter always made sense to me given my belief that an income tax is a negative price placed on work. And since all economic advancement is a function of savings, the best kind of tax is one on consumption so that neither work nor saving are penalized.

Happily, Hunter several years ago alerted me to what is arguably an even better feature of the consumption tax: it’s the only way we citizens can limit how much we hand over to the federal government each year. This is hugely important. If we can limit the federal government’s intake it not only means less in the way of economy-sapping government spending, but it also means that it will be harder for the feds to run up deficits owing to our power to limit what we send them. It says here that worry about deficits ignores the true problem which is spending, but for those kept up at night about deficits, a consumption tax is arguably the answer for them.

Thankfully for readers, Hunter has written a very interesting new book, [Taxed to Death: A Concerned Citizen’s Guide to How the Income Tax & IRS Harm Everyone in America](http://www.amazon.com/Taxed-Death-Concerned-Citizens-Everyone/dp/1457525089/ref=sr_1_2?s=books&ie=UTF8&qid=1395086005&sr=1-2&keywords=taxed+to+death). For those concerned about taxes and the growing power of the IRS, this is a book for them.

Hunter does not pull punches. He begins by saying that “Income taxes are political weapons of mass destruction used by governments against their own people,” and that “During the past century, the IRS has grown into a vicious, hydra-headed monster, a bureaucratic despot, completely out of control and in principle uncontrollable.” Hunter doesn’t shy away from being up front, and he has a point.

Indeed, how odd that a country founded on great skepticism about politicians such that its founders penned a founding document that is a monument to skepticism now has an unelected IRS bureaucracy that the citizenry must cower before each year. Something’s wrong with that, and something’s seriously wrong when we’re forced to hand over so much of our earnings each year to the very political class that was supposed to be limited in its activities by the Constitution. Of course as Hunter so entertainingly writes, “politicians and judges read the Constitution the way a sinner reads the Bible: constantly searching for loopholes.”

Hunter argues early that the situation with the IRS and the tax code is going to get worse, that “The revelations about the IRS’s most recent illegal unconstitutional targeting of individuals, non-profit organizations and businesses for their political, religious and ideological beliefs, is just the tip of the iceberg.” Figure what’s happened is bad enough. As is we have to prove our income each year, and then it’s arguable that IRS targeting of Tea Party and other political entities altered the course of history thanks to the inability of groups to influence the 2012 elections, not to mention the passage and rollout of Obamacare itself.

Still, we are ultimately talking about the federal government here. Not excusing for even a second its meddling ways, it would be interesting if Hunter had further covered the arguable truth that a federal government eager to meddle in everything meddles in nothing. These aren’t the most competent of people, by definition.

That’s why Hunter at times strikes as too negative. The IRS is undeniably a major problem, but when Hunter argues that it is or will create a “welfare-warfare superstructure of collectivism,” I think he perhaps gives these salary-takers too much credit. They lack the skill to create what Hunter presumes, and no doubt they lack the ambition.

Considering Hunter’s point that an “income tax is simply not fit for a free and prosperous people,” he’s 100% right. Still, is the IRS the problem, or is it the political class itself? Hunter correctly writes that “IRS abuse is in the nature of the beast, part and parcel of the income tax and largely uncorrelated to which political party or group of bureaucrats happens to be riding the beast at any given moment.” To reform the IRS is to miss the point. It’s the tax code that needs to be fixed, and quite realistically abolished. A Congress that writes the tax code is the problem.

Hunter writes that the U.S. “has suffered under the curse of the income tax since 1913, and it has taken an enormous toll in lost economic output and prosperity.” That’s what is most bothersome. Though we live in a staggeringly rich country, the horrifying “unseen” is how much wealthier we would be, how much higher our living standards would be, how much more advanced our healthcare would be, if the federal government hadn’t been penalizing work for 100 years, not to mention pouring gasoline on the slower growth fire through economy-sapping spending.

Hunter notes that the top 1 percent of earners pay 37 percent of total income tax revenue, but before readers assume Hunter’s dislike of the income tax is rooted in throwing a bone to the 1 percent, they should read on. Hunter writes that “it is precisely the people with too little income to tax who suffer the most.” Absolutely.

There are no companies, no start-ups and no jobs without investment first. The rich, by definition, have the most to invest. So when the tax code penalizes their achievement, or singles them out for having had the temerity to be born rich, those who ultimately suffer are those who don’t earn a lot of money, and who weren’t born rich precisely because there’s reduced investment in the companies of tomorrow that will improve our lives and employ us.

If you like taxation and government spending you must think that John Boehner, Nancy Pelosi, Mitch McConnell, and Harry Reid are better at allocating capital than Warren Buffett, Paul Tudor Jones, Jeff Bezos, and the late Steve Jobs. Think about that for a moment. Hunter’s argument isn’t partisan, rather it’s rooted in common sense. Politicians are the individuals least capable of allocating capital.  
Where there’s disagreement is in Hunter’s assertion that “the more efforts are made to redistribute income, the more inequality increases.” To be clear, forced wealth redistribution is surely abhorrent, but implicit in Hunter’s point is that inequality is something unfortunate. In truth, as inequality rises, lifestyle inequality shrinks substantially. The Forbes 400 is a monument to people who’ve grown rich through turning the former baubles of the rich into goods we all enjoy. Assuming the federal government were to get out of the way, even more capital would be allocated to the “vital few.” Inequality would grow for sure, but this would occur alongside skyrocketing living standards for us all. Something tells me Hunter agrees here.

Where we most definitely agree is that the Fed’s program of quantitative easing is a major indictment of the economics profession itself, and an economic retardant for it in Hunter’s skillful words “cleansing private banks’ balance sheets and taking worthless or underperforming assets onto the Fed’s balance sheet like some kind of financial sin eater.” The Fed defends its actions as necessary to save the economy from a severe recession, but per Hunter’s point, the Fed fails to understand that a recession is exactly what we need so that the economy can be cleansed of all the errors previously made. In vainly trying to help us, the Fed is in fact robbing us of an economic recovery.

Where we perhaps disagree when it comes to the Fed is that its creation in 1913 dissolved “the finely crafted automatic constitutional constraint on the government’s ability to borrow money.” This is a popular view, but lest we forget, the Treasuries that represent U.S. debt pay out dollars, and while the Fed’s role (or lack thereof) in the falling dollar since 1913 is much debated, it can at the very least be said that the dollar has not been very healthy for stretches of time since 1913. That in mind, logic dictates that if we had maintained a gold-defined dollar these last 100 years that the federal government’s ability to borrow would in fact be much greater. Again, Treasuries pay out dollars, if we had a stable dollar the U.S. economy would be in much better shape, and as rich countries are most able to borrow, Fed actions that have robbed us of wealth have also blunted the ability of the federal government to borrow. To reduce spending we must reform Congress, after which the Fed is a separate issue.

Hunter seems to agree, that all the deficit worrying really misses the point. He writes that ultimately “it is the amount of private resources extracted from the private sector and spent through the public sector that generates the ultimate burden on society.” Deficits are just finance, and it’s unrealistic to think they would fall absent the Fed. Logic dictates that our economy would be much better off without the Fed, and with a better economy, the ability of the political class to borrow against it would be even greater.

Considering the nominal cost of tax compliance. Hunter points to an estimate of 6.1 billion hours annually, at a cost of $377 billion as of 2008. Of course, as Hunter knows well, this doesn’t come close to telling the real story. Indeed, what’s unknown is how much bigger the economy would be if those annual hours and spending had been annually directed toward real private production over compliance with a tax code that is a monument to social engineering. It’s useful then to repeat an earlier point that the seen is what a rich country we are, but the unseen is the exponentially greater wealth we’d all be enjoying absent the tax code and compliance with same.

Hunter’s solution to all of this is not a flat tax. Indeed, such a tax would in his words still “require a powerful tax collector with direct access to individuals’ pocketbooks, their bank accounts, and their personal information.” So true, plus it could also easily be meddled with on the way to higher rates as he points out.

I would add to Hunter’s problems with a flat tax that in a sense, it might be too successful. Americans are wildly productive, and because they are, even a flat tax of 10% would involve the voluntary handoff of trillions of dollars each year to the feds.

Hunter’s previously alluded to solution is a consumption tax whereby the feds would have no clue what we earn, not to mention our ability to limit what we hand over. If we’re having bad years such that we’re buying less, so will the federal government suffer. And if we choose to starve them some years by living abroad, that’s fine too.

What I wish Hunter had talked about more is the possibility that a consumption tax would similarly become a lobbyist’s dream. Indeed, it’s easy to assume that high schools and colleges would seek exemption since the “children are our future,” grocery stores might win exemption by using imagery of starving children, the airlines might point to their frequent visits to bankruptcy court as a reason to exempt them…Hunter no doubt knows all of this, and it’s probably true that he would say any good policy needs to be guarded from errant politicians.

The one major area of disagreement concerns a passage that some readers may well enjoy. About midway through his excellent book Hunter writes that “the welfare state redistributes more and more of less and less until driven to its ultimate lunacy, it leaves everyone sharing equally in the misery it creates.” That doesn’t ring true. The reality is that Americans love success too much, and many would work long hours no matter the tax rate. This isn’t me defending the horrid tax code and the rise of the welfare state as much as it’s me saying that Americans are far too enterprising to ever share equally in misery.

That’s what’s so interesting about the tax debate in the U.S. right now. Like Hunter I believe that incentives matter, and that liberty matters even more. In that case, like Hunter I think it’s essential to scrap the tax code with liberty in mind, not to mention the growth that it would bring.

Still, what I can’t get out of my head is all the success that continues to take place in high tax New York and California. This country needs a tax revolt, and needs it badly because our tax code is an affront to free peoples. The irony might be a tax revolt that happily takes place here, in a country full of entrepreneurial people least vulnerable to taxation.

|  |
| --- |
| EDITOR’S COMMENT: Given the current financial (?) turmoil in Greece, I was thinking about introducing a **new** abbreviation for weapons of mass destruction:  C2BRNE2  **“C”** for chemical and cyber threats, **“B”** for Biological, **“R/N”** for radiological & nuclear threats and **“E”** for Explosives and Economy. |

## Racism: troubling truths

**By Michaël Privot**

Source: http://www.opendemocracy.net/opensecurity/micha%C3%ABl-privot/racism-troubling-truths

Fighting racism in Europe is not easy when Europe has two hands tied behind its back—debilitated by neo-liberal policies on the one hand and the securitisation of minorities on the other.

Fifty-four years ago, on March 21st, 69 black demonstrators were massacred in Sharpeville, South Africa. They were demonstrating for equality—they got bullets in return. The date has been declared International Day for the Elimination of Racial Discrimination, in recognition of the harmful impact of racism, and the violence it legitimises, on those targeted on the basis of visible characteristics of difference. We know racism kills but how far is the insecurity of minorities taken on board?

Insecurity is multi-faceted. The quest for security, and against precariousness, can be conceived anthropologically: human survival has been a struggle to bring stability to existence. Human beings settled and started farming to escape the insecurity of hunter-gathering. They flocked into fortified cities to reduce the insecurity of nomadic or rural life. They invented laws to protect themselves from the insecurity generated by the whims of tyrants and other arbitrary power-holders. Some imagined gods and goddesses to reassure themselves about the Hereafter at least. This struggle against all forms of insecurity has of course increased in complexity, parallel to social development, but efforts at repelling insecurity have been an historical constant.

After World War II Europe was home to the last two major attempts to further public security: in Western Europe via welfare states linked to a degree of redistribution; in Eastern Europe, Russia included, through state appropriation of the means of production with significant redistribution. Both aimed to provide stability for the longer term, with linear career development, assured progress for dependants and general improvement of living conditions. Tremendous progress was made: universal access to health services, improved housing conditions, access to tertiary education for up to 35-40% of the population … Until the 70s, narratives on both sides of the Iron Curtain were highlighting the post-war leap forward by European societies.

## Neo-liberal policies

By the early 80s, in Western Europe, neo-liberal policies had gained currency among decision-makers and were on their way to comprising a hegemonic narrative. Some social-democrat leaders, converging in social and economic policies with conservatives and liberals, shifted the terrain to cultural values to differentiate themselves. They thereby opened a broad avenue to far-right and other chauvinist movements, whose core focus is identity politics. (Their social and economic stands, beyond the nativism of “national preference” in employment, are deeply neo-liberal: less “state”, less solidarity and less redistribution but lots of high-octane exclusivist rhetoric.) Since this unfortunate shift in social-democrat politics, the far right and the populists have been on a rising curve and have made electoral gains.

Identity politics, which zoomed in on migration and, as a corollary, on the ethno-cultural and religious aspects of identities, meshed very well with neo-liberal ideology. Counter to the development of mankind over recent millennia, this actively promotes insecurity as a way of life. As a former chair of the French business association MEDEF put it, if life and love are precarious, why should it be otherwise in employment? She was echoing in euphemistic fashion the extreme Thatcherite assault in the UK on trade unions, which would knock down workers’ solidarity in preserving the social acquis for decades to follow.

After 30 years of such politics, with various levels of violence and ensuing popular demobilisation, the insecurity of most Europeans West and East after the fall of the Wall has soared to alarming levels which have severely affected public well-being. Yet the mainstream discourse on security does not address the primary economic, social and existential insecurity generated by neo-liberal policies: the dismantling of states’ obligations with regard to welfare and in sustaining demand, the weakening of workers’ status amid a race to the bottom within EU states and social dumping between them, extensive white collar fraud and tax evasion—estimated at two trillion euro a year in the EU—and so on. All this against the background noise of the incapacity of political decision-makers, faced with ‘the markets’, to bring any progressive paradigm to bear on the deteriorating reality Europeans experience. One in four is sunk in poverty, while the next quartile just breathes with its nose above the waterline, fingers crossed that nothing bad happens before the end of the month.

## Unequal protection

The insecurity about which we are constantly informed is rather linked to living conditions in multi-ethnic, multi-cultural neighbourhoods (subtext: “there is a white flight from this area”, “these people don’t want to integrate and live in their ghettoes”), where there is petty street crime (read: by “Roma”, “Arabs”, “Pakistanis” …) and where religious practices are visible in the public space (“Muslims are testing the boundaries of the Republic”). Such narratives about insecurity, or more precisely the feeling of insecurity,[1] address only the purported threats posed by minorities to the well-being of the “historical” majority in any given place.

Among these communities, a feeling of being besieged, without access to protection from the authorities or redress in the face of violence, has been growing steadily over the past decade.

Thus “ghettoes” do not spring from a desire by members of minorities to find themselves together—sometimes at the expense of an increased social control which they had sought to leave behind—but are the result of the failure of the majority to ensure equal protection of minority individuals. When political discourses drive only towards heavier policing, control and securitisation of minorities (for the implicit protection of the majority), they do not in any way protect minorities from violence by members of the majority—one of whose most salient aspects is violence by unaccountable police forces. [2]

Absent from such discourses, including in the mainstream media, is any recognition of the need to protect ethnic-minority individuals from violence in majority neighbourhoods, as a key security concern endangering peaceful coexistence. Such violence is recorded as discrete “racist incidents”—as if the victim were merely unlucky enough to be in the wrong place at the wrong time—rather than perceived as symptomatic of a lack of protection of minorities in the context of specific discriminatory patterns.

A similar logic is at work in “counter-terrorism”: the stress is on the insecurity supposedly generated by Muslim populations towards majorities and their institutions. Little is said and done to protect members of minorities from organised violence themselves. Thus in the National Socialist Underground case in Germany obsession with the securitisation of Muslim communities diverted resources within the police, the Office for the Protection of the Constitution and the judiciary from monitoring and controlling extreme-right groups and the threat they represent to ethnic and religious minorities right across Europe—in particular Roma, Muslim and Jewish communities. Since “9/11” such groups have been implicitly considered a low-security threat for the white majority, while the risk they constitute to migrants and other minority members has been completely overlooked.

Among these communities, a feeling of being besieged, without access to protection from the authorities or redress in the face of violence, has been growing steadily over the past decade. In many Eastern countries, the frequent failure of the courts to take into account the racist motivation of crimes committed against Roma has reinforced this sense of insecurity and lack of support from the state—especially when the authorities have been keen to prosecute criminal acts or misdemeanours committed by Roma themselves.

## Collective well-being

The “race” factor plays at more than one level in narratives of insecurity. It provides useful diversion from the purposefully organised insecurity deployed to put pressure on workforces and avoid claims for stronger redistribution. And it legitimises systematic discrimination in security policies targeting specific minority groups while failing to protect minorities from majority violence. Racism and related discrimination will only be dealt with consistently if they are inserted in the broader social and economic conversation, applying the right policy levers to decrease their impact.

The bulk of responsibility ultimately lies with the majority when it comes to bringing change which will protect minorities. Instead of blaming minorities for their lack of integration, legitimising increased securitisation, the EU and the member states should turn the tables, recognising—including in terms of cost-effectiveness—that it would be much better to protect equally members of minorities and majorities, to play down tensions in society and move towards inclusion of all. It is about equality, solidarity and, ultimately, our collective well-being.

**Notes**

[1] Some interesting studies have been conducted which put the “feeling of insecurity” into perspective, being much higher than the actual insecurity as revealed by police reports of the incidence of crime and studies of victimisation (see, for example, research by the King Baudouin Foundation in Belgium: http://www.kbs-frb.be/publication.aspx?id=294891&langtype=2060).

[2] See among others the Open Society report on ethnic profiling in Europe (www.opensocietyfoundations.org/reports/ethnic-profiling-european-union-pervasive-ineffective-and-discriminatory), the work of Stopwatch (www.stop-watch.org/) and the observatory of police violence in Belgium (www.obspol.be/).

***Michaël Privot*** *is the director of the European Network Against Racism.*

|  |
| --- |
| EDITOR’S COMMENT: **Racism** is actions, practices or beliefs, or social or political systems that consider different races to be ranked as inherently superior or inferior to each other, based on presumed shared inheritable traits, abilities, or qualities. It may also hold that members of different races should be treated differently. While most conceptualizations of racism include the notion of "race based discrimination", the exact definition is controversial both because there is little scholarly agreement about the meaning of the concept "race", and because there is also little agreement about what does and does not constitute discrimination. **Nationalism** is a belief, creed or political ideology that involves an individual identifying with, or becoming attached to, one's nation. Nationalism involves national identity, by contrast with the related construct of patriotism, which involves the social conditioning and personal behaviors that support a state's decisions and actions. From a psychological perspective, nationalism (national attachment) is distinct from other types of attachment, for example, attachment to a religion or a romantic partner. The desire for interpersonal attachment, or the need to belong, is one of the most fundamental human motivations. Like any attachment, nationalism can become dysfunctional if excessively applied. Apart from the above broad definitions indicating that there is no universal agreement on the exact nature of both, **there is the reality** we face in Europe – in Greece in particular. As the gate of EU, Greece is “hosting” millions of immigrants that enter the country illegally. These people came from different cultures, conflict zones and less developed countries bearing with them their way of life. So far the majority did no show signs of integration and the state does not have the means to offer the necessary umbrella leading to that. Mostly uneducated with no special skills other than their hands and physical they try to survive and gain their daily bread by employing legal and in most of the times illegal means. Existing condition is reaching a critical point and this gives the opportunity to equally “uneducated” locals to raise issues of both racism and nationalism the moment that truth is quite different. When locals and foreigners come to the point to compete for the same loaf of bread then the consequences are predictable. International community and related bodies are taking sides only when the phenomenon affects specific countries or interests. And then there is another issue: are these incoming communities willing to adapt to existing national standards? Or unconsciously desire to implement their way of life on hosting countries? There is strong evidence that this is the case. And this is something that we are not willing to accept! Nobody wants to see other people starving, lacking water, food, healthcare and education. No body wants wars and massacres near or far away from homeland. We all desire peace and a prosperous life. But those mastering global geostrategic chess seem to have different approaches on peace and prosperity. And this is the problem for the generations to follow. Articles like the above just raise questions without providing solutions. Anybody can do that! But real life is more than a “job” or an “organization”. And life demands lessons to be learned; not to be just identified… |

# http://r67.cooltext.com/rendered/cooltext1333425072.pngSmiths Detection to Supply U.S. Customs and Border Protection Miniaturized Chemical Identification Technology

Source: http://online.wsj.com/article/PR-CO-20140224-908313.html

Smiths Detection has been contracted by U.S. Customs and Border Protection to supply it miniaturized technology for fast and comprehensive in-field analysis of unknown suspicious substances at borders and points of entry.

A leader in ruggedizing and downsizing laboratory technology, Smiths Detection makes a range of portable and handheld systems used to identify suspected illegal or threat materials including narcotics, explosives, Weapons of Mass Destruction (WMDs) and Toxic Industrial Chemicals (TICs).

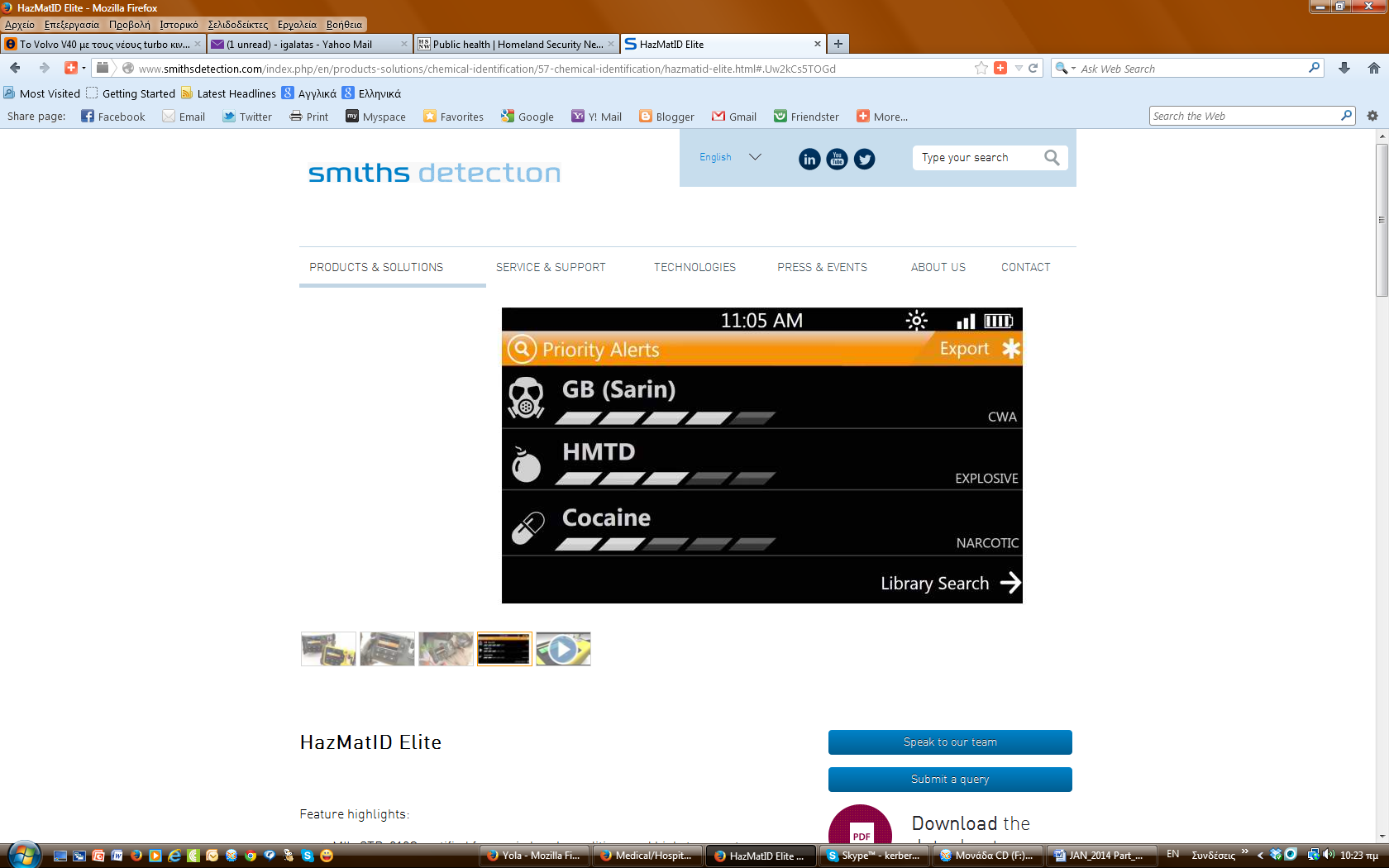
Latest product introductions have included HazMatID Elite, a Fourier-Transform Infrared Spectrometer (FT-IR) which identifies material based on its light absorption, and ACE-ID, a Raman chemical identifier that uses a laser to identify solids and liquids through certain plastics and glass.

