November 2014

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders

10 years

www.cbrne-terrorism-newsletter.com

Japan warns of increased activity at volcano near nuclear plant

Source: http://uk.reuters.com/article/2014/10/24/uk-japan-volcano-idUKKCN0ID0A520141024

October 24 – **Japan warned on Friday that a volcano in southern Japan located roughly 64 km (40 miles) from a nuclear plant was showing signs of increased activity that could possibly lead to a small-scale eruption** and warned people to stay away from the summit.

The warning comes nearly a month after another volcano, Mt Ontake, erupted suddenly when crowded with hikers, killing 57 people in Japan's worst volcanic disaster in nearly 90 years.

Ioyama, a mountain on the southwestern island of Kyushu, has been shaken by small tremors and other signs of rising volcanic activity recently, including a tremor lasting as long as seven minutes, an official at the Japan Meteorological Agency's volcano division said.

"There is an increase in activity that under certain circumstances could even lead to a small scale eruption, but it is not in danger of an imminent, major eruption," the official said.

The warning level on the mountain has been raised from the lowest possible level, normal, to the second lowest, which means that the area around the crater is dangerous, he added.

Ioyama lies in the volcanically active Kirishima mountain range and is roughly **64 km from the Sendai nuclear plant run by Kyushu Electric Power Co, which the Japanese government wants to restart** even though the public remains opposed to nuclear power following the Fukushima crisis.

Critics point out that the Sendai plant is located about 50 kms (31 miles) from Mount Sakurajima, an active volcano that erupts frequently. Five giant calderas, crater-like depressions formed by past eruptions, are also in the region, the closest one 40 kms (25 miles) away.

The plant still needs to pass operational safety checks as well as gain the approval of local authorities and may not restart till next year.

Before giving its initial greenlight to restart the plant in July, the Nuclear Regulation Authority (NRA) said the chance of major volcanic activity during the lifespan of the Sendai nuclear plant was negligible.

On Friday, the warning level for the Sakurajima volcano, which erupts frequently, was at 3, which means that people should not approach the peak.

Japan lies on the "Ring of Fire" - a horseshoe-shaped band of fault lines and volcanoes around the edges of the Pacific Ocean - and is home to more than 100 active volcanoes.

Experts warn that the mammoth 9.0 March 2011 quake may have increased the risk of

volcanic activity throughout Japan, including that of iconic Mount Fuji.

US Satellite Witnesses Construction of North Korean Nuclear Missile Submarines

Source: http://www.christianitydaily.com/articles/892/20141030/satellite-witnesses-construction-north-korean-nuclear-missile-submarines.htm

(Photo : en.wikipedia.org)Russian Golf II Class Submarine which North Korea imported to use as a model for their nuclear missile submarines

A U.S. Military Satellite spotted a strange new facility that near the shipyards of Shinpo, in the province of Ham-Gyeongdo in North Korea. The U.S. military estimated that the facility looked like a small launch pad that could potentially be used to test-fire smaller sized ballistic missiles. **Many experts have brought up the possibility that North Korea is currently developing a new class of submarine with SLBM (Submarine Launched Ballistic Missile) capabilities.**

MBC reported that the U.S. had already sent official warnings to the North Korean government to cease the development of such weapons of mass destruction. Analysts explained that the North Korean navy had imported a number of Russian "Golf" class submarines which are now decommissioned and no longer in use. The U.S. satellite had also spotted a new submarine that was about 67 meters in the port of Shinpo.

… the facility is "a 35 x 30 m concrete pad with an approximately 12-m-high test stand…

In order for a submarine to mount a launch pad that could launch long-range missiles from under the surface, the vessel itself must be at least 3,000

tons. Many experts believe that North Korea is using the Russian "Golf" class submarine as a model to construct their own version. MBC also reported that the same experts believe that North Korea has already succeeded in miniaturizing their nuclear weapons.