Bob Bohn, Vice President, U.S. Sales, Smiths Detection, said: "Smiths Detection combines cutting-edge technology in an easy-to-handle package for use in the field and in challenging environments. Our technology allows government agencies like the Customs and Border Protection to make fast decisions helping to reduce exposure, time and costs when dealing with a suspected threat or illegal substances."

**HazMatID Elite**

Feature highlights:

* MIL-STD-810G certified for use in harsh conditions and high-temperatures
* Integrated pressure device for analysis of solid materials, plus direct touch-to-sample capability
* Automated analysis of mixtures with priority alerting for explosives, CWA, TIC and narcotics
* Long-range, embedded RF wireless transmission

HazMatID Elite is a next-generation handheld unknown solid and liquid chemical identifier that performs an analysis in 1 minute or less.

Analysis is performed by placing a small amount of unknown substance onto the diamond ATR sensor and applying pressure with an integrated press for solid samples. The sample interface also includes an integrated well for the containment of liquid samples. A second, touch-to-sample, diamond ATR interface is available for rapid analysis of pooled liquids and surface films, and enables robotics applications.

HazMatID Elite has the widest thermal and solar operational range of any portable chemical identifier. Its revolutionary optical engine also provides high vibration immunity and resistance to mechanical disturbances seen during vehicle or human transport.

The HazMatID Elite user interface contains a large display screen and keypad controls for effective operation in protective gear and intuitive software.

PC-based command software provides advanced data handling capabilities for specialized users.

# question.pngNational Security Policy draft: ‘Use of chemical, biological weapons cannot be ruled out’

Source: http://tribune.com.pk/story/676210/national-security-policy-draft-use-of-chemical-biological-weapons-cannot-be-ruled-out/

**ISLAMABAD – The use of chemical and biological weapons by non-state armed groups and terrorists cannot be ruled out, read the draft of the National Security Policy presented in the federal cabinet on Tuesday.**

However, the policy draft claims that the capacity of the Ministry of Defence has been enhanced and now it is in a position to cope with non-state armed groups and terrorists.

**The draft mentions that terrorism has inflicted a loss of $78 billion to Pakistan in the last ten years.**

Terming extremism, terrorism and sectarianism threats to internal security, it calls for curbing the misuse of social media, electronic and print media.

Surveillance will be increased to improve the security. The Directorate of Internal Security will be set up under NACTA to effectively use the collected data to stop terrorist activities. After the classified information is received and analysed at this directorate, orders will be issued to the rapid action force.

According to the policy draft, no organisation alone can cope with the challenge; the provinces also need to set up counter-terrorism departments.

NACTA will take measures to push miscreants to surrender before the law-enforcement agencies.

**The draft suggests that religious seminaries will be brought into the mainstream and their curricula and syllabi will be adjusted to contemporary requirements.** Meanwhile, the financial accounts of the madrassahs will be audited so that the aid coming from abroad can be monitored. **The present laws will be revised and a campaign against the ideology of terrorists will be launched.**

# Egypt's 'AIDS Curing Device' May Be A Fake Bomb Detector

Source: http://mashable.com/2014/02/26/egypts-miracle-hiv-device/

This image made from undated video broadcast on Egyptian State Television on Feb. 25, shows a device that the Egyptian army claims will detect and cure AIDS and Hepatitis.

Image: AP Photo via AP video

On Saturday, the Egyptian army unveiled a "miraculous" device it claims will detect and cure AIDS and Hepatitis. But the device, named C-Fast, looks eerily similar to a fake bomb detector sold by a British company to Iraq in the late 2000s.

**That device, codenamed ADE 651, was later found to be a scam. One that reportedly cost the Iraqi government as much as $85 million dollars, and perhaps hundreds of lives. Its creator, James McCormick, was indicted and later sentenced to 10 years in prison.**

The possible link between the C-Fast and the fake bomb detector, named ADE 651, was first spotted by the Libyan Youth Movement, a citizen organization born after the Egyptian revolution of 2011. The group posted a picture of the two devices on Twitter.

**Dan Kaszeta, a former officer in the U.S. Army Chemical Corps, and now a counter-terrorism consultant, said he believes the C-Fast is the same device, and expressed doubts as to its efficacy.** Scientists have also met the Egyptian army's claims with skepticism.

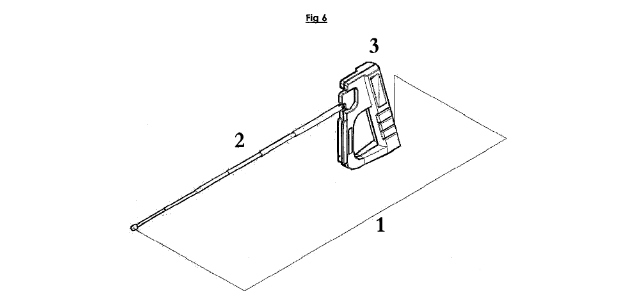
"The scientific claims behind this are completely sh\*t," he told Mashable. "The idea that somehow a virus has an electronic emanation that a device with no internal working parts and no power source can somehow pick up, it's patently ridiculous."

Both the C-Fast and the fake bomb detector sold to Iraq seem to be descendants of the infamous "Quadro Tracker," which was nothing more than a non-functional piece of plastic with a rotating antenna — basically a dowsing rod.

Between 1993 and 1996, the South Carolina Company Quadro Corp. sold the Quadro Tracker device to police departments and schools districts, claiming it could detect hidden drugs, explosives, weapons, and even lost golf balls. In 1996, however, the FBI found it to be a fraud and banned the sale of the device.

"The only thing this accurately detects is your checkbook," FBI agent Ronald W. Kelly said at the time, according to The New York Times.

Another similar explosive detector device called Sniffex was marketed in the mid 2000s. Unsurprisingly, the Navy later proved it was a scam.



A diagram of the C-Fast, taken from an alleged patent application for the device.

This is not the first time the C-Fast has gotten media attention though. The device has been already in use in Egypt since at least early 2013, according to The Guardian, which reported last year about a device that the Egyptian army claimed could cure Hepatitis C. The device was adapted from a bomb detector by Brigadier Ahmed Amien, an "engineer and bomb detection expert," according to British paper.

There's even a patent application, first reported by the BBC, that lists Amien as the alleged inventor of the C-Fast.

It's unclear whether the C-Fast is a copy of the ADE 651 or simply a repurposed bomb detector, though Kaszeta said the Egyptian government did buy these devices in the past. Moreover, as Kaszeta pointed out to us, the device can still be easily found for sale online: one listing sells it for $6,000.

# The CBRN Defense Market 2013-2023

Source: http://www.sacbee.com/2014/02/26/6191589/the-cbrn-defense-market-2013-2023.html

Reportbuyer.com just published a new market research report:

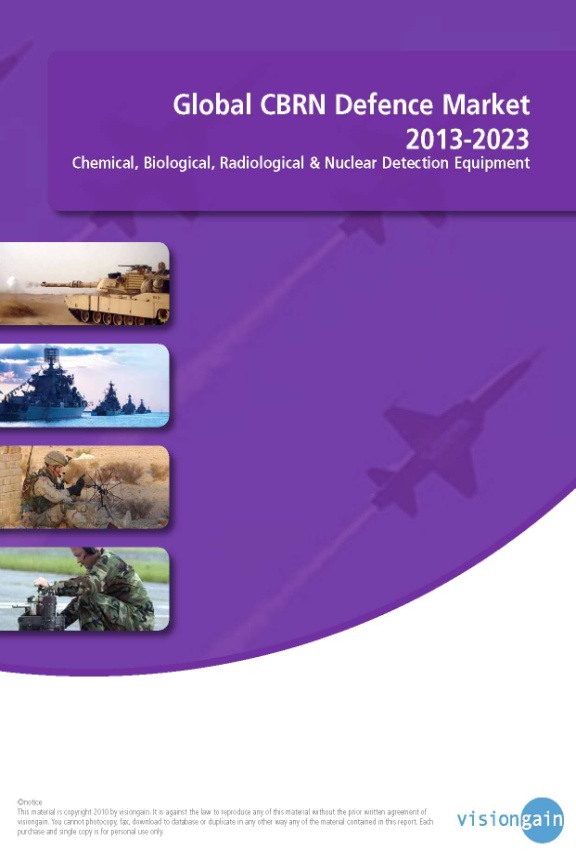
**Synopsis**

This report is the result of SDI's extensive market and company research covering the global CBRN defense industry. It provides detailed analysis of both historic and forecast global industry values, factors influencing demand, the challenges faced by industry participants, analysis of the leading companies in the industry, and key news.

**Summary**

Why was the report written? "The Global CBRN Defense Market 2013–2023" offers the reader detailed analysis of the global CBRN defense market over the next ten years, alongside potential market opportunities to enter the industry, using detailed market size forecasts.

**What are the key drivers behind recent market changes?**

The global CBRN defense market is estimated to value US$9 billion in 2013. The market consists of CBRN protection, detection, decontamination, disposal, and simulation equipment, and is expected to witness a marginal increase during the forecast period, primarily due to modernization initiatives planned in North America and Europe, and threats from terrorism and hostile neighboring countries in the Asia Pacific and Middle Eastern regions. The market is expected to increase at a CAGR of 4.2% during the forecast period, to reach US$13.7 billion by 2023. CBRN protection equipment is expected to account for the majority of the global CBRN defense market, followed by detection and decontamination systems.

**What makes this report unique and essential to read?**

"The Global CBRN Defense Market 2013–2023" provides detailed analysis of the current industry size and growth expectations from 2013 to 2023, including highlights of key growth stimulators. It also benchmarks the industry against key global markets and provides detailed understanding of emerging opportunities in specific areas.

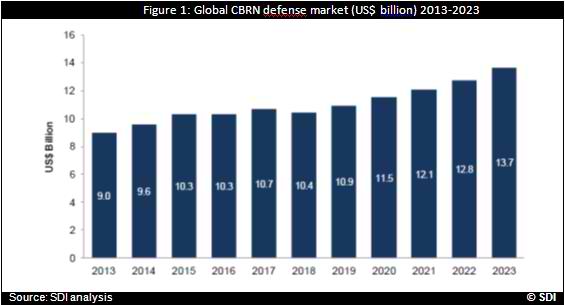
**Scope**

The report provides detailed analysis of the market for CBRN defense equipment during 2013–2023, including the factors that influence why countries are investing or cutting defense expenditure. It provides detailed expectations of growth rates and projected total expenditure.

Despite a number of developed countries, mostly in Europe, having called for a complete shutdown of nuclear reactors in all countries around the world, global nuclear energy generation is expected to increase significantly over the forecast period. Rapidly increasing demand for electricity, along with increasing fossil fuel prices, are making nuclear power an increasingly attractive option for many countries, especially in those where large-scale alternative energy generation such as wind and solar are not feasible. It has also been reported that over 60 power reactors are currently being constructed in 13 countries including Turkey, Taiwan, China, South Korea, Poland, Bangladesh, Russia, the UAE, and India. All of these countries will have to spend on CBRN incident protection in order to ensure that tragedies such as the Fukushima spillover are avoided.

**Reasons to buy**

One of the key issues facing the industry is to develop technically advanced and cost effective prototypes that can be transferred to mass production without much difficulty. The major impact is currently felt in developing advanced protective suits that need to counter changing threats while at the same time being light so as to minimize the physical load on the wearer. Specifically, companies are trying to address the heat load stress issue by aiming for a balance between a generic outfit and a highly technological garment. These innovations require significant funding and with the global economy just emerging from the economic crisis and defense budgets being cut, companies are hard pressed to get the required funding.

Since the CBRN protection industry is currently in its nascent stage, it requires considerable funding from the public and private sectors to develop effective counter measures against potential threats. However, recent years have witnessed various instances of neglect towards the CBRN sector; cancelled programs, cutbacks in research funding, and a focus on other defense sectors threaten to plague the industry. In 2004, the US Congress passed the Project BioShield Act in a bit to get the private sector to develop medical countermeasures against CBRN terrorism agents and to provide a mechanism for the government to acquire these countermeasures.

**Key Highlights**

One of the main factors resulting in continuous demand for CBRN protection, detection, and decontamination equipment is the dual use of these agents in everyday life. The advancement in the fields of biotechnology, nuclear energy, and life sciences has the potential to bring about significant benefits for the betterment of mankind; however, these developments can also be used for hostile purposes and to perpetrate various instances of bio-terrorism, which is why it is imperative for scientists and the security community to constantly engage with each other and devise methods to prevent or counter any forms of CBRN terrorism.

Budget cuts are expected to prompt DoDs to provide war fighters and first responders with products already on the market or about to hit the market. These budget constraints are also expected to encourage the modification and refit of existing technologies and equipment in order to enhance the capabilities of CBRN defense forces while maintaining low budgets. As has been seen in the case of the US, the UK, and Japan, budget constraints have urged procurement departments to opt for dual use COTS products, which enables defense departments to save costs while at the same time provides CBRN defense personnel with equipment that offers a range of flexibility to meet multiple scenarios and requirements.

►At the source’s URL you can read the **contents** of the report.

# NBC-Protective Suit 'ABC-92' with Air Distribution System

Source: http://www.army-technology.com/downloads/whitepapers/personal/nbc-protective-suit/?WT.mc \_id=WN\_WP

The 'ABC-92' (Blaschke J Wehrtechnik) is a military one-part NBC-protective suit with air distribution system, manufactured in five sizes. The suits have either a fix mounted mask at your decision or a smooth rubber sealing frame, and either fix mounted NBC-boots or fix mounted socks with a cuff, to use with any boots. The suit is closed by a gas-tight zipper from the right knee to the left shoulder of the suit.

The suit eases the strain on human heat regulation during heavy work or high ambient temperature by means of a fresh-air distribution system. Uniform air-distribution is regulated by eight outlet valves protected against fouling. This fix mounted air-distribution system brings fresh and dry air to any area of the body and is supplied by a fresh-air blower with an output of up to 250l/min.

|  |  |
| --- | --- |
|  |  |
| In a gastight suit at high ambient temperature normally the temperature rise up to 60 - 70°C within a short time. So the working time sometime is less than 30 minutes at aggravating circumstances.  With the fresh air blower and the special air distributing system the working time at the same conditions is **up to 4 hours 2 times a day with a rest of 2 hours.** The special hoses bring the fresh air to a big area of the body surface, never blowing direct to the skin 🡺 no cold areas. | |

## Libyan Islamists tried to ship mustard gas to Syrian rebels

Source: http://www.homelandsecuritynewswire.com/dr20140305-libyan-islamists-tried-to-ship-mustard-gas-to-syrian-rebels

In early March 2011 Israeli commandos killed two Hamas operatives near the city of Port Sudan in Sudan. These operatives were on their way back from Libya after negotiating a deal with anti-Qaddafi rebel leaders to sell Hamas and Hezbollah chemical warheads from Qaddafi’s arsenal. Iran was paying for the chemical weapons to be delivered to the two organizations. The deal involved 600-700 artillery shells filled with nerve and mustard gas which the rebels found in abandoned Libyan military bases in eastern Libya.

The Israeli attack – and two subsequent strikes in Sudan – put an end to this particular venture, but not to efforts by Islamic Libyan anti-Qaddafi rebels to help fellow Islamists.

Times have changed, though. In 2011, Iran supported both the coreligionist Shi’a militants of Hezbollah and the Sunni fundamentalist Hamas militants (Hamas HQ at the time was in Damascus).

Now, with the Arab world divided along Sunni-Shi’a lines, the Sunni Islamists in Libya support the Sunni rebels in Syria against the Alawite Assad regime, a regime dependent on the staunch support of its two closest allies, and the region’s two Shi’a powers, Iran and Hezbollah (the Alawaites a follow a branch of the Twelver school of Shia Islam).

In late 2011, Sunni Hamas moved its headquarters from Damascus to Qatar.

**Libyan officials report that they have recently apprehended several members of a Libyan Muslim extremist militia planning to ship chemical weapons to anti-Assad rebels in Syria.**

**Arutz Sheva reports that an Israeli Channel 2 TV quoted Colonel Mansour al-Mazini of the Libya army to say that the Islamists had been caught with a container of mustard gas. The gas was confiscated by Libyan soldiers.**

The New York Times reports that Libya, with international assistance, finished destroying its mustard agent stockpile in January, but hundreds of tons of chemical-arms ingredients are still awaiting destruction in the country.

Since the killing of Col. Qaddafi in November 2011, Libya has not had a functioning government structure. The army, police, and security services have disbanded. Different parts of the country are ruled by different militias who are fighting each other over territory and the control of oil resources.

Western intelligence services say that dozens of Libyan veterans of the fight against Qaddafi are now in Syria fighting Assad.

|  |
| --- |
| The disposal of the last of Libya’s chemical weapons closes a chapter that Colonel Qaddafi began in early 2004, when his government turned over a vast cache of nuclear technology and chemical stockpiles to the United States, Britain and international nuclear inspectors.  At that time, Libya declared for destruction 24.7 metric tons of sulfur mustard, a syrupy liquid that when loaded into bombs or artillery shells and exploded creates a toxic mist that penetrates clothing, burns and blisters exposed skin, and can kill with large doses or if left untreated. The chemical was used extensively in World War I.  http://m.ruvr.ru/2014/02/04/09/ergerge.pngMap showing former Libyan Nuclear, Biological and Chemical (NBC) facilitiesLibya had destroyed about half of these stocks when civil war broke out in 2011. Ruwagha chemical weapons storage site at Libya's Al Jufrah Air Base, some 800 km southeast of Rabta.  Western spy agencies closely monitored the destruction site in the Libyan desert to ensure the stockpiles were not pilfered by insurgents.  When the new government took control in Tripoli that fall, it signaled its intent to finish the job. Libyan officials also surprised Western inspectors by announcing the discovery in November 2011 and **February 2012 of two hidden caches of mustard**, or nearly two tons, that had not been declared by Colonel Qaddafi’s government. That brought the total declared amount of chemical to **26.3 tons.**  **Unlike the majority of Libya’s mustard agents**, which were stored in large, bulky containers, the new caches were already armed and loaded into 517 artillery shells, 45 plastic sleeves for rocket launchings and eight 500-pound bombs. |

# Israel’s New HAZMAT Training Facility

Source: http://i-hls.com/2014/03/israels-new-hazmat-training-facility/

The first class of students, including fire fighters, IDF soldiers and police officers, graduated from the Israeli Fire Fighting and Rescue Authority’s new **Hazardous Materials School**.

The new 2013 emergency response laws gave the authority responsibility over several new areas, once of them is HAZMAT training. **The purpose of the new facility, the only one of its kind in Israel, is to offer hazardous materials training to fire fighters, police, army soldiers and others.**

[](http://i-hls.com/wp-content/uploads/2014/03/18799506_m-feature.jpg)According to Fire Fighting and Rescue Authority representatives “Thousands of materials are officially recognized worldwide as hazardous. Hundreds are included in the Israeli list, and incidents involving hazardous materials are common. Gas leaks in gas stations, for examples, are defined as HAZMAT incidents, and so are cooking gas leaks, cooking gas container explosions, traffic accidents involving chemical tankers, clouds of dangerous materials over populated areas, incidents on trains and in naval ports, several pesticides in agriculture, events involving explosives and ammunition in the army – all these and more are defined as HAZMAT incidents.”

Training facility personnel explained that the authority is now responsible – by law – for knowledge involving these incidents. Students come from various emergency organizations and include paramedics, the IDF, the police, Home Front Command and HAZMAT officers in various organizations. The training programs are adapted to suit the needs of specific clients.

The recent class included 18 students from the fire fighting authority, the IDF and the Israeli Police. **25 courses are planned for 2014, offering training for around 750 cadets from various Israeli emergency response organizations.**

|  |
| --- |
| HAZMAT Highway to Hell Source: http://www.youtube.com/watch?v=FG1LGKieTxY  Ever wonder what might happen if one of those trucks carrying a load of gas cylinders is involved in an accident?  Watch the video (**at source’s URL)** and you will see what the worst case possibility is.  **Note the behaviors of the people watching this event unfold and note that many (including the police responders) don't sense the dangers of what they are observing.**  While this accident happened in Russia, it could happen anywhere in the world! |

# Syria to miss deadline to destroy 12 chemical arms sites-sources at OPCW

Source: http://www.reuters.com/article/2014/03/06/us-syria-crisis-chemical-idUSBREA2526G20140306

March 6 – **Syria will miss a major deadline next week in the program to destroy its chemical weapons production facilities,** sources at the Organisation for the Prohibition of Chemical Weapons said on Thursday.

**Syria declared 12 production facilities to the OPCW and has until March 15 to destroy them** under a deal agreed with the United States and Russia. Damascus has already missed several deadlines laid out in the agreement.

"That will definitely be missed," said an official involved in discussions with Syria, referring to the March 15 deadline.

The official, who asked not to be identified, said there were seven "hardened" aircraft hangars and five underground facilities. "None of them have been destroyed at the moment," the official said.

Syrian officials could not immediately be reached for comment.

Damascus agreed last year to destroy all chemical weapons facilities and surrender 1,300 metric tons of toxic agents to a joint OPCW/United Nations mission. It has until June 30 to eliminate its chemical weapons program completely.

The deal averted U.S. missile strikes threatened by Washington after an August 21 sarin gas attack killed hundreds of people in the outskirts of the capital.

**Syria missed a February 5 deadline** to ship all chemicals abroad for destruction and is weeks behind schedule. It has increased the handover of poisonous agents, including a shipment of mustard gas this week, but will not meet a March 30 deadline to neutralize all the chemicals overseas, sources at OPCW said.

That process was already supposed to have started on board the U.S. MV Cape Ray, a cargo ship outfitted with special chemical neutralization equipment. **But only a quarter of the so-called priority 1 chemicals, the most dangerous ingredients for chemical weapons, have been relinquished,** officials said.

**Deadlines ingonred**

**Syria is not taking the deadline for the destruction of production facilities seriously**, another source at the OPCW said on Thursday.

"They are not doing things in the timeframe they promised they would," the source said. "The process is in volatile waters."

The latest comments in The Hague, where members of the OPCW are meeting until Friday, came after sharp criticism of the government of Syrian President Bashar al-Assad on Wednesday by the U.S. ambassador to the United Nations, Samantha Powers.

A Syrian request to convert for peaceful use some of the facilities declared under its weapons program has already been rejected, because Western governments fear they could easily be re-converted for military use.

**Damascus proposed "sealing" the sites with cement,** the sources said, but that idea was dismissed by several Western diplomats at an OPCW executive council meeting this week.

"Destroyed means destroyed," the second source said. "Why should a country that used chemical weapons against its own people be given special privileges?"

Syria has missed almost every deadline of the agreement reached last year, which is being jointly overseen by the Nobel Peace Prize-winning OPCW and the United Nations. The OPCW said Syria will have shipped out roughly one third of its chemical weapons by the end of this week.

"You can say they have upped the momentum and shipped out nearly a third, or you can say they haven't given up two-thirds of the stuff they should already have sent out of the country," one OPCW source said.

**Missing the June 30 deadline would have serious political implications, with Washington and Moscow having both invested diplomatic credibility in the chemical weapons elimination process**, brokered by U.S. Secretary of State John Kerry and his Russian counterpart Sergei Lavrov.

The international community is footing the bill for the complex operation involving ships from the United States, Norway and Denmark, Chinese and Russian security, an Italian port and commercial destruction facilities in Britain and Germany.

|  |
| --- |
| EDITOR’S COMMENT: It seems that Assad is proved to be a better chess player than his competitors. Basically because he inherently knows that without his CWAs his future moves will lead to loose the queen. For the time being he is sacrificing “*soldiers*” – slowly! |

## Determining long-term effects of West Virginia chemical spill

Source: http://www.homelandsecuritynewswire.com/dr20140311-determining-longterm-effects-of-west-virginia-chemical-spill

**A chemical mixture called crude 4-methylcyclohexane methanol (MCHM) is used during the separation and cleaning of coal products. More than 10,000 gallons of the chemical leaked from a storage tank near Charleston, West Virginia, and entered the river upstream of a water-treatment plant on 9 January. The drinking water of more than 300,000 West Virginians was contaminated. Water restrictions began to be lifted on 13 January, but residents are still detecting the telltale odors of MCHM.** Virginia Tech faculty engineers and students are unravelling fundamental chemical and health properties of MCHM.

Fueled by a $50,000 National Science Foundation Rapid Response Research grant, the team seeks to understand the properties of a chemical mixture called crude 4-methylcyclohexane methanol (MCHM), according to study leader Andrea Dietrich, a professor of civil and environmental engineering.

The research team, which includes associate professor Daniel Gallagher, assistant professor Robert Scardina, and senior analytical chemist Jody Smiley of the Department of Civil and Environmental Engineering, is determining the long-term fate of the chemicals in the drinking water distribution system and the environment.

“Residents were alerted by a strong licorice odor that led many people to think at first that the air was polluted,” Dietrich said. “In that respect, consumers are important sentinels for exposure to low levels of MCHM. As is typical of chemicals that were grandfathered under the Toxic Substances Control Act, not a lot of data exists about the product.”

Dietrich said many knowledge gaps exist about the short- and long-term fate of the chemical in water systems. The research will provide fundamental chemical properties that can be used to estimate human exposure through drinking water and indoor air pollution.

Other parameters will evaluate if MCHM interacts with plastic pipe and epoxy liners in water tanks. This research will help determine long-term remediation measures for the water distribution system.

**The release notes that graduate students in Dietrich’s Civil and Environmental Engineering Techniques for Environmental Analysis class jumped into the lab to develop analytical chemical techniques that isolated the six major components in the crude mixture and identified their chemical structures.**

**After identifying the chemicals, they scoured government and industrial databases and realized how little is known about the properties of the compounds. This forced them to master modeling techniques to estimate toxicity and interaction with drinking water pipes and plumbing.**

“We capitalize on opportunities to engage engineering students in real-world situations that allow them to make important civic contributions and expand their knowledge,” Dietrich said.

“We will share what we learn with the scientific and engineering communities for future planning, and with citizens who want to understand more about the effect of this chemical on the water supply.”

“**This is one of the largest human-made environmental disasters in this century.** In instances such as this, where the situation is still developing and public health is involved, timing is everything,” said William Cooper, a program director in NSF’s division of Chemical, Bioengineering, Environmental and Transport Systems, in a news release that announced the awards. “RAPID grants give researchers the support they need to be on the ground and to collect data immediately.”

**RAPID awards have been given before in similar circumstances, such as the 2010 Gulf of Mexico oil spill and the 2004 Indian Ocean tsunami.**

# The Russian CBRNe Threat

**By Ilja Bonsen**

Source: http://www.cbrneportal.com/the-russian-cbrne-threat/

After the Russian occupation of Crimea, questions have been raised about means Russia will likely deploy to reinforce its foreign policy objectives. Further escalation in Eastern Ukraine may very well lead to a situation where both parties deploy “all necessary means”. This special issue of the NCT/CBNW Newsletter addresses the issue of Russian CBRN capabilities and what defenses the West has against such a threat. Dave Sloggett addresses the Russian capabilities, with a focus on the “known-unknowns” of the secret Russian Chemical Weapon Programs. Over the years, defectors and whistleblowers have shed some light on these programs, but hard evidence of the existence and exact contents of these programs are limited. One of the few instances when we could see evidence of such a Russian weapon program is the Moscow Theatre Siege in 2002 which is covered by Patrick Kozakiewicz’ article.

The Western side of the equation is briefly covered in this article. Although a proper examination of Western preparedness for a CBRN scenario would be useful, we have asked European industry and researchers for their opinion on the preparedness of NATO and the EU.

# CBRN Countermeasures

Is the west prepared for the worst? Of course, this question rises more than a few eyebrows. **A Russian CBRN attack is largely considered highly unlikely.** “Why and for what reason would Russia do that within the current geo-political situation?” is the answer relayed by many CBRN experts. In any case, NATO and the EU have sufficient countermeasures to counter CBRN attacks on the military side in an operational environment. Many companies offer equipment that provides perfect protection against all classical Chemical and Biological warfare agents. **However, some concerns are raised about the unprotected civilian population during CBRN attacks.**

According to Dr Nobert Kloepper from Bruker Daltonics, the West is sufficiently prepared against a CBRN attack from Russia. From the “Cold War scenarios” to more recent investment in civil and industrial emergency preparedness, the West has built up sufficient capability to encounter the average threat Russia can pose. He emphasize on the fact that already more than 80% of Russia’s chemical weapons stockpile has been destroyed under the auspices of the OPCW. With the remaining arsenal, Russia can only cause “terrorist turmoil” for which the West is prepared.

However, not everyone is that optimistic about Western CBRN preparedness. **A senior spokesperson from one of the western defense research institutes, who insisted on anonymity, stated that: “NATO is not prepared at all. Although, the official answer is of course that NATO is sufficiently prepared.”**

# Novichoks

A specific concern has to do with the Novichoks; these are agents that were designed by the Russians with the specific goal to be undetectable using standard NATO chemical detection equipment; and to defeat NATO chemical protective gear, whilst being safer to handle. **Although, it was claimed that these criteria were met, this has not been proven to date.** In addition, it’s widely believed that the Russians halted these research activities before the end of the Cold War. However, the spokesperson stated that: “**to date there are clear signs that Russia is still developing new chemical and biological agents**.”

Others argue that the threat of Novichoks is to be neglected. According to Norbert Kloepper, Novichoks, should not be considered as that novel. At least for all agents that are known to the West, there is detection equipment available.

# NATO Standards

Although the threat allegedly stemming from Russian R&D is debatable, Bruno David from NBC Sys raises another issue in connection with Novichoks. If these agents are really undetectable using standard NATO chemical detection equipment, one should ask the questions if these standards, implemented to guarantee a certain level of protection, now actually serve as a limitation. Industry does not take the lead in developing equipment that offers more than is required at an international level and industry will not facilitate in the protection against speculative threats. NATO sets the standard and it’s only when the standards prove to be insufficient to protect against a realistic threat level that the latter should be changed and in turn the industry can develop new solutions.

This raises further questions about the ability of standards to safeguard against current potential threats. Indeed, while standards have had and have their purpose, they should not be carved in stone and evolve according to the changing threat spectrum. Consequently, both the EU and NATO should put much emphasis on adapting standards to ongoing and future potential threats. By providing up to date equipment and training requirements, evolving standards would hence enable to adapt to current threats and provide increased levels of security and preparedness. For example, by constantly updating agents’ lists and thresholds, NATO and EU members could procure relevant detection and decontamination equipment enabling them to be better prepared against current potential CBRN attacks.

# Civil Defense

When it comes to civil defense, the EU seems to be divided. Some of the larger countries, like France and Germany, have built up a significant civil defense capability against CBRNe threats. However, that is not always the case for smaller countries in the EU. Spending budget on a “one-in-a-trillion” threat is difficult to justify in times of austerity. While the EU CBRN Action Plan has enabled to strengthen CBRNe preparedness and response in the EU, many concrete measures have yet to be taken. Indeed, in its last CBRN report, the European Parliament emphasizes on the necessity to further implement the various CBRN actions in order to meet the objectives spelled out in the EU’s CBRN Action Plan.  
CBRN is one of those examples where it is difficult for individual EU Member States, especially small ones, to justify building a full capacity, but where the EU would be able to build such a shared capacity against lower costs per capita. Much as deeper EU integration in field of CBRN preparedness and response would increase EU Member States CBRN security as a whole at a marginally low cost, these same Member States remain reluctant to let go of matters that have to do with their own national security. In so doing, overall CBRN preparedness and response is not cost effective and EU citizens’ security varies tremendously from one member to the next.

# Enhancing CBRN Preparedness

In general, it seems that the west does have sufficient military countermeasures in place in case of a CBRN attack from Russia. The real problem lies with Russia’s unpredictability with regards to its foreign policies in general and its current and future offensive CBRN capabilities.

According to another industry spokesperson, who also wishes to remain anonymous, western industry has the know-how to develop the right CBRN countermeasures, but as the Russian threat is not clearly defined, there will always be a gap in western CBRN defense. Therefore, in order for the West to be fully prepared, the importance of intelligence gathering should not be underestimated. So long as the exact state-of-the-art the Russian CBRN capabilities remains unknown to the West, it will be impossible to honestly state that the West is prepared against a Russian CBRN threat.

***Ilja M. Bonsen*** *is founder and Managing Director of IB Consultancy, an independent defence and security firm specialising in non-conventional threats.*

|  |
| --- |
| EDITOR’S COMMENT: **European CBRN Civil Defense!** **That was a good one!** Joke I mean! There is confusion between “response” and “preparedness”. Even “big” nations cannot deal with a real CBR incident in urban environment. Even the Israelis stopped their program for distributing gas mass to all their citizens – due to “high” cost they stated! How can populace be protected when citizens are now aware of simple “shelter-at-home” measures? Govs are afraid to speak about it in public due to inherent belief of causing panic and havoc. This “one-in-a trillion” threat would be catastrophic whether it happens in Paris or Athens. The threat is real and those who might advocate it are out there looking for an opportunity. This is the simple truth and the best we can do is to pray that the unexpected will NOT happen this time… |

# thumbs up.jpg.png

# World's First Handheld Mass Spectrometer

Source: http://www.908devices.com/products/



M908™ is specifically engineered for your most time-critical missions. The first and only handheld tool utilizing high-pressure mass spectrometry™ (HPMS), M908 provides civilian, federal and military responders with expanded analysis capabilities for CBRNE identification and detection at the point of action. Weighing just 2.0 kg (4.4lbs), M908 boasts an intuitive interface designed for effortless operation in full protective gear. Alerts are provided within seconds delivering immediate intelligence on high priority threats and rapid clear down between measurements means less down time in the hot zone — getting you in fast, and out faster.

**Expanding Capabilities**

The unique proficiency of handheld high-pressure mass spectrometry™ (HPMS) expands the first responder tool kit adding deep chemical, explosive and precursor material identification and detection capabilities beyond traditional tools. The selectivity of mass spectrometry allows M908 to detect trace quantities of critical threats amongst the myriad of interferents that plague other less selective technologies.

****

**Credible threat recognition without interference**

The selectivity of HPMS coupled with smart on-board analytics allows M908 to focus on detecting and identifying the most critical compounds and extreme hazards in liquid, solid and vapor form without the clutter of low-threat background chemicals and with extremely low false alarm rates.

**Expect the unexpected**

From chemical warfare agents (CWAs), toxic industrial chemicals (TICs), toxic industrial materials (TIMs), and explosives to the use of unconventional agents, today’s first responders must be prepared for the unexpected. An expandable threat list enables M908 to adapt with each mission and serve as a true proactive performance tool in the hot zone.

**Key Highlights**

* High Pressure Mass Spectrometry
* Handheld 2.0kg (4.4lb)
* Multi-phase detector - vapor, liquids, solids
* Trace to bulk detection and identification
* Effortless operation in full PPE
* Extremely low false alarm
* Results in seconds
* 4+ hours of operation on a single replaceable battery
* Expandable threat list
* Designed to meet MIL-STD-810G
* High-speed continuous monitoring
* Steadfast performance
* Low-maintenance

**Technical Data Table**

* Technology High Pressure Mass Spectrometry or HPMS
* Confirmation Capability Full MS/MS
* Size 8.7 x 7.3 x 3in (22 x 18.5 x 7.6cm)
* Display Size Adjustable backlit display for direct sunlight and nighttime conditions, 10.9cm (4.3 inch) Landscape 9.1x5.5cm (3.6x2.2 inches)
* Weight 2.0kg (4.4lbs), including battery
* Mass Spectrometer Microscale Ion Traps
* Mass Range 60-450 Da
* Ionization Source Non-radioactive, internal ionization, variable energy, dual polarity
* Sample Introduction Continuous gas/vapor analysis; rapid trace-to-bulk solid/liquid analysis via thermal desorption swabs
* Software Embedded, self contained, on-board analytics
* Decontamination IP-53 rated, chemical resistant housing spray/splash and wipe down
* Operating Range 32° - 110°F
* Storage Temperature -4° - 140°F

# Almost half of Syria's chemical weapons removed - OPCW

Source: http://www.bbc.com/news/world-middle-east-26662801

Almost half of Syria's declared stockpile of chemical weapons has now been removed, the Organisation for the Prohibition of Chemical Weapons says.

The latest consignment of the most dangerous chemicals was loaded on to cargo vessels at Latakia on Thursday, according to an OPCW statement.

**A total of 11 consignments have been shipped, including all of Syria's sulphur mustard, a blister agent.**

The OPCW aims to destroy or remove the country's entire arsenal by 30 June.

The Syrian government approved the initiative last year after a chemical weapons attack outside Damascus left hundreds of people dead.

**Revised schedule**

The OPCW said three consignments of both "Priority 1" chemicals and less hazardous "Priority 2" chemicals have been shipped from Latakia over the past week.

**The 11 consignments represent 49.3% of all the chemicals that must be removed from Syria for destruction, including 34.8% of Priority 1 chemicals and 82.6% of Priority 2 chemicals.**

The OPCW said all stocks of sulphur mustard had now been removed.

Sulphur mustard is a "unitary" agent that is stored in a form that can be deployed immediately. In contrast, Syria's nerve agent sarin is thought to be stored in a "binary" manner, meaning it is kept as two distinct chemical precursors that are combined just before use.

Although the OPCW-UN Joint Mission said earlier this month that "good progress" is being made in the removal of the chemical stockpile even though the Syrian government has missed a series of deadlines.

The removal of Priority 1 chemicals was initially due by 31 December, while the deadline for the shipment of Priority 2 material was 5 February.

The Syrian government, which says the shipments have been delayed by security and logistical issues, has presented a revised schedule that aims to have them completed by 27 April.

### Dartford company helping fight the battle against terrorism

Source:http://www.newsshopper.co.uk/news/11090693.Dartford\_company\_helping\_fight\_the\_battle\_against\_terrorism/?ref=var\_0

You may be surprised to hear there is a Dartford company helping fight the battle against terrorism by destroying bombs and chemical weapons across the globe. MELISSA HILLS finds out more.

I decided to head down to the Crossways Business Park near Bluewater to find out a little bit more about this unusual company and meet its CEO Dr Wolfgang Gödel .

Dynasafe is an international organisation that specialise in the removal and management of UXO (Unexploded Ordnance), chemical, biological, radiological, nuclear explosives and other hazardous materials on land and under water.

They are employed by governments, the United Nations, oil and mining companies and commercial and energy companies to undertake this important work.

The Dartford headquarters of Dynasafe is where much of the project management and co-ordination for demining and battle area clearance takes place.

I quickly found out that they are one of the world's leading companies 'making the world a safer place' as put by Dr Gödel providing an extensive range of unique services.

Dr Gödel said: "Our main aim is to minimise and eliminate the risk posed by mines and unexploded bombs and ammunitions.

"We have the unique capability of offering a full range of services to a client.

"We provide area clearance by searching areas for land mines and bombs.

"We provide counter terrorism equipment such as blast proof steel chambers for safe handling of terrorist devices or suspicious objects and we also build the plants for the destruction of bombs and ammunition.

**"One of our most recent projects was destroying chemical weapons left behind by Colonel Gaddafi in Libya.**

"Our experts designed a munition disposal plant, which was then delivered at a secret location in the desert. In Libya, our engineers supervised the operation of the plant.

"There are no other companies across the globe which can offer this service.

"We have a complete solution to getting rid of explosive devices.

"We have made about 20 of plants worldwide which are used to safely dispose of these and other weapons."

One of the company’s biggest area clearance projects is currently going on in Mozambique where more than 1000 people are employed.

Dr Gödel added: "We employ local people in the countries we are working. It's important we contribute to the economies of where we are working." Dynasafe is also working in Afghanistan, Iraq, South Sudan and in the Falklands.

Dartford MP Gareth Johnson recently visited the site and said: "This is a fascinating company and something unique that Dartford can be proud of.

"They carry out vitally important work on the world stage.

"I met with their enthusiastic and dedicated staff who told me about their work disarming weapons and diffusing bombs and incendiary devices both here in the UK and worldwide.

"They are also involved with disposing of chemical weapons.

"I am delighted to hear they are involved in such important work.

"The disposal of chemical weapons is imperative to making the world a safer place and it is great news to see a Dartford-based company recognised internationally."

## Debate over inherently safer technology (IST) at chemical plants intensifies

Source: http://www.homelandsecuritynewswire.com/dr20140319-debate-over-inherently-safer-techno logy-ist-at-chemical-plants-intensifies

Recent accidents at chemical facilities around the country have prompt environmental groups and workplace safety advocates to highlight the need for implementing inherently safer technology (IST) at facilities using hazardous chemicals.

**IST is a methodology that encourages substitution or minimization of hazardous materials, and the simplification of complex industrial processes which use hazardous materials.** According to research scientist Anna-Mari Heikkilä, “an inherently safer design is one that avoids hazards instead of controlling them, particularly by reducing the amount of hazardous material and the number of hazardous operations in the plant.”

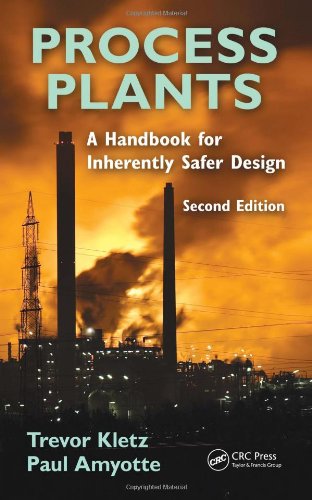
Chemical *&* Engineering News reports that IST proponents are asking regulators to mandate IST implementation, but some industry officials consider IST to be common sense, and say facilities could adopt IST standards as needed without a regulatory mandate.

“What we have now is risk management; what we need is risk prevention,” says Rick Hind, legislative director of the environmental group Greenpeace. “Risk management accepts the risk and simply cleans up the mess afterward. This isn’t acceptable and shouldn’t be acceptable to people who lost family members or their homes” in the recent accidents.”

An April 2013 ammonium nitrate explosion at a West, Texas fertilizer distributor claimed fifteen lives and injured 180 others. Since then, President Barack Obama has assigned a task force to explore ways to make chemical facilities safer and more secure. Led by the EPA, the Occupational Safety & Health Administration (OSHA), and DHS, the task force has until May 2014 to deliver recommendations. OSHA and state regulators do not currently require an IST assessment. C&*EN* notesthat the Chemical Safety & Hazard Investigation Board (CSB) is also exploring an IST mandate after a rash of refinery accidents, including one at a Chevron facility in Richmond, California which sent 15,000 residents to area hospitals.

**IST was developed by Trevor Kletz, a chemical engineer with Imperial Chemical Industries, a British chemical company. For Keltz, IST functions well when implemented according to a hierarchy of actions: minimize use of hazardous chemicals, substitute or replace hazardous chemicals with safer ones, moderate or shift to less hazardous chemicals or processes at lower temperatures and pressures, and simplify processes and design plants to eliminate unnecessary complexity.**

“The very best way to prevent an explosion is to simply replace the material that explodes with one that does not, or at least keep the stock down so low that it hardly matters if it all leaks out,” Keltz told C&*EN* in 2003.

In response to a New York Times editorial in which CSB head Rafael Moure-Eraso called for regulators to require IST, and for industry to adopt it, three industry trade groups — the American Chemistry Council, the Society of Chemical Manufacturers & Affiliates (SOCMA), and the American Fuel & Petrochemical Manufacturers — published a letter to the editor in the Times, claiming IST is “an engineering philosophy, not a technique,” adding that the United States “has some of the most stringent regulations in the world.”

The trade groups urged regulators to focus on fully enforcing current regulations instead of making new ones. According to industry officials, adopting IST could lead to the elimination of some hazardous yet essential chemicals. Reducing or eliminating storage of some chemicals “would prevent some companies from effectively meeting their customers’ needs,” adds Jennifer Gibson, vice president of regulatory affairs at the National Association of Chemical Distributors.

**IST also calls for facilities to reduce the amount of materials or chemicals they store on-site; which would increase transportation of the materials or chemicals, thereby spreading the risk of chemical accidents to different points along the supply chain.** “Inherent safety is a superficially simple but truthfully very complex concept, and one that is inherently unsuited to regulation,” adds William E. Allmond IV, SOCMA’s vice president of government and public relations.

**One school of thought on the implementation of IST argues that IST will not prevent all facility incidents, but that it should be the first approach when considering ways to reduce risk at industrial facilities.** The U.K.’s Health & Safety Executive (HSE), which regulates workplace safety in England, operates a program which aims to reduce facility risks “as low as reasonably practical.” According to Ian Travers, head of HSE’s chemical hazard division, under the regulatory program facilities must consider the cost-benefit analysis of IST implementation. New facilities are required to conduct an initial risk review, including IST options during design, and existing facilities must periodically review and revise their operations to reflect IST implementation or consideration.

For American facilities, the CSB suggests that the EPA could require IST testing through the General Duty Clause of the 1990 Clean Air Act, which requires companies which deal with toxic chemicals to identify hazards, design and maintain safe facilities, and minimize the consequences of potential chemical accidents. Industry officials argue that current regulations, and the interest of facility operators to maintain a safe workplace, are sufficient incentives for companies to consider and adopt safer alternatives, including IST.

**In opposition, Christine Todd Whitman, former EPA administrator, insist that companies cannot be left to adopt IST methodologies themselves. “People’s lives are at stake. That’s why we need to have action at the federal level,” Whitman says.** A mandate to require facilities to adopt some IST concepts “when they’re available, effective, and affordable is common sense.”

*— Read more in Trevor Kletz and Paul Amyotte,* Process Plants: A Handbook for Inherently Safer Design*, 2nd ed. (CRC Press, 17 May 2010); and* Inherently Safer Chemical Processes: A Life Cycle Approach*, 2nd ed. (Wiley, December 2008).*

# Understanding the NFPA 473 Improved Standard for EMS Hazmat Professionals – 2013 update

Source: http://www.jems.com/article/major-incidents/understanding-nfpa-473-improved-standard

Response to emergency incidents involving hazardous materials (hazmat) and weapons of mass destruction (WMD) places public safety responders at greater risk of morbidity and mortality than the general public.1 Incidents involving hazmat can cause physical harm to both the public and first responders,2 necessitating the delivery of medical care during treatment and transport.3

EMS providers must be prepared for the challenges hazmat/WMD incidents present from chemical, biological, radiological, thermal, mechanical and asphyxiation hazards.4 This article details the latest National Fire Protection Association (NFPA) standard for EMS hazmat professionals.

**The NFPA Standard**

NFPA 473, “Competencies for Emergency Medical Services Personnel Responding to Hazardous Materials/Weapons of Mass Destruction Incidents,” was written in 1992 as a companion standard to NFPA 472, “Standard for Competence of Responders to Hazardous Materials/Weapons of Mass Destruction Incidents.”5

The NFPA Technical Committee on Hazardous Materials Response Personnel originally developed NFPA 473 because of the absence of existing guidance for the roles and responsibilities of EMS personnel at hazmat incidents and the recognition that hazmat incidents present unique challenges for EMS.

Although NFPA 473 has existed for more than 20 years, it’s often overlooked in the presence of its predecessor, NFPA 472.6 For the 2008 and 2013 editions, the Technical Committee felt it was time to breathe new life into NFPA 473, matching NFPA 472’s format and content by clarifying the roles of BLS and ALS responders during hazmat incidents, as well as introducing new mission-specific competencies for ALS responders.

**BLS Responders**

NFPA 473 defines a BLS responder as an EMS responder functioning at a level defined by the medical authority having jurisdiction either as an emergency care first responder (ECFR) or as an EMT-ambulance/basic (EMT-A/B).5

The goal of the competencies in NFPA 473 at the BLS responder level is to define the knowledge and skills necessary to safely deliver BLS medical care at hazmat/WMD incidents.

**The competencies defined for a BLS responder include:**

>> Analysis of a hazmat/WMD incident to determine potential health hazards;

>> Development of a plan to deliver BLS to any exposed patient within the scope of practice; and

>> Implementation of the prehospital treatment plan within the scope of practice by determining the nature of the hazmat/WMD incident.

**ALS Responders**

NFPA 473 defines the ALS responder as an EMS responder functioning at a level beyond the BLS level as defined by the medical authority having jurisdiction, either as an EMT-intermediate (EMT-I); paramedic (EMT-P), medical director or as a medical team specialist such as a nurse, nurse practitioner, physician assistant or physician.5

The competencies defined for an ALS responder include all competencies required of a BLS responder, plus:

>> A more detailed analysis of a hazmat/WMD incident to determine the potential health hazards, including an assessment of health risks and identification of patients who may be candidates for advanced clinical care;

>> The development of a plan to deliver ALS to any exposed patient within the responder’s scope of practice, including identification of supplemental regional and national resources; and  
>> Implementation of an enhanced prehospital treatment plan within the responder’s scope of practice by determining the nature of the hazmat/WMD incident, including an assessment of available equipment and evaluation of the need for advanced clinical care.

**Additions to the 2013 Edition**

Following the release of the 2008 edition of NFPA 473, the NFPA Technical Committee focused on bringing the document more in line with the philosophies of NFPA 472, in particular by defining mission-specific competencies for ALS responders who wish to specialize in specific skill areas.

**For the 2013 edition of NFPA 473, competencies were incorporated for the ALS providers assigned to:**

1. A hazmat team;
2. Provide clinical interventions at a hazmat/WMD incident; and
3. Treatment of smoke inhalation victims.5

The specialty areas are designed to provide guidance for EMS agencies that have a desire to integrate with a hazmat team, perform hazmat clinical procedures in the prehospital environment or protect response personnel from the hazards of smoke inhalation.

There’s no requirement for agencies meeting the competencies for BLS and ALS responders in NFPA 473 to train to the new mission-specific competencies, as the specialties are an optional enhancement to existing ALS response capabilities.

**ALS Responders Assigned to Hazmat teams**

Medical support to hazmat teams can present complex problems for ALS providers who aren’t aware of the procedures and responsibilities surrounding hazmat response operations.

Assigning dedicated ALS providers to participate with the hazmat team on training and response operations allows them to become advocates for the health and safety of hazmat team personnel.

The mission-specific competency for ALS responders assigned to a hazmat team is designed to provide guidance for hazmat teams that choose to integrally include ALS providers.

The competency defines the assigned ALS responder as “that person assigned to provide direct medical support and intervention to the members of an established hazardous materials team.”5

**The competency is organized into three primary areas:**

1. Plan a response within the authority of the agency having jurisdiction (AHJ) to support hazmat team operations;
2. Implement the planned response consistent with the standard operating procedures of the AHJ to support hazmat team operations; and
3. Terminate the incident consistent with the standard operating procedures of the AHJ to document hazmat team operations.

As part of the planning process, the competency guides the ALS responder to become a medical advocate for the team, including organizing team medical records, encouraging team fitness, ensuring appropriate team medical surveillance and establishing liaison with medical facilities that may potentially receive injured or ill team members.The competency also guides implementation of the planned response, including functioning in medical capacities within the incident command system, coordinating medical support to the team, ensuring rehabilitation is established and becoming a patient care advocate in the event of team member injury or illness.

**ALS Responders Providing Clinical Interventions**

There are numerous clinical interventions available to ALS medical providers who respond to hazmat/WMD incidents, based upon approved protocols from the AHJ’s medical director. The delivery of clinical interventions, such as antidotes for chemical exposure and associated clinical techniques, may provide improved patient outcomes, especially during extended transport times to definitive care.7

The provision of ALS clinical interventions should be viewed as a “tool in the toolbox,” utilized as necessary following an analysis of patient treatment and transport options. The ALS responder should base that analysis on existing AHJ treatment protocols, impact on favorable patient outcomes, available toxicological information and overall safety concerns.

Implementation of ALS clinical interventions within the exclusion or “hot” zone must be considered cautiously from the perspectives of responder safety, patient exposure times and available medical resources.

The mission-specific competency defines the ALS responder assigned to provide clinical interventions as “that person who is assigned to provide antidotes, antibiotics, and/or radiological countermeasures to persons contaminated by hazardous materials.”8

**The competency is organized into two primary task areas:**

1. Plan a response within the authority of the AHJ to provide advanced clinical interventions; and

2. Implement the planned response consistent with the medical protocols of the AHJ to provide advanced clinical interventions.

**Three competency areas are included to guide the ALS responder assigned to provide clinical interventions:**

1. Toxidromes for chemical, biological, and radiological materials;
2. Clinical intervention pharmaceuticals; and
3. Clinical intervention skills.

The mission-specific competency is designed to be flexible to fit the AHJ’s approved protocols for the delivery of clinical interventions; the AHJ utilizes competencies only for authorized interventions.

**ALS Responders Treating Smoke Inhalation Victims**

Smoke products released during structural, vehicle, aircraft and hazmat fire incidents present challenges for EMS responders. The presence of carbon monoxide, cyanide and other smoke products are sources of potential exposure for both victims and responders at every fire incident.

The competency is designed to provide guidance for the knowledge and skills of ALS providers treating smoke inhalation patients.5

The mission-specific competency identifies the considerations for ALS responders assigned to treatment of smoke inhalation victims and is organized into three major areas:

1. Analysis of the incident, including a survey of the incident and collection of information from potential victims and responders to determine if smoke inhalation has occurred;
2. Development of a plan to deliver ALS care to victims of smoke inhalation, including the availability of antidotes and identification of local treatment facilities; and  
   3. Implementation of a treatment plan for smoke inhalation victims, including decontamination,
3. Treatment of burns or other trauma, complete patient assessment including carbon monoxide levels, delivery of antidotes, and transport to an appropriate treatment facility.

The competency emphasizes the location, method of transport and routes of travel to appropriate treatment facilities such as trauma centers, burn centers, hyperbaric chambers and hospitals prepared for antidotal treatment of cyanide toxicity.

**Summary**  
EMS responders to hazmat incidents face significant challenges; however, integration of medical care providers into the planning process for hazmat incidents can facilitate a more efficient response. The competencies found in NFPA 473 provide thorough guidance for EMS professionals during planning, preparation and response to hazmat/WMD incidents.

**Disclaimer:** Names of commercial manufacturers are provided for identification purposes only, and inclusion does not imply endorsement of the manufacturer, or its products or services by the FBI. The views expressed are those of the author and do not necessarily reflect the official policy or position of the FBI or U.S. Government.

**References**  
1. Suyama J, Rittenburger JC, Patterson PD, et al. Comparison of public safety provider injury rates. Prehosp Emerg Care. 2009;13(4):451–455.

2. Maquire BJ, Hunting KL, Smith GS, et al. Occupational fatalities in emergency medical services: A hidden crisis. Ann Emerg Med. 2002;40(6):625–632.

3. Occupational Safety and Health Administration: Best practices for protecting EMS responders during treatment and transport of victims of hazardous substance releases. U.S. Department of Labor: Washington, DC, 2009.

4. Noll GG, Hildebrand MS: Hazardous materials: Managing the incident, 4th edition. Jones & Bartlett Publishers: Burlington, Mass., p. 270, 2012.

5. National Fire Protection Association: NFPA 473: Competencies for emergency medical services personnel responding to hazardous materials/weapons of mass destruction incidents. NFPA Publications: Batterymarch Park, Mass., 2013.

6. Schnepp R. EMS at haz-mat/WMD incidents? Well it depends... Fire Engineering. 2005;158(11):S21–S22.

7. Managing hazardous material incidents, vol. 1. (July 3, 2013.) Agency for Toxic Substances and Disease Registry. Retrieved on Jan. 15, 2014, from www.atsdr.cdc.gov/MHMI/mhmi-v1-2.pdf.

8. Emergency medical services: A planning guide for the management of contaminated patients. Centers for Disease Control Printing: Atlanta, Ga., 2000.

# UAE ready to join hands with global bodies to fight proliferation of weapons of mass destruction

Source: http://gulfnews.com/business/economy/uae-ready-to-join-hands-with-global-bodies-to-fight-proliferation-of-weapons-of-mass-destruction-1.1305000

March 16 – The UAE is keen on cooperating with the international community to prevent the spread of all types of weapons of mass destruction, said Dr Anwar Mohammad Gargash, Minister of State for Foreign Affairs.

Gargash pointed out that the UAE has harnessed financial and human resources by introducing national laws that enforce the monitoring of exports and cargos that pass through the country.

Gargash issued the statement when he inaugurated the **14th Export Control Conference**, which kicked off its activities in Dubai yesterday, and is held under the patronage of the UAE Ministry of Foreign Affairs and US Government.

**The conference represents a forum for participants to explore challenges, and discussing practical solutions and expertise on developing and effective implementation of strategic trade control. Other topics that will be touched upon include the UN Security Council Resolution No. 1540, monitoring transit cargo for strategic commodities and dual use goods, and the importance of monitoring the transportation of strategic commodities.**

The 14th International Export Control Conference has succeeded in developing the capacities of different countries to implement control on the strategic commodities to combat the proliferation of weapons of mass destruction and acknowledge the importance of regulatory compliance and multilateral non-proliferation of the weapons of mass destruction.

“The UAE has set up various regulatory bodies, such as the ministry’s Committee on Commodities Subject to Import and Export Control in 2009. In cooperation with federal and local government bodies, the committee has enforced various regulations on strategic commodities that are key components in the manufacturing of the weapons of mass destruction,” Gargash said.

“The committee was successful in seizing and uncovering a number of suspicious consignments, some of which have been returned to the country of origin,” he added.

Gargash said the **UAE, in cooperation with American and European teams, hosted 30 training workshops for staff of relevant government bodies, and was keen on promoting a culture of export control among these bodies.** He added that training courses were also organised for private sector companies, and that through such massive efforts, the UAE has become a networking hub between countries involved in the import and export of strategic commodities due to its strategic location as a meeting point between the west and the east.

Gargash thanked the UAE side and other organisers of holding such an international event to give the UAE an opportunity to demonstrate its achievements in this respect.

He highlighted the UAE policy on development of its peaceful nuclear programme adheres to the highest specifications and standards to non-proliferation of nuclear weapons, adding that the UAE joined The Treaty on the Non-Proliferation of Nuclear Weapons in 1995.

Becoming biohackers: Learning the game (Part I)

Source: http://www.bbc.com/future/story/20130122-how-we-became-biohackers-part-1

*When you have lunch courtesy of the FBI, you are offered chicken Caesar salad, hamburger or fish. Soft drinks are extra. Throughout our two-day visit we were happy to dine on FBI hamburgers and Caesar salad, but declined the seafood option. The atmosphere seemed fishy enough.*

*We were in Walnut Creek, California, at the invitation of agent Nathaniel Head. He is a nice guy with a pleasant demeanour; there’s no furtive spy-like behaviour or obvious demonstration of power. He may be dressed in a smart khaki suit and striped tie (red, white and blue, of course), but he acts more like a professor. And thanks to a university background in microbiology, he is able to talk knowledgably about science. Head spared no effort in making us feel at ease, and the other agents present tried to do the same – all wide smiles and “glad-to-have-you-heres”.*

*But despite this bonhomie, sitting in the windowless conference room in the basement of a nondescript hotel building in Walnut Creek still left us feeling uncomfortable. And it wasn’t just because there was a palpable Big Brother atmosphere in the room. Instead, we were acutely aware that we must have done something to bring us to the attention of Head; someone whose area of expertise is weapons of mass destruction.*

*But we don't smuggle plutonium. We don’t supply chemical weapons. We don’t build rockets.*

*Instead, we have a hobby that the FBI believes could be so dangerous that they have come up with a special programme to make sense of it.* ***That hobby is to play with genes, proteins and bacteria in our spare time in a homemade lab we constructed from scratch. We are part of a rapidly growing community of amateur geneticists, who are often labelled biopunks, or outlaw biologists. Or, better still, in an analogy to the computer programming enthusiasts of a generation ago, some call us biohackers.*** *But instead of software code, we try to tinker with DNA, the code of life.*

*And we’re far from alone. For several years a growing number of do-it-yourself biologists around the world have been carrying out the sorts of experiments that, until recently, were only possible in professional labs.*

*Now, in an attempt to keep track of what’s going on, the FBI has set up the Biological Countermeasures Unit, which Nathaniel Head is a part of. One of their goals in preventing acts of terrorism is to reach out to leading names in the field to quiz them about what they do. Which is how we ended up in Walnut Creek, as part of a workshop involving FBI agents and around 30 of the most prominent members of the growing DIYbio movement.*

**Acid test**

This movement has become possible being because the techniques used in molecular biology have become simpler and cheaper. A couple of decades ago, it took three years to learn how to clone and sequence a gene, and you earned a PhD in the process. Now, thanks to ready-made kits you can do the same in less than three days. Specialised materials and second-hand equipment are much more affordable, not to mention more available. Machines for amplifying DNA can now be purchased online, whilst enzymes and chemicals for creating, manipulating and sticking together DNA can be ordered off the shelf. The cost of sequencing DNA has plummeted, from about $100,000 for reading a million letters, or base pairs, of DNA code in 2001, to around 10 cents today.

So, in theory, there is now nothing to stop someone from constructing a lab, donning a white coat and becoming an amateur genetic detective – especially three science writing friends from Berlin and Munich with university degrees in biology (though admittedly we’d earned these more than a dozen years ago).

Or is there? That was what we wanted to find out. Could we manipulate and analyse genes like professional scientists do? Could we break into cells and hack their DNA? Would we be able to transfer this material from one basic organism to another? How far would we be willing to test the ethical or legal issues surrounding this work? Or is biohacking just another fad that is too tricky and laborious to ever take off beyond the level of geek-driven enthusiasm?

More than two years ago, we set out to build a lab for ourselves to see what was possible and to help us understand this burgeoning field. When we started, we were not aware of any DIY biologists in our native Germany; biohackers were (and still are) mostly in the US.

Since then, biohacker communities have popped up around the globe, with hundreds of do-it-yourself biologists testing their experimental prowess. Visit one of the many online forums dedicated to the field and you will find thousands willing to join the movement, all eager to try and engineer DNA in their kitchen or garage labs. Like home chefs scouring and testing recipes available on the web, biohackers use freely downloadable protocols to clone genes in bacteria. You can, for example, make bacteria glow in the dark – just for fun.

But back in 2010, there was no thriving virtual community, no convenient how-to guides for the curious. So, on a cloudy morning in April we found ourselves on a plane heading to the US for the first of several road trips to meet the leading lights of the biohacking community and ask if they could help us out.

**Bedroom genetics**

One of the first people to open their doors to us was Kay Aull. A superstar of the biohacking world, Aull rose to prominence after building her own genetic testing kit in the small room she used to live in as a student in Cambridge, Massachusetts. In her makeshift lab, she analysed a specific gene mutation linked to a disease her father was diagnosed with, called haemochromatosis. If you have it, the body is unable to get rid of excess iron. With relatively simple – and cheap – tests, the Massachusetts Institute of Technology (MIT) graduate found both the faulty gene from her dad and the unaffected one, inherited from her mother, in her own DNA. The result meant she is a carrier but unlikely to contract the disease.

When we first met Aull, she shared an apartment in the Cambridgeport area near MIT with other students and her three cats. With bobbed hair, glasses, and wearing a skiing vest, she looked like the picture-perfect nerd, but we soon discovered an inviting, open-minded person with an engaging attitude.

After opening pleasantries, she led us to her bedroom, with nosy cats following, and proudly opened her closet door to reveal her $500 genetic engineering lab. Chemical reagents, syringes, Petri dishes, pipette tips and Erlenmeyer flasks sat on the top shelf, next to a pile of T-shirts. A power supply and a home-made lightbox that makes DNA visible were neatly arranged below. On the bottom shelf, was a vintage block-like contraption for copying DNA that showed its 10-year age by the noise of its ventilation system whenever it was turned on.

Aull decided to investigate her own genetic legacy when her father was first diagnosed with haemochromatosis. He was given pages and pages of documents packed with scientific jargon that he was “unable to make sense of”. Frustrated, she decided “to show people in a similar situation that genetic testing is not magic” – that it is a routine technique just like an oil change for a car.

Her apartment-turned-lab was testimony to that, and to the innovative spirit which underpins biohacking. To get samples of cells swabbed from her cheek to pop open and release their DNA Aull did nothing more sophisticated than heat them in a saucepan of boiling water in her kitchen. Her second-hand equipment made over a million copies of the gene that might carry the haemochromatosis mutation. And to visualise the amplified DNA to see if the gene carried a mutation, she used blue Christmas tree lights instead of the expensive high-end trans-illuminators that professional labs use.

If this sounds like the kind of thing you should probably not be doing alongside your pot of pasta, Aull reassured us her experiments were harmless. Her test? She only used materials that would do no harm to her cats if they inadvertently encountered anything.

Aull embodies the common purpose that drives most people in the biohacking world. Many do not just want to play with something new. Instead, they share an impulse to empower themselves, and to not leave everything to the experts. They are happy to show novices the fruits of their labours. It was an enlightened vision of the democratisation of science.

Yet it is impossible to avoid the negative connotations of this utopian outlook. Mention scare stories, and the name of Steve Kurtz will undoubtedly crop up. When we visited the arts professor at the State University of New York, he still had vivid memories of the day in May 2004 when the FBI, accompanied by a special anti-bioterror unit, raided his house in Buffalo, NY. His wife Hope had died at home the previous day. Kurtz called 911. When the paramedics arrived at the scene, they saw Petri dishes with bacterial cultures. “They were looking at this stuff, and thought maybe I killed her by some kind of biochemical toxin,” recalled Kurtz. Next day, the grieving Kurtz, on his way to making arrangements for his wife's funeral, was detained by the FBI and interrogated for 22 hours as a bioterrorism suspect. His cat was confiscated on the suspicion it was being used as a vector for spreading a deadly infection in the neighbourhood, though Kurtz said he found it locked up in the attic when he returned.

It was a false alarm in the most tragic of circumstances. Hope had died from heart failure. The bacteria in the house were part of a video installation project called Marching Plague, a re-creation of a 1952 British military experiment in which guinea pigs were infected with bubonic plague to see how fast it would spread. The bacteria Kurtz used was harmless with no more potential for harm than the mould growing on a lump of Roquefort – Kurtz said he even licked some off the Petri dishes in front of the agents to make the point. But it took four years for Kurtz to be acquitted of all the charges. “You would think that I would be feeling light as a feather and dancing down the street,” said Kurtz at the time of acquittal. “Quite the opposite; it's more like having some kind of post-traumatic stress disorder.”

**Community support**

It is from these underground, sometimes disorganized, often misunderstood roots that biohacking has started to become more mainstream in recent years. No longer is it just confined to basements, garages and kitchens. Instead, so-called biohacker spaces have begun to spring up, such as Genspace in Brooklyn, New York. Set up 2010 and supported and advised by a scientific board that includes the eminent geneticist George Church at Harvard Medical School, Genspace is a state-of-the-art laboratory where everyone from aspiring to advanced biohackers can experiment for a fee of $100 per month. There’s no need for someone to buy their own vintage equipment, no need to repair it themselves and no need to cultivate bacteria in their kitchen. And there is always someone around who can help – the biohackers at the next bench, or one of the professional bioscientists running the lab.

Its president is Ellen Jorgensen, whose enthusiastic greeting suggested she takes the labs motto – “remember the time when science was fun” to heart. “The advantage of community labs is that what you attempt to do doesn't have to be economically or medically important, it can be anything you want,” said Jorgensen, an experienced geneticist, and probably the world's most prominent voice behind the DIYbio movement. “But then, the thing that really hooks you in the end is the enthusiasm. People are doing this by choice, they are not doing it because they have to make a living out of it, they are doing it because they have a passion for science.”

For instance, one artist there was experimenting with bacteria that can produce “beautiful patterns”, using different nutrients which make colonies grow in specific ways and change colour. Another group was preparing balloons to be sent into the stratosphere to detect traces of DNA from unknown bacterial species that might be floating up there**.**

The seeds of the DIYbio movement were sown in 2003 at MIT with a programme called iGEM (International Genetically Engineered Machine). The following year, it hosted the first of its annual competitions, where teams of high-school and college students are given “BioBricks” – chunks of genes with standardised structures and known functions which they can tinker with and build upon. They get their name because they are like genetic Lego pieces.

Some of the results of these experiments are impressive: teams have created a designer vaccine against the bug that causes most ulcers, Helicobacter pylori; turned bacterial cells into hemoglobin-producing blood substitutes; and converted bacteria into tiny “sniffer dogs” which can detect rotten meat. iGEM has become so successful that it was recently spun out from MIT to form an independent non-profit organisation hosting regional play-offs in Europe and Asia. Last year’s competition hosted 190 teams and over 3,000 participants from 34 countries.

Its popularity helped see biohacking spread. For instance, in Sunnyvale, California, the heart of Silicon Valley, a hackerspace called Biocurious opened its doors in the summer of 2011, thanks to donations raised through the crowdsourcing funding platform Kickstarter. Back in Cambridge, Massachusetts, there’s the Boston Open Source Science Lab (BOSSLab) in a nerd shelter called Sprout. In Baltimore, a hackerspace called BUGSS recently emerged thanks to an iGEM team from a local community college.

Many of these enthusiasts are also working out clever ways to make inexpensive tools. BOSSLab’s founder, Mac Cowell, used to offer an amateur genetic testing kit via the internet and his new goal is to sell entire DIYbio starter kits. Biocurious members Tito Jankowski and Josh Perfetto are building cheap machines for PCR (polymerase chain reaction), the all-important method to amplify large amounts of identical pieces of DNA from tiny samples.

The ideas, energy and drive behind these people are reminiscent of the early computer pioneers who built the software and hardware that kick-started the computer revolution, and went on to found household names like Microsoft and Apple. So, it’s not too great a stretch of the imagination to see that the next generation of entrepreneurs could be biologists, not programmers. In fact, during our US road trip Microsoft's founder Bill Gates told Wired magazine that, if he were young today, he “would be hacking biology, creating artificial life with DNA synthesis”. Creating artificial life with DNA synthesis is similar to machine-language programming, he added. “If you want to change the world in some big way, that’s where you should start – biological molecules.”

All of this left us determined to find out for ourselves. As our plane back to Germany touched down, we looked at each other's red eyes. “Let's do it ourselves,” we said on that gloomy Frankfurt morning – a phrase that would be repeated time and time again in the weeks and months that followed.

# Becoming biohackers: The experiments begin (Part II)

Source: http://www.bbc.com/future/story/20130123-hacking-genes-in-humble-settings

It’s amazing what you can buy on eBay nowadays. Scan down the main categories, past Antiques, Art, Baby and Books, Comics & Magazines, and you’ll find the Business, Office & Industrial section. Click on it and you will see various subcategories, including one for Medical/Lab Equipment. This, as you’ll discover, is a biohacker’s dream world.

Almost everything you need to run a basic do-it-yourself biology lab is up for grabs. Need a centrifuge to separate your DNA from cellular junk? Take your pick of 20. How about a lightbox to illuminate your DNA fragments? No problem. It is the same for the scales you need to weigh minuscule amounts of chemicals; pipettes, pipette-tips, and plastic tubes to handle and dispense tiny amounts of liquids; and Bunsen burners (or, in our case, a much cheaper camping gas burner) to sterilise equipment.

Other biohackers had told us that eBay was like this, but it wasn’t until we began to look for everything on our shopping list for our own lab that we believed them.

The biggest piece of machinery on the list was the PCR machine, also known as a thermocycler. It’s essentially a souped-up water bath, but it enables an indispensable technique worthy of a Nobel prize. Invented by Kary Mullis in 1983, the Polymerase Chain Reaction, or PCR for short, amplifies genetic material quickly and reliably, creating up to one billion times the DNA you started out with. It’s the technique used by forensic teams to get evidence from crime scenes, by lawyers for paternity tests, and – we hoped – by a group of German journalists to successfully carry out genetic experiments.

While chatting with one seller about some technical details, we learned he had another one that he found at his university waste tip. Twenty years ago the machine would have cost a professional lab as much as a home in the Berlin suburbs. We agreed to take it together with a power supply unit for 320 euros.

The amazing thing was that no one asked any questions during our shopping spree. True, we did receive a suspicious look from the person behind the pharmacy counter when we wanted to buy a bottle of 100% alcohol. But once we assured her that it was for genetic experiments rather than drinking, she was happy to hand over the big brown glass bottle.

We were also held up by customs when we tried to bring in a small lightbox that helps to illuminate DNA fragments. We tried several times to explain what biohacking was and how we planned to use the machine, but the customs officers didn’t seem to believe that anyone would – or could – set up a genetics lab in their kitchen. Exasperated, one officer interrupted another fruitless attempt to explain what the machines did. “So, it's something for computers?” she asked. Her male colleague, clearly tired of the conversation, cited a procedure concerning items with a value of no more than 250 euros.

“Is it something electrical?” he asked. “Er... it does need electricity, yes,” we replied. With that, he waved us through.

This completed our lab list: total cost, including the chemicals and biological materials needed, was 3,500 Euros and 51 cents. It's a lot of money, but splitting the cost between us, we paid less for a working lab than the cost of an Apple laptop each.

**Lonesome warriors**

As our partners weren’t keen on using any of this stuff at home, we decided to build the lab in our office in the Schoneberg district of Berlin**.** We got strange looks from those in the neighbouring offices, who were used to journalist's long phone calls but not the whirrs and beeps from PCR machines or centrifuges.

Once we had the equipment assembled, the worries began. We had vague memories of the practicals we had to do in our university biology classes – some good, but mainly bad, a litany of failures and frustrations. Some of the procedures we were about to try in our improvised lab were exactly those kinds of experiments. The only difference was that this time we could not count on a supervisor or skilled colleague to help us. We had to rely on our faded memories of lab work and on internet sources to help us whenever we got stuck. We had a lot of questions. Would we be able to isolate DNA? Would we amplify genes with a machine salvaged from the trash? Would even the simplest experiments be beyond our meagre skills? Would we join the legions of people who bought a surfboard but never really rode a wave, or who bought a guitar and never got beyond “Country Roads”?

There’s an open secret that every professional scientist knows about lab research. It’s difficult. It’s frustrating. It rarely goes right. The amount of blood, sweat and tears you put into an experiment bears little reflection on whether it will actually succeed.

We learned the hard way that lab work – especially in a DIY setting – consists of a lot of trial and error. The trials are promising, the errors devastating. You make a small mistake with the buffer solutions that keep your samples stable, and days of work can go down the drain. You misplace or accidentally contaminate a tiny drop of liquid while pipetting into a tube that's smaller than a thimble, and your experiment fails. You try different salt concentrations to make the experiment run better, you vary heat and cool cycles for your PCR machine, you test whether a little more of the DNA-copying enzyme might do the trick. You have to improvise and be patient.

Added to that, of course, there's the downside of the cheap supplies and the vintage machinery you use. It’s like making a souffle in a kitchen you’ve never cooked in, using old utensils you’ve never used, and an old oven that may or may not reach the temperature required. You have the correct recipe and the ingredients but you have no idea if the souffle will rise. If it doesn’t, your only option is to start again, add a bit more of an ingredient, whisk the mixture a bit more, or turn an oven dial slightly, and cross your fingers that at some point it will rise.

To make things worse, the makeshift observation room where we looked at our abject failures was the toilet in the Schoneberg office building. It was the only room without windows, which made it the only room dark enough to be able to see any traces of amplified DNA in our gels.

After days and nights of fruitless effort in our overheated office corner, not knowing where the glitch in the system was, our nerves were on edge. Nothing seemed to work. We made countless trips to and from the toilet, staring at countless blank gels, willing a band to appear that never did.

When we had been researching our venture in the United States Kay Aull, one of its pioneer biohackers, had warned us: “There's a lot that can go wrong, and you don't have colleagues who can come to the rescue and explain what your mistake was and what to do about it – you're lonesome warriors.” In our case, we tried not to think of the money wasted on failed experiments, or the fact that our regular daytime jobs which paid the rent were taking a hit because the experiments had become an obsession.

**Glowing triumph**

But after many efforts something magical happened. Two of us were locked in a toilet in the usual fashion, both looking at a gel, like we had done a dozen times before, weakly hoping that this time we would be able to see a trace of DNA. Then it appeared: an orange band. It was pale at first, a small, rectangular glowing band that told us there was DNA within it. It had been copied a million-fold in our second-hand PCR machine saved from the tip, separated from all the other gunk by running the sample in a gel, and we could see it thanks to the “electric item” that the customs people had quizzed us about. All the effort, work, frustration and expenses of the last couple of months were forgotten in a single, triumphant moment. We had done it. We could officially say we were biohackers.

What we were staring at was DNA from a piece of fish we had bought from our local sushi restaurant. The gene is called COX1, and is found in mitochondria, the energy-converting machines found in the cells of all higher life forms. Scientists call this gene the barcode of life, as its makeup varies slightly but noticeably between species. If we had more sophisticated equipment, or were ready to pay a service laboratory, we could have deciphered the code a bit more, and seen which kind of fish it was from. Amateur scientists had done this before, for example, high-school students in New York found several cases of sushi restaurants selling mislabelled fish.

For us, though, it was enough to know that we could test what was inside our food. Our experiment was the proof of principle we had been looking for. The next step was to see what else was possible in a home lab, and so we turned to our own genes.

That’s where we hit the first legal barrier. Analysing sushi doesn’t contravene any laws, but analysing human genes might. Clause no. 7 of Germany’s Genetic Diagnostics Law, passed in 2009, states that only physicians are allowed to do “diagnostic genetic testing”. One of the law's main objectives is to protect any individual from having their personal genetic information exploited. It's not that clear cut, though. There is also the entitlement to informational self-determination, which the German constitutional court has defined as a basic right. We decided to take the value of this basic right above the letter of the law. After all, we didn’t want to look into other people's genes – just our own.

After much discussion, we decided not to look at genes related to disease, agreeing this is best left to trained doctors. But there were other areas we could look at in our genome, using the same methods and principles. For example, there’s one gene which, depending on what version you inherit, may make you more likely to be a good sprinter or a good long-distance runner. The gene in question is ACTN-3, or alpha-actinin-3, and it’s active in skeletal muscle. Two of us had memories of our high school athletics performances – one was more of a Usain Bolt, the other more like Mo Farah. So we isolated DNA from two saliva samples. We amplified the DNA with our PCR machine. We looked around on the internet and bought an enzyme that cuts the mutated version of the gene in two places, but the normal version only once. We saw different patterns in the gel: the Usain Bolt-type of us appeared to carry the intact ACTN-3 version, whereas the Mo Farah-like runner showed the signs of a tiny, but important mutation which might give endurance runners an edge.

**Security risk**

So, after checking the DIY box for food analysis, we ticked the one for human genetic testing. The third step was the most serious. We wanted to explore the security and safety aspects of the biohacker movement.

Within a few days, a courier for a biotech company arrived at our office, looking a little surprised that the delivery address wasn’t a working lab. He handed us a package that cost us 23.73 euros. Within it were two tubes containing DNA, whose codes spelled out the beginning and end of the gene for a powerful botanical toxin. It’s usually produced by the castor oil plant, Ricinus communis, but is better known as ricin. As a quarter of a milligramme is enough to kill a heavyweight boxer, it's officially a bioweapon according to the United Nations, and US counterterrorism officials fear al Qaeda members in Yemen are trying to produce bombs containing the toxin.

According to the US Centers for Disease Control and Prevention’s website: “Ricin works by getting inside the cells of a person’s body and preventing the cells from making the proteins they need. Without the proteins, cells die... Death from ricin poisoning could take place within 36 to 72 hours of exposure, depending on the route of exposure (inhalation, ingestion, or injection) and the dose received.”

The gene, though, is inert. It’s not poisonous, it just contains the biological code to make the bad stuff. But it is on the list of potentially dangerous DNA fragments, which can only be ordered by specially registered laboratories. We did not want to produce anything dangerous, but we did want to probe how easy or hard it might be to do so – to legally obtain the required molecular ingredients for example, and to handle genes which might be the blueprint for producing something that could serve as a bioweapon. We only ordered portions of that code, the beginning of the gene, and the end. But, in theory, that’s enough for a biohacker to make the whole thing.

This could be considered the first step towards bioterrorism. The most disconcerting part is that the routine is not much different from our sushi experiments. After some trial and error, some consultation of freely available web-based databases and protocols and some tinkering with our kit, we succeeded. We looked at another band glowing in a gel. This time, it was the ricin gene.

In our hands, embedded in a gel of agarose sugar, were millions of copies of a gene that contains potentially deadly information. There was nothing to stop us from trying to put the gene for one of nature's most potent toxins into bacteria to see if we could make them produce unlimited copies – clone the ricin gene in other words. It could be done in a day; cloning genes is a mundane, everyday task in professional labs worldwide, even for biohackers at home or in collectives. This wouldn’t be a threat on its own – microbes may be able to produce a full ricin protein, but they can’t process it in a way the castor plant does to arm the poison. On the other hand, there are protocols available to work around these hurdles. There is scientific literature showing how to produce only the toxic part of ricin and turn it into a therapeutic agent against cancer cells. But it begs the question of whether we could – in an improvised office laboratory – do the experiments needed to create a potential bioweapon?

We stopped short of trying what would be an illegal and dangerous step. We needed to reflect on what we’d learned. We succeeded not only in getting all the materials we needed, but also doing almost everything we had set out to do.

Not long after we paused our experiments the word spread through the community that the FBI planned an event with biohackers from the US as well as Europe and Asia. We requested an invite. The FBI was asking the same questions we were, questions we thought society should be asking, too. What could the future look like in terms of biotech citizen science, but also in terms of DIY-bioterror and sabotage? And how do you try to guard against threats that may not exist yet? Those are the questions we will try to answer in the third and final part of our journey into the world of biohacking.

# Becoming biohackers: The long arm of the law (Part III)

Source: http://www.bbc.com/future/story/20130124-biohacking-fear-and-the-fbi

We were late. The route to Walnut Creek using San Francisco’s public transport took longer than we thought. When we eventually arrived, breathless, at the lobby of the Marriott Hotel, signs saying “FBI workshop” led the way to the basement. We hesitated. Should we really be part of this? Should we really reveal what we had been doing for the last two years to the FBI? Before we could reconsider, we saw a friendly, 40-something man in a khaki suit and white-collared shirt welcoming a crowd of more than 30 other people from across the globe. “We appreciate you guys coming, it's good to put names to email addresses,” said Nathaniel Head, the supervisory special agent of the FBI’s Biological Countermeasures Unit.

The other faces in the room showed just how much the field of biohacking had evolved since we began our own experiments nearly two years earlier. Then, almost all amateur geneticists – tinkering away with DNA in their kitchens and garages – were based in the US. By the time of the conference, we knew hackers around the world, from Ireland to Indonesia, from Singapore to Denmark, even in our native Germany. There were now biohacking organisations, biohacking events, virtual networks and co-working spaces for enthusiasts to swap stories, advice and protocols.

As the field has steadily grown, so have the headlines. Some have been positive, trumpeting its promise and hailing it as a demonstration of democratic science. Others have been much less welcoming, fearing a possible dawn of bioterrorism, where rogue biohackers manipulate toxic genes to create dangerous, pathogenic microbes.

Although the truth is perhaps less sensational, one thing is clear: biohacking is a rapidly growing field, driven by ever more powerful – yet affordable – technology. It’s only a matter of time before anyone with an eBay account and the right motivation could do the type of DNA experiments we did in our make-shift lab.

No one is more acutely aware of this than the FBI. To counter the threat posed by weapons of mass destruction (WMD), the US intelligence agency established the WMD Directorate in 2006, aimed at dealing with “incidents involving nuclear, radiological, biological, or chemical weapons”. Since then, its Biological Countermeasures Unit has closely followed the emerging field of biohacking. Agents in 56 FBI offices across the US reached out to the field’s leading names, acknowledging their efforts and learning about what they do. And, as the movement spread beyond the US, Head organised the first international DIYbio Outreach Workshop – which is where we found ourselves breathlessly shaking hands with the special agent in June 2012, and rubbed shoulders with well-known members of the biohacking community, such as those based in Copenhagen's Biologigaragen, Manchester's Madlab, New York's Genspace or Paris's La Paillasse.

Head, who holds a university degree in microbiology, seemed open-minded towards biohackers. He called the gathered crowd “great thinkers” and “innovators”, who were changing the world. But he left no doubt as to the reason behind the workshop. “We want to learn about biohacking and to be able to separate between the white and the black hats,” he said, differentiating between harmless amateur tinkerers and potential bioterrorists misusing genetic engineering technology.

Is it justifiable to fear that amateur biologists might see it as a personal challenge to make a killer virus in their garage, as Michael Osterholm of the US National Science Advisory Board for Biosecurity put it in 2012? Is every second-hand biotech machine sold on eBay and every new DNA technology kit marketed by biotech companies a step in that direction? The FBI clearly see it as a possibility, and it is perhaps easy to see why.

**Bioterror agents**

Take the recent controversy surrounding man-made forms of the flu virus. Last year, two teams of scientists – one led by Ron Fouchier at the Erasmus Medical Center in Rotterdam, the Netherlands, the other led by Yoshihiro Kawaoka at the University of Wisconsin-Madison in the US – announced they had each mutated the H5N1 bird-flu virus in such a way that it could spread between mammals more easily. Fouchier and Kawaoka argued they were trying to understand how natural viruses evolve into more dangerous forms, but their announcements sparked an international storm: should the work be published in full to help authorities prepare for a potential pandemic, or should it be withheld from the research community to prevent possible misuse by amateur scientists or even bioterrorists? As a result of months of pressure from scientific journals and notable names in the field, the work was eventually published last summer, but as a compromise the researchers agreed to a self-imposed moratorium on such work. After a year of discussions, the ban has just been lifted.

But some academics – and many within the biohacking community – are sceptical about such fears. Most biohackers, ourselves included, aren’t doing new science – though it is a new way of doing science. “Just having the right cookware doesn't make you a great chef just yet,” says Jason Bobe, director of the Personal Genome Project at Harvard University and co-founder of the organisation DIYbio.org. “It's misguided to think that everything a professional lab can do will also be possible in a home setting.”

Others point out that any bioterrorist who is focused on causing havoc, could do so by far simpler means. “You don't even need to synthesise anything new,” says Eckhard Wimmer, a virologist at New York State University at Stony Brook who first demonstrated that the polio virus can be reassembled from tiny pieces of hereditary material. His work raised fears that rogue groups could create something similar, but he argues the complexity of the work is enough of a barrier. He also cites previous examples of bioterrorism, which required little understanding of genetics and its techniques. For example, 11 years ago a number of American federal politicians were sent anthrax spores through the post, something that required a lot less effort than trying to reactivate polio in the lab.

Similarly, the ricin toxin found naturally in castor beans has been manufactured and used as a bioweapon, but no use of synthetic ricin bacteria or man-made toxin has been heard of – it is much easier to isolate the poison from plants or seeds than produce it from genetically engineered organisms. “Nature is the better bioterrorist,” says Wimmer.

But, the FBI are still wary. To try to spot any potential issues, the agency encourages biohackers to adopt a neighbourhood-watch-style approach – to be the “first-line defence” against “nefarious actors”, as Craig Fair of the FBI's Counterterrorism Division in San Francisco put it during the Walnut Creek workshop. The biohacking community in the US has largely responded in kind. Collectives such as Genspace in New York began working with the FBI early on, and the agency even helped them in their dealings with the local fire safety and health authorities. A spokeswoman for the agency told us there is currently no surveillance or investigation of any biohacker labs. No lab ever had to be closed, and DIYbio activities have “absolutely nothing criminal about them”. The experiences by now “are overwhelmingly positive”, she added. That’s the official line, anyway.

One session at the conference asked the assembled group to think about possible worst-case scenarios. In one example, a biohacker called “Deb” was sneaking castor beans into the lab, and engaging in aggressive, politically-charged discussions with lab members. “How do you respond in this situation,” Kate Carley, another charming FBI officer, asked the biohacker crowd. “Do you report the incident?” Regardless of what we thought, the FBI’s answer is a resounding yes. Her next slide showed Deb leaving the community lab to secretly work at home, before being arrested for experimenting with human pathogens and toxins. Even worse – for us at least – the fictitious slide showed newspaper stories where Deb was described as being part of the biohacker community.

These slides were clearly designed to show the most extreme examples and to drive home the FBI’s point. When asked whether a real “Deb” had ever been investigated, arrested, or even heard of, the FBI’s Head had to admit: “No.”

**Surveillance systems**

The idea that well-meaning biohackers could help the FBI by reporting any suspicious activities, has many in the field worried, particularly those outside of the US. “[It] reminds me of the Stasis's methods,” says Rudiger Trojok, one of Germany's most active biohackers, comparing the policy to the infamous spying network that operated in East Germany between 1950 and 1990. “Biohacking is not the FBI's, it's a civilian business.”

Of course no one in the biohacking community wants to see any rogue biopunks creating headlines that would bring the entire community into disrepute. To try to counteract this, the DIYbio community is running a survey that it hopes will dispel any misconceptions about its motives. The German biohackers we got to know, such as Trojok from Freiburg and Lisa Thalheim of Berlin, have even started to draft rules for what they call “biohacking ethics”. Their code of conduct would include moratoria on certain kinds of experiments, a registration system and mutual voluntary inspections of labs by biohackers.

But even this concerns some practitioners, who worry that a field that has flourished precisely because it is informal and unregulated, will be stifled. When Trojok and Thalheim presented their ideas about a “web of trust” at a meeting at the London School of Economics in 2011 some felt it was too restrictive. Instead, people like Jason Bobe from the Personal Genomes Project at Harvard University, favours a much more liberal approach, with general Hippocratic rules like “do no harm” at its core.

Together with Todd Kuiken from the Woodrow Wilson Center in Washington, Bobe has just launched an initiative called “Ask a Biosafety Expert” that, in their view, best meets the hobbyist’s needs. The idea is that biohackers from all over the world can go to the diybio.org website anonymously and submit any questions, from how to clean things up to aspects of the safety of experiments. Within a day or so they’d receive an answer from a biosafety expert. This way, according to Kuiken, people could operate in a safe manner, relying on personal responsibility rather than control.

Of course, nobody knows if a stick or a carrot is the right tool as we enter the age of personal biotech. But whoever is given the task of devising rules will have to consider the virtues of having molecular biology among the masses – can personal biotech improve society, will it lead to valuable inventions and innovations, will it be a democratising force, will it help distribute wealth, economic and intellectual power more widely?

These are all big questions for a field that is still in its infancy, says Ellen Jorgensen, president of the community biotechnology laboratory Genspace in New York. “It’s too early to tell,” she says. “You can argue, that if you get people with radically different backgrounds, you get fresh perspectives and new ideas. And you can argue that science is so complicated now, that DIY could not make any valid contribution, that you need to have too much expertise and infrastructure, (something) that DIY would never have.”

Jorgensen is optimistic, however. “There’s certainly a great potential, and I’m not the one who would say, that it is not going to happen. I want to see it happen!”

Of course, all the nice, well-meaning people we met during our long journey through the world of DIY biology are no guarantee that there isn't anyone out there putting their criminal energy into biotech. But limiting the work and the opportunities of the former just because of fear of the latter will do nothing to change that.

Methods and materials, such as the ones we used, are on the verge of becoming available to a wider public. It is that public which will have to decide how to use biotech in the future. To be able to do that, people need to have the opportunity to get to know and use it, rather than leaving the decisions about its future to the political, industrial and scientific elites.

The hope is that we and others in the DIYbio movement can and will continue to switch on a light which allows people to better understand a technology that may shape their future in major ways. We may have locked ourselves up in a toilet so that we could see our first DIY-produced gene. But we did so in order to keep the light out, not the police.

***Hanno Charisius, Richard Friebe*** *and* ***Sascha Karberg*** *are science writers living in Berlin (RF and SK) and Munich (HC).*The full account of the authors’ experiments will be published in Biohacking: Gentechnik aus der Garage (Genetic Engineering from the Garage), and an English e-book version is also planned.

|  |
| --- |
| EDITOR’S COMMENT: I think that these three articles represent a “first” on a new field of possible future threats. Now that somebody rang the bell we have no excuse to close our eyes or say (as usual) that writers exaggerate reality. This is how things start… |

## Exclamation_red.png25 children in California stricken with polio-like illness

Source: http://www.homelandsecuritynewswire.com/dr20140225-25-children-in-california-stricken-with-poliolike-illness

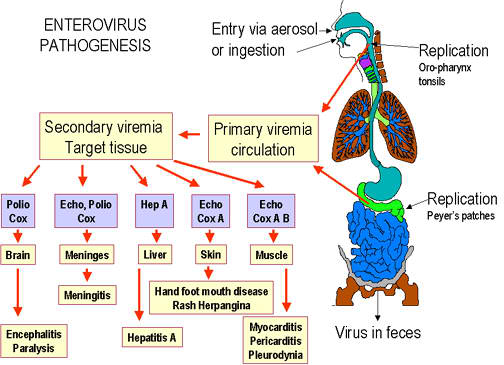
**Twenty-five children in California have been exhibiting a “polio-like syndrome,” leading to paralysis in one or more of their limbs.**

 “What’s we’re seeing now is bad. **The best-case scenario is complete loss of one limb, the worst is all four limbs, with respiratory insufficiency, as well.** **It’s like the old polio,”** Keith Van Haren, a pediatric neurologist at Lucile Packard Children’s Hospital in Palo Alto, California, told *USA* Today.

CNN reports that neurologists have identified five patients who have developed paralysis in one or more limbs between August 2012 and July 2013. All five children had been vaccinated against the poliovirus, and treatment did not help the children regain their motor function.

Scientists say that samples from two of the children **tested positive for enterovirus 68**, a rare virus linked in the past to severe respiratory illness. Dr. Emmanuelle Waubant, a neurologist at the University of California, San Francisco, told CNN that samples from the other three children were not collected or tested soon enough to offer conclusive results.

Waubant, who, with her colleagues, is planning to present a report about these patients’ illnesses at the annual meeting of the American Academy of Neurology in late April, said that health care providers should be on the lookout for similar cases and send her in samples from any patient exhibiting these symptoms.

Dr. Carol Glaser, chief of the Encephalitis and Special Investigation Section at the California Department of Public Health, told CNN that the state is aware of the paralysis cases but believes the risk to families is very low.

“We are evaluating cases as they are reported to us,” Glaser said. “We have not found anything at this point that raises any public health concerns.”

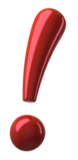
Experts note that the poliovirus has been eradicated in the United States for more than thirty years. The World Health Organization (WHO) says that only three countries in the world are not free of the disease: Afghanistan, Pakistan, and Nigeria. In these three states, Islamist militants disrupt polio vaccination campaign and kill NGO doctors who administer the vaccine, saying that the vaccination effort is a Western plot against Islam.

CDC reports that Enterovirus 68 was first identified in a California lab in 1962, after four children came down with a severe respiratory illness. **Only twenty-six cases of enterovirus 68 in the United States were reported to the CDC between 1970 and 2005.** Dr. Steven Oberste, chief of the Polio and Picornavirus Laboratory Branch at the CDC, told CNN that since 2000, the government agency has kept a closer watch and has seen forty-seven cases.

**CDC reports that more concerning to health officials is enterovirus 71,** which was discovered by the same California lab in 1969. The CDC report notes that there were several outbreaks of paralysis caused by enterovirus 71 in Europe in the 1960s and 1970s. In the late 1990s and early 2000s, fatal encephalitis was a big problem in Malaysia and Taiwan.

“Ever since then, the virus has circulated in high levels in Southeast Asia,” Oberste said.

**Between 1983 and 2005, 270 cases of enterovirus 71 were reported in the United States,** but they have not led to a larger outbreak despite the virus’s infectious nature.

“That’s the really odd thing,” Oberste said. “We see cases from time to time in the United States. Occasionally they’ll be severe. **Basically it’s identical to what’s circulating in Asia …** but it doesn’t cause the same big outbreak in disease. And we really don’t know why.”

Waubant and her colleagues stress they do not want to alarm anyone. “We would like to stress that this syndrome appears to be very, very rare,” one of Waubant’s colleagues, Dr. Keith Van Haren, said in a prepared statement.

|  |
| --- |
| Poliovirus is part of the Picornaviridae family, which also includes enteroviruses and rhinoviruses (better known as the common cold). There are more than 100 types of enterovirus that cause 10 million to 15 million infections in the United States each year, according to the Centers for Disease Control and Prevention.  Most people who become infected with an enterovirus do not get sick or experience only mild symptoms, said Dr. Steven Oberste, chief of the Polio and Picornavirus Laboratory Branch at the CDC. **Common symptoms** include fever, runny nose, cough, skin rash and body aches.  Enterovirus is often the cause of **"summer colds,"** whose cases spike in July, August and September. Children and teens are more likely to fall ill because they have not yet built up immunity to these common viruses.  However, some types of enterovirus are **more serious**. These can cause hand, foot and mouth disease; viral meningitis; encephalitis (inflammation of the brain); an infection of the heart; and paralysis in some patients. |

Real-time Public Health Modeling & Decision Support

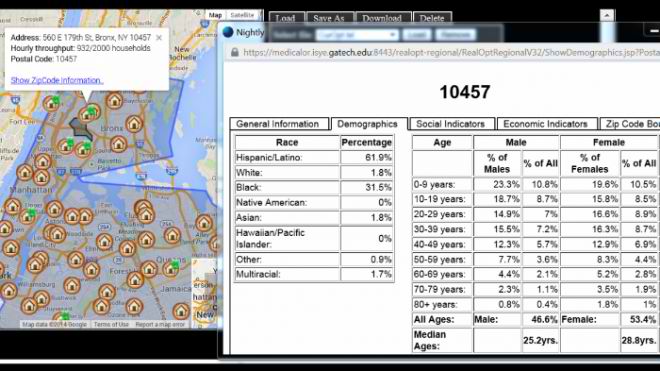
Source: http://www2.isye.gatech.edu/medicalor/realopt/index.php

The U.S. Centers for Disease Control and Prevention (CDC) has partnered with a research team at Georgia Institute of Technology to produce a modeling tool to help health personnel with the challenge of mass dispensing of medical supplies in an emergency. The software, known as RealOptC, has decision support capabilities for modeling and optimizing the public health infrastructure for hazardous emergency response.

**Use Case –** **Your city has 48 hours to vaccinate every man, woman and child to prevent a dangerous pandemic. Where do you put the clinics, how many health care workers will you need and how do you get 2 million people to a finite number of emergency clinics?**

Additional Information – The real-time capability of RealOptC means that users can enter different parameters into the system and obtain results very quickly. This rapid computational time of RealOptC facilitates analysis of "what-if" scenarios, thus it serves as an invaluable tool for planning and reconfigurations.

**RealOptC** is a software enterprise system developed by Dr. Eva Lee and her research team at the Center for Operations Research in Medicine and HealthCare, School of Industrial and Systems Engineering, Georgia Institute of Technology. RealOptC consists of various decision support capabilities for modeling and optimizing the public health infrastructure for **all hazard emergency response, and has been used in the areas of biological or radiological terrorism preparedness, infectious disease outbreaks planning, and natural disasters response.** The enterprise system consists of stand-alone software and decision support systems, including RealOpt-PODC, RealOpt-RegionalC, RealOpt-CRCC, RealOpt-RSSC, and RealOpt-evacuateC. An agent-based biosurveillance and disease mitigation module is integrated within the RealOpt-PODC and RealOpt-RegionalC systems.

The real-time capability of RealOptC means that users can enter different parameters into the system and obtain results very quickly. This rapid computational time of RealOptC facilitates analysis of "what-if" scenarios, thus it serves as an invaluable tool for planning and reconfigurations

.

►*Click on “download request” at the* ***main menu*** *to download certain components of the this very useful software.*

# Pfizer, MIT in 3-year collaboration focusing on biologics manufacturing

Source: http://www.biopharma-reporter.com/Bio-Developments/Pfizer-MIT-in-3-year-collaboration-focusing-on-biologics-manufacturing

#### Pfizer and MIT have announced a new three-year collaboration to advance biopharmaceutical discovery using synthetic biology.

The collaboration “*spans multiple therapeutic areas at Pfizer and involves several core investigators within the MIT Synthetic Biology Center*,” MIT spokesman Dan Darling told us. All financial terms are confidential.

Biologics based in recombinant DNA technology “*have transformed the treatment of many diseases over the last few decades.  However, the bio-manufacturing process can be time-consuming and costly, and has remained largely unchanged since the earliest product approvals*,” Darling said.

The hope is that new technologies can help lower the cost of producing some of the most complex biologically based drugs.

This is not the first partnership between Pfizer and MIT, but it is the first focused on developing a better way to manufacture drugs.

MIT’s biomanufacturing program also recently won a $10m US Defense contract. **The funding will be for building a new prototype biologic manufacturing system in two years.**

“*There is an opportunity to re-evaluate standard operations, identify areas for improvement, and develop methodologies that potentially may make the biopharmaceutical value chain more cost-efficient*,” Darling said.

**The goal of the Pfizer-MIT partnership is to improve the efficiency with which researchers are able to produce specific proteins synthetically by using these new technologies, which utilize more genes in the process — around 40 or 50 — versus just one, according to other media reports .**

“*We believe we are reaching a key inflection point where advances in synthetic biology have the potential to rapidly accelerate and improve biotherapeutics drug discovery and development*,” Darling added.

“*This includes early-stage candidate discovery through product supply, which could bring better, more effective therapies to patients more rapidly*.”

Doug Lauffenburger, head of MIT’s Department of Biological Engineering, added: “*This collaboration supports our goal to develop sophisticated synthetic biological systems from standardized, well-characterized modular parts for useful application in multiple fields, including biopharmaceutical molecular and bioprocess design*.”

# Quicker anthrax detection could save millions of dollars, speed bioterror response

Source: http://decodingscience.missouri.edu/2014/02/quicker-anthrax-detection-could-save-millions-of-dollars-speed-bioterror-response/

Imagine researchers in hazmat suits moving slowly and deliberately through a lab. One of them holds up a beaker. It’s glowing.

This light — or the absence of it — could save millions of dollars for governments and save the lives of anthrax victims.

**Scientists at the University of Missouri Laboratory of Infectious Disease Research proved a new method for anthrax detection can identify anthrax quicker than any existing approach.**

**When the “bioluminescent reporter phage” — an engineered virus — infects anthrax bacteria, it takes on a sci-fi-movie-type glow.**

George Stewart, a medical bacteriologist at MU’s Bond Life Sciences Center, and graduate student Krista Spreng, observed the virus against a variety of virulent strains of bacillus anthracis, the bacteria causing anthrax disease.

“For this technique, within a few hours, you’ll have a yes or no answer,” Stewart said.

The research, funded by the USDA, was published in the Journal of Microbiological Methods in Aug. 2013. David Schofield at Guild BioSciences, a biotech company in Charleston, S.C, created the reporter phage.

**This new method could save a significant amount of money associated with the decontamination of anthrax from suspected infected areas.**

**Expensive clean-up from the 2001 “Letter attacks”**

With the country on high-alert following Sept. 11, 2001, a slew of bioterrorists mailed anthrax letters, filled with a powder that if inhaled could cause death.

Numerous Post Offices and processing facilities were closed and quarantined.

**The clean-up bill for the 2001 Anthrax Letter attacks was $3.2 million,** according to a 2012 report in Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science.

Theoretically, the new detection method would alert of a negative result potentially five hours into clean-up efforts instead of two or three days into expensive decontaminating.

Current methods take anywhere from 24 hours or longer to produce a definitive answer for anthrax contamination.

**A five-hour benchmark**

Stewart said from contamination levels expected from a bioterrorism threat, **a positive answer could be found in five hours.** If contamination levels were higher, results would come back much more quickly.

Prior to this bioluminescent reporting phage, experts used techniques that were **culture based or PCR (polymerase chain reaction) based. Both methods, require additional time for a definitive answer, a minimum of 24 to 48 hours,** Stewart said.

“Normally to identify whether an organisms is present, you have to take the material culture, the organism and all the bacteria that might be present in the sample,” Stewart said. “You have to pick colonies that might be bacillus anthracis and do chemical testing which takes some time.”

From a bio-threat standpoint, breathing in anthrax, is the highest concern for public health and homeland security officials and has the highest fatality rate among forms of anthrax.

“If you have a situation and need a quick yes or no answer, this is a tool that will help that,” Stewart said.

Terrorists have used a powder form of anthrax, which has been slipped into letters of political persons and media. A person is infected when an anthrax spore gets into the blood system, most commonly through inhalation or an abrasion on the body, according to Centers of Disease Control and Prevention.

For low levels of contamination, the bioluminescent reporter phage would still detect the presence of the bacteria, but it would take longer.

“This method will be as quick as any of the others and quicker than most,” Stewart said.

**The bioluminescent-detection method can detect low levels of anthrax bacteria and rule out false positives. The added benefit to this reporting system is its ability to show that anthrax bacteria are present and it’s alive,** Stewart said.

**What’s next?**

The next step in the bioluminescent reporter phage is getting it approved so a product can be produced and branded. The agency that would warrant the stamp of approval would depend on the eventual use of the phage — food-related testing would likely go through the Food and Drug Administration, Stewart said.

When that happens, a product would not necessarily require a formal lab — it would need a place where cultures could grow at 37 degrees.

“Samples could be collected, brought back to the state public health lab for example and then the testing could be done within a few hours of the collection of the samples and you would have a result,” Stewart said.

The last anthrax attack was in 2001, but the possibility of one happening again, Stewart said, remains a driver for proactive research.

“In the years since the postal attacks, we haven’t had any bona fide anthrax attacks,” Stewart said. “That doesn’t mean it’s not going to happen — we have to be prepared for when it does occur again.”

## Positive safety results Marburg drug candidate announced

Source: http://www.homelandsecuritynewswire.com/dr20140228-positive-safety-results-marburg-drug-candidate-announced

Marburg hemorrhagic fever is a severe and potentially fatal disease in humans first recognized in 1967. It is caused by an RNA virus of the Filoviridae family and is understood to be endemic to Africa. The Marburg virus is classified as a Category A bioterrorism agent by the Centers for Disease Control and Prevention (CDC), and in 2006 was determined by DHS to be a material threat to national security and public health. **There are currently no treatments for Marburg virus infection beyond supportive care.** Cambridge, Massachusetts-based Sarepta Therapeutics, a developer of innovative RNA-based therapeutics, announced **positive safety results from a Phase I multiple ascending dose study of AVI-7288 in healthy volunteers**. AVI-7288 is the company’s lead drug candidate for the treatment of Marburg virus infection.

Cambridge, Massachusetts-based Sarepta Therapeutics, a developer of innovative RNA-based therapeutics, earlier this month announced positive safety results from a Phase I multiple ascending dose study of AVI-7288 in healthy volunteers. AVI-7288, which uses Sarepta’s proprietary PMOplus chemistry, is the company’s lead drug candidate for the treatment of Marburg virus infection. Sarepta has been developing AVI-7288 under a Department of Defense (DoD) contract managed by the Medical Countermeasure Systems BioDefense Therapeutics (MCS-BDTX) Joint Product Management Office.

The company says that the Phase I clinical study was a randomized, double-blind, placebo-controlled trial that enrolled forty healthy adult volunteers, and was designed to characterize the safety, tolerability, and pharmacokinetics of AVI-7288 after daily repeat dosing. In each of five cohorts, six subjects received AVI-7288 and two subjects received placebo, daily for fourteen days.

**Results showed that AVI-7288 was well tolerated through the highest dose tested, 16 mg/kg per day, which is higher than the anticipated therapeutic dose, with no reported serious or clinically significant adverse events.** An independent Data and Safety Monitoring Board reviewed blinded safety results from the study and recommended continued clinical development of AVI-7288.

“We are very encouraged by the AVI-7288 study results announced today,” said Chris Garabedian, president and chief executive officer of Sarepta Therapeutics. **“These safety data, combined with previously reported efficacy results showing up to 100 percent survival in infected animals, differentiates AVI-7288 as the most advanced medical countermeasure in development for the treatment of Marburg infection.”**

“The new data for AVI-7288 add to a growing body of evidence supporting the safety and activity of Sarepta’s PMO-based chemistries,” said Art Krieg, M.D., senior vice president and chief scientific officer of Sarepta Therapeutics. “Our proprietary RNA technologies offer a versatile drug development platform with broad potential utility across a spectrum of therapeutic areas.”

**The Marburg virus**

Marburg hemorrhagic fever is a severe and potentially fatal disease in humans first recognized in 1967. It is caused by an RNA virus of the Filoviridae family and is understood to be endemic to Africa. The Marburg virus is classified as a Category A bioterrorism agent by the Centers for Disease Control and Prevention (CDC), and in 2006 was determined by DHS to be a material threat to national security and public health. Onset of the disease is often sudden, and the symptoms include fever, chills, nausea, vomiting, chest pain, and diarrhea. Increasingly severe symptoms may also include massive hemorrhaging and multiple organ dysfunctions. There are currently no treatments for Marburg virus infection beyond supportive care.

# 14 lab workers had orthopoxvirus infections in past decade

Source: http://www.cidrap.umn.edu/news-perspective/2014/02/cdc-14-lab-workers-had-orthopoxvirus-infections-past-decade

At least 14 US laboratory workers contracted vaccinia or cowpox virus infections from on-the-job exposures in the past decade, a Centers for Disease Control and Prevention (CDC) official reported at a federal advisory committee meeting yesterday.

Speaking to the Advisory Committee on Immunization Practices (ACIP), Brett Petersen, MD, said **26 lab-worker exposures to orthopoxviruses have been reported to the CDC since 2004, and 14 (54%) of those resulted in infections. Four of the workers had to be hospitalized, he said.**

**Twelve (86%) of the 14 infections involved vacinnia virus and 2 (14%) involved cowpox virus,** said Petersen, who is a medical officer in the CDC's Poxvirus and Rabies Branch.

**In 4 of the 14 cases (29%), he added, "It was found that the strain . . . was other than the one the researcher thought they were working with," which demonstrates the uncertainty of the risks. He also noted that 18 of the 26 exposures involved recombinant viruses.**

The information represents only the cases that were reported to the CDC or in the literature and therefore probably does not cover all those that have occurred, Petersen told CIDRAP News today.

Vaccinia virus, the active ingredient in smallpox vaccine, is used in laboratory research for such purposes as expressing genes from other organisms, Petersen noted at the meeting.

### Smallpox vaccination

Because of the risk of infection for lab workers, the ACIP in 2001 recommended smallpox (vaccinia) vaccination for lab workers who handle cultures or animals contaminated with vaccinia virus that is not highly attenuated, Petersen explained.

**He reported that 7 of the 26 reported exposures involved workers who had been vaccinated in accordance with ACIP recommendations, and only 1 of those 7 became infected.**

ACIP member Lee Harrison, MD, who chairs the ACIP's smallpox vaccine work group, said the smallpox vaccine protects against all orthopoxviruses, including vaccinia. He said the work group was set up last year to review the requirements for working with orthopoxviruses.

Harrison, a professor of medicine and epidemiology at the University of Pittsburgh, said the review is deemed necessary because the ACIP has not updated its recommendations since 2003. In 2007, the smallpox vaccine ACAM2000 was licensed, and it has since replaced the Dryvax vaccine in the US national stockpile.

Petersen said the CDC is comparing data on ACAM2000 and Dryvax to assess whether ACAM2000 should be routinely recommended for persons at risk for orthopoxvirus infections. He said the smallpox vaccine work group hopes to present updated recommendations at a future ACIP meeting.

# 30,000-year-old giant virus 'comes back to life'

Source: http://www.bbc.com/news/science-environment-26387276

**An ancient virus has "come back to life" after lying dormant for at least 30,000 years, scientists say.**

**It was found frozen in a deep layer of the Siberian permafrost, but after it thawed it became infectious once again.**

The French scientists say the contagion poses no danger to humans or animals, but other viruses could be unleashed as the ground becomes exposed.

The study is published in the Proceedings of the National Academy of Sciences (PNAS).

Professor Jean-Michel Claverie, from the National Centre of Scientific Research (CNRS) at the University of Aix-Marseille in France, said: "This is the first time we've seen a virus that's still infectious after this length of time."

**Biggest virus**

**The ancient pathogen was discovered buried 30m (100ft) down in the frozen ground.**

**Called Pithovirus sibericum, it belongs to a class of giant viruses that were discovered 10 years ago.**

These are all so large that, unlike other viruses, they **can be seen under a microscope.** And this one, measuring 1.5 micrometres in length, is the biggest that has ever been found.

The last time it infected anything was more than 30,000 years ago, but in the laboratory it has sprung to life once again.

Tests show that it attacks amoebas, which are single-celled organisms, but does not infect humans or other animals.

Co-author Dr Chantal Abergel, also from the CNRS, said: "It comes into the cell, multiplies and finally kills the cell. It is able to kill the amoeba - but it won't infect a human cell."

However, the researchers believe that other more deadly pathogens could be locked in Siberia's permafrost.

"We are addressing this issue by sequencing the DNA that is present in those layers," said Dr Abergel.

"This would be the best way to work out what is dangerous in there."

**'Recipe for disaster'**

The researchers say this region is under threat. Since the 1970s, the permafrost has retreated and reduced in thickness, and climate change projections suggest it will decrease further.

It has also become more accessible, and is being eyed for its natural resources.

**Prof Claverie warns that exposing the deep layers could expose new viral threats.**

He said: "It is a recipe for disaster. If you start having industrial explorations, people will start to move around the deep permafrost layers. Through mining and drilling, those old layers will be penetrated and this is where the danger is coming from."

He told BBC News that ancient strains of the smallpox virus, which was declared eradicated 30 years ago, could pose a risk.

"If it is true that these viruses survive in the same way those amoeba viruses survive, then smallpox is not eradicated from the planet - only the surface," he said.

**"By going deeper we may reactivate the possibility that smallpox could become again a disease of humans in modern times."**

However, it is not yet clear whether all viruses could become active again after being frozen for thousands or even millions of years.

"That's the six million dollar question," said Professor Jonathan Ball, a virologist from the University of Nottingham, who was commenting on the research.

"Finding a virus still capable of infecting its host after such a long time is still pretty astounding - but just how long other viruses could remain viable in permafrost is anyone's guess. It will depend a lot on the actual virus. I doubt they are all as robust as this one."

He added: "We freeze viruses in the laboratory to preserve them for the future. If they have a lipid envelope - like flu or HIV, for example - then they are a bit more fragile, but the viruses with an external protein shell - like foot and mouth and common cold viruses - survive better.

"But it's the freezing-thawing that poses the problems, because as the ice forms then melts there's a physical damaging effect. If they do survive this, then they need to find a host to infect and they need to find them pretty fast."

# Pakistani polio strain threatens global campaign

Source: http://timesofindia.indiatimes.com/world/pakistan/Pakistani-polio-strain-threatens-global-campaign/articleshow/31412318.cms

Just a few weeks ago, 11-month-old Shaista was pulling herself up, giggling as she took her first wobbly steps with the helping hand of her teenage mother.

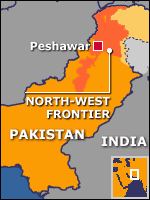
Then the polio virus struck and Shaista was no longer able to stand, her legs buckling beneath her weight. Today, her mother cries a lot and wonders what will become of her daughter in Pakistan's male-dominated society, where a woman's value is often measured by the quality of her husband.

"It is not a hardship just for the child, but for the whole family," said the child's 18-year-old mother, Samia Gul. "It is very difficult for a poor family like us. She will be dependent on us for the rest of her life."

Shaista is one of five new polio cases to surface in Pakistan in just the first month of this year. **Last year, Pakistan recorded 92 new cases, beating Nigeria and Afghanistan — the only other polio-endemic countries — by almost 2 to 1, the World Health Organization said.**

Pakistan's beleaguered battle to eradicate polio is threatening a global, multi-billion-dollar campaign to wipe out the disease worldwide. Because of Pakistan, the virus is spreading to countries that were previously polio-free, UN officials say.

**"The largest polio virus reservoir of the world," is in Peshawar, in northwestern Pakistan near the border with Afghanistan, according to WHO.**

Shaista and her parents share a two-room mud house with a couple of goats, a half-dozen squawking chickens and 10 other relatives in Pakistan's western Khyber Pukhtunkhwa, or KPK, province, where Islamic militants often gun down health workers distributing vaccines and send suicide bombers to blow up police vehicles that protect them.

The latest casualty was a police constable killed on Tuesday protecting a team of vaccination workers in northwest Pakistan. **During a two-day vaccination campaign in Peshawar earlier this month, 5,000 police were deployed to protect health workers, most of whom earn barely $2 a day.**

Fresh cases of polio — traced through genetic sequencing to the Pakistani strain of the disease — are showing up in countries that were previously polio-free, including Syria and Egypt, as well as in the Gaza Strip, said Ban Khalid Al-Dhayi, the spokeswoman for UNICEF in Pakistan. Unicef is tasked with persuading a reluctant tribal population that lives along Pakistan's border with Afghanistan — perhaps one of the most dangerous places on the planet — to vaccinate their children.

"A lot of countries that spent so much money and resources eradicating polio are worried," Al-Dhayi said in an interview.

Pakistan's neighbours are particularly vulnerable.

The same genetic sequencing found that 12 of the last 13 new polio cases in Afghanistan originated in Pakistan. Just last week, a 3-year-old was diagnosed with polio in the Afghan capital of Kabul, the first case since 2001.

**Neighbour India, with a population of 1.2 billion, has been polio-free for three years.** Fearful that Pakistan could wipe out that achievement, India is demanding that Pakistani visitors provide proof of vaccination.   
It wasn't so long ago — 1988 — that more than 350,000 people, most of them children under 5, were afflicted by polio in 125 countries where the disease was endemic. Today the disease is endemic in only three.   
Last year, the Bill and Melinda Gates Foundation, a multi-billion-dollar charity that funds polio vaccinations, vowed to wipe out the crippling disease by 2018.

Underlining the danger that Pakistan poses to achieving that goal, Al-Dhayi said **there are 350,000 Pakistani children in just one small area of the country who have not been vaccinated — and it takes only one child left unvaccinated to reverse global gains against the disease.**

The area — North and South Waziristan — is too dangerous for health workers to venture. Islamic militants, many with ties to al-Qaida, banned polio vaccinations there in 2012 to press their demand that the United States end its use of drones to target their hideouts.

Militants have also created suspicion among ultraconservative parents in Pakistan's deeply religious northwest, saying the polio vaccine will make their children impotent. The vaccine, they claim, is a ploy by the West to limit the world's Muslim population.

But health workers and militants alike agree the biggest setback was the highly publicized use of a Pakistani doctor and a vaccination ruse to ferret out al-Qaida chief Osama bin Laden in May 2011. Dr Shakil Afridi is in jail in Pakistan for his role in the CIA operation that uncovered bin Laden's hideout in the northwestern city of Abbottabad, 60 miles (100 kilometres) from the capital, Islamabad.

While Afridi never got DNA samples from the bin Laden family, his involvement in the covert operation that led to bin Laden's death caused residents to look with suspicion on many vaccination programs. Devastating for the polio campaign were the images of Afridi standing beside a banner promoting polio vaccinations as television commentators told of his collusion with the CIA.

"We have deep sensitivity about the polio vaccination after the martyrdom of the great mujahed and leader of Muslims, Sheikh Osama bin Laden," Taliban spokesman Ehsanullah Ehsan told The Associated Press. "We still have strong suspicions that the vaccination campaign could be used again and again to spy on Muslims and the mujahedeen."

The ruse also turned the polio campaign violent. The first attack against a health worker occurred in June 2012, said Dr Imtiaz Ali Shah, the KPK provincial government polio campaign coordinator. Since then, 40 people participating in vaccination campaigns have been killed in Pakistan and another 39 injured, according to UNICEF figures.

"Before 2011, we never saw health workers being attacked," he said. "Now there are parts of Pakistan that are so volatile that vaccinators can't go there."

Mohammad Wasil's 19-year-old son, Hilal, was killed by militants as he vaccinated children in rural northwest Pakistan. Sitting on a bed made of rope in his village, where women are rarely seen without the all-enveloping burqa, Wasil said his son volunteered because he loved children and wanted to earn money for his education.

Still, there have been small gains. **In 2012, new polio cases in northwest Pakistan were found in 13 districts; a year later, that was reduced to six districts.** But the virus is stubborn, and in the provincial capital of Peshawar, it keeps reappearing, forcing tens of thousands of children to be revaccinated because they may not have built up enough immunity.

"That makes everyone suspicious," said Al-Dhayi, the UNICEF spokeswoman. "They wonder whether there was something wrong with the vaccine or with the new vaccination being administered."

It has been impossible to eradicate the polio virus from Peshawar, says Shah, because people from the heavily infected tribal regions that are off limits for health workers arrive daily in the city, bringing with them a fresh outbreak.

The tribal regions "are producing so many cases and the (tribal people) travel regularly", he said.

Al-Dhayi said some of the new polio cases showing up elsewhere in Pakistan have also been tracked to Peshawar and other areas of northwest KPK province.

In the meantime, UNICEF is trying to get Pakistan's senior Islamic clergy to support the polio campaign, with some success, according to Al-Dhayi. Among those recruited is the so-called father of Afghanistan's Taliban movement, Maulana Sami-ul-Haq.

"The effort is really intensive and proving positive," she said, but the clock is ticking. "Pakistan is the worst of the three (polio-endemic countries) in terms of the number of cases and the complexity."

# DARPA Advances Laser Technology for Chem-Bio Detection

Source: http://globalbiodefense.com/2014/03/05/darpa-advances-laser-technology-for-chem-bio-detection/

A new Defense Advanced Research Projects Agency (DARPA) program seeks technology that may make ultraviolet-based laser detection equipment for chemical and biological defense more readily available in the field.

Raman spectroscopy uses lasers to measure molecular vibrations to quickly and accurately identify unknown substances. Ultraviolet lasers have the optimal wavelength for Raman spectroscopy at stand-off distances, but the DoD’s current UV-based tactical detection systems are large and expensive and have limited functionality.

**DARPA’s Laser UV Sources for Tactical Efficient Raman (LUSTER) program seeks proposals for compact, efficient and low-cost deep-UV lasers for highly deployable biological and chemical agent detection.** The goal is to create a new class of UV lasers that are more than 300 times smaller than current lasers and 10 times more efficient. The resulting technology could be dropped into current detection systems to save size, weight and power (SWaP) or to create new systems that are smaller and more sensitive.

“Today’s standoff detection systems are so large and heavy that trucks are required to move them,” said Dan Green, DARPA program manager. “LUSTER seeks to develop new laser sources for breakthrough chemical and biological agent detection systems that are compact and light enough to be carried by an individual, while being more efficient than today’s systems. We also want to take a couple of zeroes off the price tag.”

**DARPA hopes LUSTER can build on the accomplishments from the recently completed Compact Mid-Ultraviolet Technology (CMUVT) program.** CMUVT developed record high-power UV light emitting diodes (LEDs) with high efficiencies and wavelengths approaching those sought under LUSTER. LEDs, however, have limited sensitivity, which is required for discriminating among compounds. LUSTER seeks to develop a new laser technology that has the accuracy of today’s expensive lasers but with the low cost and high reliability of LEDs.

“In addition to detecting chemical and biological agents in the field—or at home to protect against mass terror attacks—UV lasers have many other uses,” said Green. “The new class of UV lasers envisioned from the LUSTER program is expected to impact a broad range of applications such as point-of-need medical diagnostics, advanced manufacturing and compact atomic clocks.”

**LUSTER plans to consider a variety of technical approaches, as long as they operate within a 220-240 nanometer wavelength (deep UV) and have greater than 1 watt power production, wall-plug efficiencies greater than 10 percent and line widths less than 0.01 nanometers.**

|  |
| --- |
| Compact Mid-Ultraviolet Technology (CMUVT) Warfighters need to be able to detect and identify biological and chemical agents that may be in use by enemy forces. Current detection methods require large, heavy equipment, and a great deal of power. To address these deficiencies, the Compact Mid-Ultraviolet Technology (CMUVT) program is developing the essential heteroepitaxy, waveguides, cavities, contacts, and micro/nanostructures necessary to enable efficient LEDs and chip-scale semiconductor lasers operating at wavelengths below 275 nm.  http://www.darpa.mil/uploadedImages/Content/Our_Work/MTO/Programs/Compact_Mid-Ultraviolet_Technology/CMUVT_3_SET.JPGThe middle ultraviolet (UV) spectral region (200-300 nm) is of significant interest to DoD for applications involving detection, identification and decontamination of biological and chemical agents. Amino acids and many other common biological molecules are absorbing at these wavelengths, and the resulting near UV (300-400 nm) and visible fluorescence can signal their presence and aid in their identification in aerosol clouds, liquid suspensions or powders. Spectroscopic identification via Raman scattering is enhanced for excitation in the mid-UV because the Raman cross section is increased several orders of magnitude, and there is little to no fluorescence background at these wavelengths to obscure the scattered signal. Many absorption bands also exist at these wavelengths to increase the efficacy of intense UV irradiation for sterilization and chemical decontamination.  Mature laser and detector technologies exist in the mid-UV. Large excimer lasers, such as KrF (248 nm), are common tools for lithography. A small Q-switched laser with 4th harmonic generation and a photomultiplier tube are currently used in company- and battalion-level chem/bio detection systems, such as the Joint Biological Point Detection System. However, all these systems are too heavy, fragile and expensive for widespread expeditionary deployment at levels from platoons down to the individual warfighter. Realizing semiconductor solutions for bright, efficient light-emitting diodes (LEDs) and lasers across the mid-UV wavelength regime will provide the critical path to compact future systems.  CMUVT will pursue two primary tracks targeting LEDs at 250-275 nm with an output of 100 mW with 20 percent wall-plug efficiency and lasers producing 10 mW between 220 and 250 nm without nonlinear frequency conversion. A secondary effort will investigate bulk AlN substrates. The majority of the program will address the fundamental material and device challenges that currently limit the performance of group III-nitride-based semiconductor devices in the mid-UV. The resulting UV components will significantly improve the size, weight, power, and capability of chemical/biological-agent detectors, portable water purification illuminators and other UV-dependent applications of commercial interest. |

# White Powder in Letters Puts Hong Kong on Edge

Source:http://online.wsj.com/news/articles/SB10001424052702304585004579419120158519350?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB100014240527023045850045794 19120158519350.html

Hong Kong was briefly shaken on Tuesday after **suspicious-looking letters containing white powder were sent to nearly a dozen recipients.**

The recipients included four media outlets, a government office, two financial institutions in the city's center and other addressees in Hong Kong's Western and Wan Chai districts, police said.

Dozens of police fanned out across the city in response to the letters, along with bomb-disposal agents, recipients said.

**Subsequent testing indicated that the powder was corn flour, rather than anthrax or other harmful biochemical substances as initially feared, police said.**

The content of the letters pertained to complaints about investment services, police said, without naming recipients or providing further details.

Hong Kong has seen several similar incidents involving disgruntled investors who have sent letters containing corn flour, monosodium glutamate and other substances to financial institutions including the Bank of China and the city's monetary authority, as well as various media outlets.

The incident struck a nerve in a city where last week a former editor at a Hong Kong daily newspaper was stabbed on the street, sparking fears that he may have been targeted for his work at the paper.

On Sunday, thousands of people marched in support of media freedom and Kevin Lau, editor of the Chinese-language daily Ming Pao before his dismissal in January.

No arrests in this week's cases have been made. The police are investigating whether Tuesday's incidents have any connection to a similar series of letters mailed to various addresses late last year, a spokesman said.

### Saudi Arabia reports two MERS cases, one fatal

Source: http://www.cidrap.umn.edu/news-perspective/2014/03/news-scan-mar-05-2014

Saudi Arabia's Ministry of Health (MOH) announced two new Middle East respiratory syndrome coronavirus (MERS-CoV) infections today, one of them fatal.

Few details were available about the patients, according to a statement in Arabic posted on the MOH Web site. Both of them are from Riyadh. One is a 55-year-old man with a chronic health condition who died from his infection, and the other is a 51-year-old man who also suffers from an underlying condition and is hospitalized in an intensive care unit.

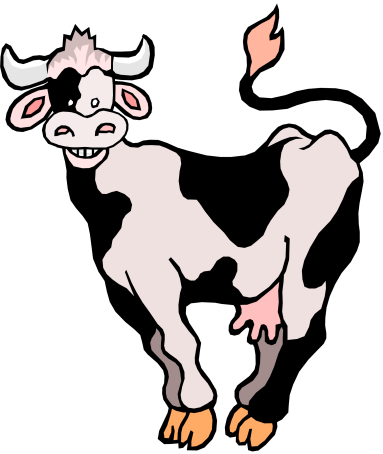
No other details were posted, such as any possible exposure to animals.

**The two new cases bump Saudi Arabia's MERS total to 150 cases, of which 62 were fatal.** The country has by far the most cases of any nation reporting infections.

So far the World Health Organization (WHO) has yet to confirm three previous cases reported recently by Saudi Arabia. They involve a 56-year-old woman from Riyadh, a 58-year-old man from Al-Ahsa, and an 81-year-old woman from Riyadh who died. **The agency's latest MERS count, updated Feb 28, is 184 cases, including 80 deaths.**

### vCJD blood test accurate enough for large-scale screening

Source: http://www.cidrap.umn.edu/news-perspective/2014/03/news-scan-mar-05-2014

**In a large trial, a test to detect the abnormal prion protein associated with variant Creutzfeldt-Jakob disease (vCJD) performed well enough to conclude that it can be used to screen populations at risk for the disease,** scientists reported in JAMA Neurology.

Variant CJD, a degenerative brain disease, is the human counterpart of bovine spongiform encephalopathy (BSE, or mad cow disease), which, the report notes, may have infected as many as 3 million cattle in the United Kingdom.

The authors, led by Graham S. Jackson, PhD, of the University College of London Institute of Neurology, used the test on blood samples from 5,000 US blood donors, 200 healthy British donors, 352 patients with nonprion neurodegenerative diseases, 105 patients deemed likely to have prion diseases, and 10 patients with confirmed vCJD.

**The test showed 100% specificity** (no false-positives) in the US donors (who were presumed to be free of prion disease) and in the healthy British donors. Likewise, it produced **no false-positives** among the patients with nonprion neurodegenerative diseases.

Among patients believed likely to have a prion disease, two who had sporadic CJD tested positive (98.1% specificity; 95% confidence interval [CI], 93.3% to 99.8%). And in a small set of samples from unaffected persons and patients known to have vCJD, the test showed 70% sensitivity (95% CI, 34.8% to 93.3%), which reconfirmed previous findings.

The authors said the test performed well enough to justify using it to screen a large sample of the British population and at-risk groups to estimate the prevalence of blood prions among British blood donors. Such an estimate would help policy makers decide whether routine vCJD screening is needed for blood, tissue, and organ donations and for patients facing high-risk surgical procedures.

Assessment of the bio-preparedness and of the training of the French hospital laboratories in the event of biological threat

**By A Mérens, J D Cavallo, F Thibault, F Salicis, J F Munoz, R Courcol and P Binder**

*Eurosurveillance, Volume 17, Issue 45, 08 November 2012*

Source: http://www.eurosurveillance.org/ViewArticle.aspx?ArticleId=20312

**A national laboratory network ‘Biotox-Piratox’ was created in 2003 in France with the purpose of detecting, confirming and reporting potential biological and chemical threat agents. This network is divided into three levels: Level 1 is dedicated to the evaluation of risks (biological, chemical, radiological), to sampling and packing. Level 2 consists of university and military hospitals, who deal with biological specimens, and of environmental and veterinary laboratories, who deal with environmental and animal samples. Level 3 comprises national reference laboratories and the Jean Mérieux biosafety level (BSL)-4 laboratory in Lyon. This report presents the results of four bio-preparedness exercises to check critical points in the processing of samples. These exercises took place in 2007, 2009, 2010 and 2011. Each of them consisted of two parts. The first part was the identification of an unknown bacterial strain and its susceptibility to antibiotics used as a default in case of a bioterrorist event. The second part was the detection of Class III microorganisms, mainly by molecular techniques. The main lesson learnt in these exercises was that the key to successful detection of biological agents in case of a biological threat was standardisation and validation of the methods implemented by all the laboratories belonging to the network.**

**…**

The **conclusion** that can be drawn from these exercises is that the key to successful detection of biological agents in case of a biological threat is the training of the laboratory personnel (microbiologists and technicians) dealing with class III organisms as well as the standardisation and validation of methods implemented by all laboratories of the network. This last point was exemplified during the third exercise for molecular methods. However, the French Biotox-Piratox laboratory network is a network of networks. Thus it is not possible or realistic to force all laboratories to use identical equipment or techniques. Nevertheless, it is important to provide specific guidelines to all laboratories involved in the network. The publication of such guidelines for biological specimens is in progress. Moreover, administrative procedures should be adapted to accommodate for national exercises.

►**You can read the full paper at source’s URL.**

## Synthetic biology makes bioweapons easier to make

Source: http://www.homelandsecuritynewswire.com/dr20140317-synthetic-biology-makes-bioweapons-easier-to-make

Scientists and policy makers are no longer unconditionally promoting scientific innovation for fear that current and future biological breakthroughs may lead to dangerous applications. **The increasing use of biological engineering for commercial purposes beyond medicine has generated wealth, inspiring individuals in the form of DIYbio (a network of biohackers, amateur biologists, and do-it-yourself biological engineers) to embark on future biological discoveries.**

**CBRNePortal** notes that traditionally, government-backed institutions and pharmaceutical firms fueled biological innovation, but today, the barriers that limited innovation to those institutions are diminishing. The low cost and significantly reduced level of necessary expertise have provided anyone interested in developing biological technology the tools to engage in the practice, anyone including terrorist organizations. San-Diego-based Illumina recently announced its ability to sequence a human genome for $1,000. The implications for terrorism, according to CBRNePortal, are that “the emergence of synthetic biology and DIYbio has increased the likelihood that Al Qaeda will succeed in developing biological WMDs”.

Synthetic biology, the design and engineering of biological devices and systems, has given terrorists the capability to launch attacks using synthetic organisms without detection. CBRNePortal notes that terror groups favor biological weapons because they are “difficult to detect and difficult to attribute without a specific perpetrator claiming responsibility.”

So far, the use of bioweapons by terrorists has been infrequent. Of the more than 113,000 terrorists attacks recorded globally since 1971, only thirty-three have been biological. Seventeen recorded biological attacks occurred during 2001, ten occurred before 2001, and six biological attacks have occurred since 2002 (not counting the most recent Ricin attacks). Bioterrorism has been an uncommon terrorist weapon due to the technical complexity and financial resources required, but as technical complexity diminishes and terrorist organizations increase their investment in bioterrorism capabilities, the potential for large-scale bioterror attacks will increase.

The al-Qaeda network has called for the development of biological WMDs because such weapons have the potential to cause the greatest harm. CBRNePortal reports that before the Afghanistan invasion, al-Qaeda had invested in a bio-laboratory and began recruiting scientists. Thirteen years later, al-Qaeda continues to invest in biological weapons. Last year the New York Times reported on al-Qaeda’s experimentation with ricin production.

Making an effective biological weapon is not easy, and it still requires expertise and financial resources; but these barriers are steadily becoming less difficult to overcome. The international community must thus more urgently develop policies to prevent dangerous applications of synthetic biology. The Biological Weapons Convention prohibits the production of an entire category of WMDs by nation-states, but there is a need to put more effort into preventing non-state actors from developing the capabilities to do so. CBRNePortal notes that “a successful attack with a potent biological weapon, where no pharmaceutical interventions might exist, will be deadly and the impact of such an attack will reverberate around the globe because biological weapons are not bound by international borders.”

# Bioterrorism Simulations Educate Unprepared Healthcare Workers

Source: http://guardianlv.com/2014/03/bioterrorism-simulations-educate-unprepared-healthcare-workers/

Simulated exercises of bioterrorism events are now being used to educate and build confidence in healthcare workers. **Multiple evaluations have thus far found many doctors and nurses do not feel ready to handle a bioterrorism event**. Therefore it is hoped that these hands-on simulations will educate and prepare healthcare workers on how to handle a public health emergency of the kind that would be caused by a bioterrorist attack.

Bioterrorism refers to the deliberate dissemination of disease-causing pathogens for the purposes of causing illness or death. The Center for Disease Control classifies bacteria, fungi, and viruses as potential bioterrorist agents based upon four factors: the mortality rates, ease of person-to-person transmission, whether or not special action from health institutions would be required, and the estimated panic and the disturbance that an outbreak would instill in the public.

The CDC currently lists 45 different pathogens that could be potentially used as a bioterrorist weapon. These agents include anthrax, botulism, small pox, and the plague.

Numerous studies have indicated the healthcare workers do not feel adequately prepared to handle a bioterrorism event. **A 2009 study from Yale indicated that 71 percent of physicians said that they did not feel confident in their abilities to recognize weaponized pathogens. Other reports note that in particular older practitioners, doctors in rural areas, and surgeons have had little to no training in these matters. Another 2012 study also found that nurses similarly lack confidence in how to manage a bioterrorist attack.**

In an effort to better prepare healthcare workers as to how to handle a bioterrorist attack, institutions are developing hands-on training programs to better educate their personnel. **Such training programs use simulated patients that require a diagnosis and a specific treatment plan.** Though medical students reported these exercises to be highly informative and valuable, collectively they were unable to correctly initiate standard protocol measures such as having themselves and the patient take respiratory precautions (e.g. face masks). However in discussions after the simulation, students reported that they felt more confident in how to deal with a bioterrorism attack and that they would be more likely to take respiratory precautions and other safety measures with their real patients.

One of the difficulties that health care workers face in dealing with a bioterrorist attack is that the weaponized agent may not resemble commonly-found disease pathogens. For example, the bacteria *Yersinia pestis* can cause at least three different disease variations commonly referred to as “the plague.” **Plague variations are not commonly encountered in day-to-day hospital activities, and it is possible that a patient who initially presents with the characteristic fever, coughing, nausea, and/or vomiting, might be misdiagnosed for any number of other afflictions.** In addition, it is speculated that a deliberately weaponized variation of the plague might result in extremely rare variations such as pharyngeal plague or ocular plague. The last person-to-person transmission of the plague in the United States was reportedly in 1925. Consequently, doctors have little or no experience with the pathogen, and would be unlikely to immediately make the correct diagnosis. **This is especially troubling because *Yersinia pestis* causes a rapid decline in patient health and the mortality rate is quite high if treatment is not administered in 24 hours.**

Hopefully these simulated exercises will adequately educate healthcare workers as to how to handle a bioterrorism event. Already heralded as an improvement over traditional lecture-based information sessions, in the future researchers and administrators might try to expand this kind of training to address other disaster scenarios.

## Microbial detection array detects plague in ancient human remains

Source: http://www.homelandsecuritynewswire.com/dr20140320-microbial-detection-array-detects-plague-in-ancient-human-remains

Scientists who study past pandemics, such as the fourteenth century Black Death which devastated much of Europe, might soon be turning to an innovative biological detection technology for some extra help.

**The apparent first use of this technology, known as a microarray, for studying pathogens from ancient DNA, was reported today by a team of scientists in Scientific Reports.**

An LLNL release reports that researchers at McMaster University, led by Hendrik Poinar, an associate professor of evolutionary genetics, and Lawrence Livermore National Laboratory (LLNL) tested the application of a novel microarray, the Lawrence Livermore Microbial Detection Array (LLMDA), to identify human bacterial pathogens from archaeological remains. The team tested two samples that had been previously verified as containing pathogens through another technology.

One of the samples, an intestinal substance, showed the presence of cholera and was preserved from a patient who died from the disease during an 1849 outbreak in Philadelphia. The specimen was provided by the Philadelphia-based Mütter Museum.

The other sample tested with the LLMDA indicated the presence of Yersinia pestis (or plague) in a medieval tooth from 1348 from the East Smithfield burial ground in London. An estimated 30 to 50 percent of the European population succumbed to plague from 1347 to 1351.

Both Poinar and LLNL biologist Crystal Jaing believe that the Lab’s LLMDA technology will be tenfold faster and tenfold less expensive than current genomic sequencing as a means of studying pathogens in ancient DNA.

“Microarrays may be a potential alternative solution, as well as a complementary tool, to genomic sequencing for studying ancient DNA,” Jaing said. “It offers a faster and cheaper approach to studying complex samples.”

Poinar, who is an expert on ancient DNA, agreed.

“We know that most bacterial pathogens likely go undetected in ancient remains due to the overwhelmingly strong contaminant signal from molecules that don’t originate in human organs. One way to access this information would be to sequence everything in the sample and analyze it. But this is prohibitively costly and requires a lot of bioinformatics time.

“The LLMDA selectively targets pathogens that are likely to be of interest from an evolutionary standpoint and appears to work well with heavily degraded DNA, typical of most fossil and archival remains, so this is an excellent tool,” Poinar continued.

Scientists studying the origins of infectious disease and population health over time normally find that ancient human remains contain highly degraded DNA in which the pathogen represents only a tiny fraction of the total DNA yield.

Ancient pathogen DNA is heavily mixed with other human and environmental DNA. Lengths of these fragments are often as small as 30 to 50 bases compared with regular DNA fragments that are hundreds to thousands of bases long. The **amounts of pathogen in the two samples tested with the LLMDA were three ten-thousandths of the total sample for cholera and eight ten-thousandths for Y. pestis.**

“We found other pathogens in the chlorea and Y. pestis ancient DNA samples,” Jaing said, noting that tetanus was found along with Y. pestis.

The release notes that beyond showing the potential for microarrays to become a useful screening tool for archaeological samples, the team’s findings demonstrate that the LLMDA can identify primary and/or co-infecting bacterial pathogens in ancient samples.

Developed in early 2008, **the LLMDA permits the detection of any virus or bacteria that has been sequenced and included among the instrument’s 135,000 probes — on a one-inch wide, three-inch long glass slide — within 24 hours.** The LLMDA version run for the cholera and Y. pestis tests could detect about 1,850 viruses and about 1,400 bacteria.

While the Livermore instrument has previously been used to analyze the purity of infant vaccines, human clinical samples and diseased animals, it had not been deployed to study ancient pathogen DNA until this collaboration.

In Jaing’s view, the value of studying ancient human remains for infectious disease is that the research can offer clues as to how past pandemics happened and why they were so deadly.

“By looking at differences between modern DNA and ancient DNA, we may be able to better understand the evolution of diseases and that could help us better understand future disease outbreaks.”

She noted that she believes the use of microarrays will speed up the discovery and identification of pathogens from ancient human remains.

“The LLMDA could serve as an excellent screening tool to rapidly identify pathogens. Then genomic sequencing could be used to provide detailed genetic comparison.”

Genomic sequencing is the process of determining the precise order of the four different DNA bases — adenine, guanine, cytosine and thymine — within a cell of anything from bacteria to plants to animals.

Two other institutions participated in the research — the College of Physicians of Philadelphia (Mutter Museum) and the University of South Carolina.

“This collaboration has gone very well,” Jaing said. “Our groups have complementary skills and expertise. Hendrik’s group is a leader in biological archaeology and in analyzing ancient DNA. The LLNL team has expertise in microarrays, pathogen detection and bioinformatics.”

*— Read more in Alison M. Devault et al., “Ancient pathogen DNA in archaeological samples detected with a Microbial Detection Array,”* Scientific Reports *4, article number: 4245 (6 March 2014)*

# The Only Thing Scarier Than Bio-Warfare is the Antidote

Source: http://mag.newsweek.com/2014/03/21/bioerror-bio-error-labs-bio-warfare-bioterror.html

**As poorly regulated labs race to find the next antidote, bio-error may be more likely to cause an epidemic than bio-terror.**

It was spring 1979 in Sverdlovsk, Russia, a large industrial city straddling the border of Europe and Asia in what was then the Soviet Union. Without warning, 96 residents became ill, with symptoms similar to a severe flu: fever and chills, sore throat and headaches, with some nausea and vomiting. Just the usual one-week flu...except in this case, many of the people who got sick-at least 64-died within six weeks.

In the months following this alarming turn, Soviet medical, veterinary and legal journals all attributed the illnesses to an outbreak of anthrax originating in livestock raised south of the city. Government officials concurred, announcing that anyone who had contracted anthrax either ate contaminated meat or handled animals infected with the disease (the bacteria cannot be spread from person to person).

Anthrax, however, rarely appears out of thin air, and in the West speculation grew about a cover-up. The U.S. Department of Defense and the Central Intelligence Agency believed the anthrax infections stemmed from a biological weapons laboratory the Soviet Union had built in the city—implicitly accusing the Kremlin of violating the Biological Weapons Convention signed in 1972. In turn, the Soviets denied conducting biological weapons activities and scrambled to prop up their contaminated meat story at international conferences. Intense debate about the incident raged in both scientific and government circles.

Thirteen years later, then Russian president Boris Yeltsin finally admitted that a military research facility near the city (since renamed Ekaterinburg) had accidentally released spores of "Anthrax 836" into the air. Later still, the former first deputy chief of the civilian part of the Soviet biological weapons program told PBS Frontline that the leak occurred because workers forgot to replace a filter in the facility's exhaust system. He also said that had the wind been blowing in a different direction the day of the leak, hundreds of thousands could have died.

What became known as the "biological Chernobyl" should have taught the world a lesson. But in the United States today, there are hundreds of laboratories sprinkled across the country working on the exact same type of bioweapons research, with equally dangerous biological materials, in a regulatory environment that some say could blow up with an equally devastating event.

**Anthrax Spores in the Mail**

In great secrecy, the United States has spent billions on the Project BioShield Act, a program meant to keep its citizens safe from bioterrorists. Despite these good intentions, that program may have put the nation at greater risk of a homegrown disease escaping from a lab and quickly infecting millions. That's because while the real threat of bioterror is minimal—there have been only a handful of such attacks in modern history, and none since 2001—the risk of bio-error is actually quite high.

The BioShield Act was written in the frenzied wake of September 11, 2001, after letters containing anthrax spores were mailed to media companies and two U.S. senators, killing five and infecting 17 others. When the act was being shepherded through Congress in 2003, there was a global SARS outbreak, a viral infection that spread within weeks to 26 countries and caused more than 8,000 infections and 774 deaths.

Representative Jim Turner (D-Texas), a ranking member of the Committee on Homeland Security, opened the 2003 congressional hearing with an alarmist screed, claiming, "We know there was a very active biological weapons program in the former Soviet Union where they developed at least 30 deadly agents, but we do not know if the stockpiles created are secure. We know that Saddam Hussein had a biological warfare program that produced massive amounts of biological agents. Thus far, we have not been able to find them."

Whipped into a froth, the Senate and House hastily approved the act with nearly unanimous votes.

The goal of BioShield was, and remains, to protect public health during a biological disaster so catastrophic that it might affect national security. It works, essentially, by providing funds to the Department of Health and Human Services (HHS) to develop and acquire medicines for the civilian population in the event of an emergency caused by biological, chemical, radiological or nuclear agents.

Given the peculiarly volatile nature of the things being researched and the limited market (even that is optimistic) for the resulting drugs, the act had to adjust the ways in which these medicines were researched and developed. Most important, and worrisome, it had to speed up the process. Like many laws forged in the heat of war, BioShield was framed in terms of life-saving urgency, and that meant removing many of the roadblocks that regulate how labs do their research and develop new drugs.

The problem is that those safeguards are carefully crafted to protect the public. Normally, the Food and Drug Administration (FDA) approves a medicine only after its team of physicians, statisticians, chemists and pharmacologists has reviewed extensive testing data and determined that its health benefits outweigh known risks. To speed up its acquisition of rare drugs, the act has set up what amounts to an FDA fast-track review process. Some of these bio-terror drugs also have what is known as emergency-use authorization, which means testing has not been completed but they could still be used if there were an attack.

In 2010, the Public Readiness and Emergency Preparedness Act was passed to add liability protection to companies producing these drugs. It's easy to imagine someone becoming seriously ill from a less than perfectly tested vaccine and then putting a small biotech company out of business with a lawsuit. This regulatory concession creates an incentive for companies to pursue otherwise risky drug research.

As a result of these shortcuts, some of the drugs acquired under BioShield have not been subject to the usual consumer protections of regulation as well as natural marketplace corrections—consumers don't buy a medicine with bad side effects.

In 2003, only one member of Congress spoke out against the act: Donna Christensen, who, as the delegate of the U.S. Virgin Islands, did not get a vote. "[This] appears to be another attempt to bypass congressional oversight," she said, going on to ask for a legitimate reason why "good science as the basis of decisions should be allowed to be compromised."

Christensen was prescient. Though BioShield's initial goals made sense when the threat of biological warfare seemed imminent, the act may have permanently undermined some of the essential protections against unsafe practices in at least one area of science research: the regulations that keep untested drugs off the market, and labs from leaking deadly biological agents into the environment.

**Creating a Weaponized Virus**

Much of the work funded under BioShield is bio-defensive—intended to be used in a biological emergency to cure those who have been infected, and to stop the spread of disease by preventing infection in others.

The intriguing and potentially lethal paradox there is that in order to learn how a particular infection causes morbidity, says Dr. Gigi Kwik Gronvall, a senior associate at the UPMC Center for Health Security, "you're also learning how to inflict that [same infection]. You're learning where the switches are." Treatments—particularly vaccines—are usually reverse-engineered: scientists take a pathogen like a bacteria or virus and work with it in the lab until they know how to defeat it, often using parts of the infectious agent itself in the treatment.

That's easy enough when dealing with agents researchers already know about (such as anthrax and smallpox), but when it comes to bioterrorism, researchers also need to investigate what former defense secretary Donald Rumsfeld might have called the known unknowns. That's why, along with funding the cures, the HHS is also funding the creation of new bio-weapons, to be used to pre-emptively develop cures and vaccines for diseases that might break out in the future.

**In other words, to create a drug to counteract what people in the bio-terrorism world call a weaponized virus, researchers must know how to create a weaponized virus: devise a delivery system that infects as many initial hosts as possible, and mutate the agent so it spreads from person to person even more quickly than nature intended.**

Even a small vial of some of this stuff can be devastating, and these deadly agents can be easily let loose on the public.

In **1971**, a Soviet research ship puttered around the Aral Sea—basically a lake between current day Kazakhstan and Karakalpakstan—taking samples of aquatic life from the cold waters. One lab technician would dredge up plankton samples twice a day, and by the time the vessel docked at the Kazakhstani city of Aral, she had a fever, headache and muscle pain. The young technician went home but then developed a severe cough and temperature; her doctor prescribed aspirin and antibiotics. Days later, a rash appeared on her face and back.

It was a telltale sign of smallpox, one of the deadliest diseases in human history.

The technician had been vaccinated for smallpox, so she survived—as did her 9-year-old brother, to whom she had unwittingly passed the infection. However, two children and one adult infected by the same strain of smallpox died soon afterward. A massive public health response ensued: 50,000 residents of Aral were immediately vaccinated, and quarantines were enacted all over the city within two weeks.

**Years later, Pyotr Burgasov, a Soviet general and a former senior researcher in the Soviet bioweapons program, told the Russian press that the Soviets had been testing weaponized smallpox formulas on the island of Vozrozhdeniya, about 10 miles from where the ship had trawled. About 3.5 cups of smallpox in powder form had "exploded on the island," according to Burgasov. By the time it was in the plankton, though, the amount of smallpox virus that infected the technician was probably microscopic-but enough to quickly create a 150-mile radius area of contamination.**

Smallpox is a deadly and highly infectious disease, one of a handful of "select agents" on the HHS list of biological toxins that pose a severe threat to human, animal and plant health. It has been entirely eradicated from nature but lives on in research labs.

Many people, both domestic and abroad, have called for the U.S. to destroy its smallpox stockpile. (Russia and the U.S. are the only two countries that say on the record they hold samples of the virus.) "We fully agree that these samples should-and eventually will-be destroyed," wrote Secretary of Health and Human Services Kathleen Sebelius in a 2011 New York Times op-ed titled "Why We Still Need Smallpox." "However, we also recognize that the timing of this destruction will determine whether we continue to live with the risk of the disease re-emerging through deliberate misuse of the virus by others."

**In other words, the U.S. is keeping its smallpox virus alive just in case somebody else decides to turn it into a weapon.** Under the BioShield Act, HHS will not only maintain that virulent stockpile; it will also continue to make fate-tempting experiments in anticipation of its re-emergence.

**Armed Guards, 24 Hours a Day**

"Fear of not having offensive bio-weapons when others have them can motivate a self-defensive offensive bio-weapons arms race, as existed between the USA and the former Soviet Union during the Cold War," wrote Allen Buchanan and Maureen C. Kelley in a recent paper on the ethics of biodefense and what they call "dual-use" research (meaning research that is intended for benefit but could also lead to harm).

Those alive during the Cold War remember the massive stockpiling of nuclear missiles by both the U.S. and the Soviet Union—with other countries doing some minor stockpiling of their own-but, thankfully, no weapons were detonated during this time. It seems reasonable to hope that the lessons of restraint and mutual benefit learned from the nuclear missile race with Russia should guide the way forward on bio-terrorism. Of the thousands of missiles made (and retired) during that era, were all of them truly necessary to defend the nations involved? Similarly, it should be clear that a small number of high-risk labs is all that is required for bio-defense today.

But, in fact, the opposite has happened. **In 2007, the Government Accountability Office warned, "A major proliferation of high-containment BSL-3 and BSL-4 labs is taking place in the United States." Translation: A lot more of the scariest stuff is being studied in more and more labs across the country.**

Research laboratories are rated by biosafety levels; BSL-3 and BSL-4 labs are where the most dangerous research takes place. An easy way to keep this straight: The high-containment laboratories are where scientists have to use gear that makes them look like astronauts. They are also where scientists create medical countermeasures and investigate the risks posed by select agents to human and animal health, the food supply and the economy.

By the GAO's reckoning, there were 1,356 BSL-3 labs and 15 BSL-4 labs in 2009. In a 2013 report, the agency stated that the number had increased, but also warned that because there is a lack of counting and registration standards, it can no longer provide an accurate estimate.

Expansion of BSL-3 and BSL-4 labs has outpaced even the government's understanding of what's going on in these high-security kitchens. According to the GAO report, "There is still no one agency or group that knows the nation's need for all U.S. high-containment laboratories, including the research priorities and the capacity, number and location, to address priorities."

**The GAO doesn't know how many labs are in the U.S. and doesn't even know what the safety standards are in them.** The agency has noted there are still no national standards for "designing, constructing, commissioning, and operating high-containment laboratories, including provisions for long-term maintenance." These issues, they say, make it difficult to guarantee or even assess safety.

There are some safeguards in place. For example, scientists handling the most dangerous biological agents must register with the federal government, and facilities must develop and implement a security plan, which in turn must be okayed by HHS. Dr. James LeDuc, director of the Galveston National Laboratory, a BSL-4 facility at the University of Texas Medical Branch, tells Newsweek, "Part of the complex includes a very robust security force. We have armed guards 24 hours a day, seven days a week controlling access to the facility."

But, according to the GAO, there are no national standards, so Galveston may be an outlier. And with the swift buildup of biodefense over the past decade, that means an increasing number of scientists are working with the most dangerous pathogens in the highest-containment labs, which have serious safety risks. "No one is doing due diligence on any of the labs, so we don't really know if they're well run," Edward Hammond, a policy researcher and co-founder of the now-defunct Sunshine Project, tells Newsweek. For years, Hammond tracked the U.S. biodefense program. One of his many projects involved contacting institutional biosafety committees (IBCs) across the country and asking for the minutes from their latest meeting. He quickly discovered that many IBCs exist on paper only.

He also found that the lack of safety measures has already had serious consequences. "We caught them not reporting," Hammond tells Newsweek. He tracked biosafety and security lapses at Texas A&M University, where a student researcher accidentally contaminated him or herself with brucella, a deadly bacteria, while trying to clean an advanced piece of containment equipment in which mice had been exposed to particles. The researchers, according to a government report, were conducting experiments in a room not authorized for such research. The student—the university never released his or her identity—recovered from brucellosis but was seriously ill for several months.

Thomas Ficht, lead investigator of the Texas A&M research team, tells Newsweek he was out of town at the time of the accident, which was the result of "people not adhering to protocols." Asked if he received any sanctions, he says, "The university paid $1 million to the [Centers for Disease Control and Prevention]."

At the Federal Institute for Risk Assessment in Berlin, a scientist holds a bag containing plant shoots which are suspected to contain bacterial strains of Escherichia coli O104:H4, a rare enterohemorrhagic strain of E. coli which has caused the recent outbreak of illness in Germany, so far killing 35 people. Stefan Boness/Panos

Ficht suggests that there's a clash of ideas between scientists and regulators, and that when it comes down to it, the lab's scientific goals prevail—even if it means putting lives on the line. "We don't necessarily think of all the regulatory steps," he tells Newsweek. "It's taken a lot of spontaneity out of [research], but the potential risk to investigators warrants that."

Mistakes such as the one made at Texas A&M are not new to science—pioneering nuclear scientists, for example, often subjected themselves to contamination in their labs, and Marie Curie, who won a Nobel Prize for her research into radioactivity, died from a bone marrow disease caused by years of radiation exposure.

Bio-error can be as simple (and as human) as a scientist pricking herself with a needle that contains some infectious agent, or in some inadvertent way transferring a virus outside the lab. It can also mean an improperly shipped select agent—yes, they are sometimes sent through the mail—or simple ignorance of appropriate lab safety.

Accidents also occur due to events beyond human control. A bird flew into a power transformer in the summer of 2008, knocking out power to the Centers for Disease Control's (CDC) Emerging Infectious Diseases Laboratory in Atlanta for an hour. Primary as well as backup generators were temporarily down, and the negative air pressure system, which is essential for keeping dangerous agents from escaping the containment area, shut down. A building housing a BSL-3 lab-in which scientists are believed to have been studying a deadly strain of avian flu-was among those that lost power. It was dumb luck that no one became infected—an hour doesn't sound like much, but that's about 59 minutes more than a virus like the H5N1 flu needs to find a host and spread.

**No Known Cure**

Government agencies insist that BioShield work remains safe and effective. According to HHS, as of July 2013, BioShield, which was originally appropriated $5.6 billion, has acquired 17 medical countermeasures meant to fight anthrax, smallpox, botulinum toxin and radiological threats, while about 80 other candidate countermeasures are in development.

It's also clear that some good has come out of BioShield. In October 2010, while working under a Biomedical Advanced Research and Development Authority grant, Novartis, the J. Craig Venter Institute and Synthetic Genomics Vaccines Inc. used synthetic biology to dramatically accelerate the production of the flu vaccine virus strains required to make a new vaccine. This breakthrough may enable scientists to closely follow viral emergencies, transfer the genomic information through the Internet and then synthesize DNA at a remote spot. Vaccine making could occur more or less in real time.

The nation's bio-stockpile "continues to evolve, and [we are] more prepared today than ever before to respond to all-hazards threats, including chemical, biological, radiation/nuclear incidents as well as pandemic influenza," a CDC spokeswoman told Newsweek in an email.

Biodefense has grown swiftly in the past decade and should continue to expand. On the horizon is the National Bio- and Agro Defense Facility, a 574,000-square-foot complex near Kansas State University tasked with developing treatments for animal diseases that could pose threats to human health and the food supply. One-tenth of the space will be devoted to BSL-4 laboratories for handling fatal, air-transmissible pathogens that have no known cure.

Last year, BioShield was reauthorized by Congress (this time by a vote of 370-28) and is set to receive an additional $2.8 billion in unchecked funding. With that much money on the table and a welcoming regulatory environment, biodefense research seems bound to spread like, well, an infectious disease.

|  |
| --- |
| EDITOR’S QUESTION: Reading this article I remembered an unpublished study I layed my eyes on supporting the hypothesis that the rare *E.coli* “attack” in Germany could be a form of “bioterrorism”. ***Could it be?*** |

# Guinea deaths: Ebola blamed for deadly fever outbreak

Source: http://www.bbc.com/news/world-africa-26701733

The Ebola virus has been identified as the cause of an outbreak of haemorrhagic fever now believed to have killed nearly 60 people in southern Guinea, government officials say.

Scores of cases have been recorded since the outbreak began early last month.

There is no known cure or vaccine for the highly contagious Ebola virus.

It is spread by close personal contact with people who are infected and **kills between 25% and 90% of victims.**

Symptoms include internal and external bleeding, diarrhoea and vomiting.

Outbreaks of Ebola occur primarily in remote villages in Central and West Africa, near tropical rainforests, the World Health Organization says.

**Analysts suggest it has never been recorded in Guinea before. Recent years have seen outbreaks in Uganda and Democratic Republic of Congo.**

**'Overwhelmed'**

"We got the first results from Lyon yesterday (Friday) which informed us of the presence of the Ebola virus as the cause of this outbreak," Guinean health ministry official Sakoba Keita told AFP.

**"The Ebola fever epidemic raging in southern Guinea since 9 February has left at least 59 dead out of 80 cases identified by our services on the ground."**

"We are overwhelmed in the field, we are fighting against this epidemic with all the means we have at our disposal with the help of our partners but it is difficult."

Medical aid charity Medecins sans Frontieres said on Saturday it would strengthen its team in Guinea and fly some 33 tonnes of drugs and isolation equipment in from Belgium and France.

Dr Armand Sprecher, an emergency physician and epidemiologist working with MSF in Guinea, told the BBC that doctors had to identify all patients with the disease and monitor anyone they had been in contact with during their illness.

The latest outbreak could be brought under control if people acted quickly, he said.

"Based on our history with these sorts of outbreaks it will happen. Ideally, sooner rather than later," said Dr Sprecher.

"The more quickly we can contain this the fewer cases we'll have, then the smaller the scale of the epidemic. That's the idea of going in as strong as we can early on."

**Update (March 24):** UNICEF said the virus had spread quickly from the communities of Macenta, Gueckedou, and Kissidougou to **the capital Conacry**.