In the case that North Korea acquires this technology, then they would be able to stealthily transport their nuclear warheads and launch them at literally any target. With these new submarines, they would be able to fire their ICBMs at targets as far as Alaska. Right now, **the KPA (Korean Peoples' Army) is believed to possess at least 500 missiles that could hit any part of South Korea, and at least 200 missiles that could target any part of Japan.**

Some experts however, are more skeptical. They explained that it is still uncertain whether North Korea had succeeded in miniaturizing the nuclear warheads, and many still doubt whether they have the necessary technology to mount a vertical launcher in a vessel. Most of North Korea's naval vessels, according to Korea's Channel A, do not even have conventional sonar capabilities, and most of their submarines are mini-subs that could only fire two to three torpedoes.

North Korea's navy, though unconventional in many ways was always a source of fear for the South Koreans because of the sheer amount of submarines they have**. It is believed that North Korea possesses the world's largest submarine fleet with 200 vessels in total.** Though the Republic of Korea Navy, considered the 10th most powerful navy in the world which is composed of mostly destroyers with anti-submarine capabilities, they are vastly outnumbered. **South Korea also only possesses 12 submarines.** Though these are state-of-the-art diesel subs with ballistic missile capabilities, many military experts have expressed some serious doubt as to how well they will overcome North Korea's vast numbers.

Meanwhile, MBC and Yonhap reported that North Korea's Kim Jong Un, the 1st Secretary of the Labor Party was witnessed to be overseeing the construction of their new line of nuclear missiles submarines. It appears acquiring these weapons of mass destruction are a priority for the isolated totalitarian state in the world.

Drones spotted over seven French nuclear sites

Source: http://www.theguardian.com/environment/2014/oct/30/drones-spotted-over-seven-french-nuclear-sites-says-edf

October 30 – **France's state-run power firm Électricité de France (EDF) on Wednesday said unidentified drones had flown over seven nuclear plants this month, leading it to file a complaint with the police.**

The unmanned aircraft did not harm "the safety or the operation" of the power plants, EDF said, adding that the first drone was spotted on 5 October above a plant in deconstruction in eastern Creys-Malville.

More drone activity followed at other nuclear power sites across the country between 13 October and 20 October, usually at night or early in the morning, EDF said, adding that it had notified the police each time.

Greenpeace, whose activists have in the past staged protests at nuclear plants in France, denied any involvement in the mysterious pilotless flight activity.

But the environmental group expressed concern at the apparent evidence of "a large-scale operation", noting that drone activity was detected at four sites on the same day in 19 October – at Bugey in the east, Gravelines

and Chooz in the north and Nogent-sur-Seine in north-central France.
Neither EDF nor the security forces had given any explanation about the overflights, the group said, urging the authorities to investigate. "We are very worried about the occurrence and the repetition of these suspicious overflights," said Yannick Rousselet, head of Greenpeace's anti-nuclear campaign, in a statement.
Greenpeace has repeatedly tried to highlight alleged security weaknesses at French nuclear sites. In May 2012, a Greenpeace activist flew a paraglider over the Le Bugey plant and landed on the site. The group used a drone to film the stunt.
French police arrested two Greenpeace members in 2012 after an activist flew into the grounds of a nuclear power plant using a paraglider in a stunt aimed at revealing alleged security flaws.
The French nuclear safety authority (ASN) did not comment on the claims, saying only: "We don't discuss matters outside our field of expertise."
In France, aircraft are not allowed to fly within a five-kilometre (three-mile) radius and 1,000-metre altitude over a nuclear plant.
France, the world's most nuclear-dependent country, operates 58 reactors and has been a leading international cheerleader for atomic energy.
But in a deal with the Greens before the 2012 parliamentary and presidential elections, President François Hollande's Socialist party promised to cut reliance on nuclear energy from more than 75% to 50% by shutting 24 reactors by 2025.

How one can intercept a commercial drone in urban environment?

(except the solution below)

China successfully tests laser weapon to shoot down drones

Source:http://economictimes.indiatimes.com/news/international/world-news/china-successfully-tests-laser-weapon-to-shoot-down-drones/articleshow/45014719.cms

November 02 – China today claimed to have successfully tested a homemade laser defence system specially targeting small-scale drones flying at low altitude.

The weapon is able to shoot **down various small aircraft within a two-kilometre radius** and can do so **in five seconds** after locating its target, said a statement released by the China Academy of Engineering Physics, one of the system's co-developers.
Characterised by its speed, precision and low noise, the system is designed to destroy unmanned, small-scale drones flying within an **altitude of 500 metres and at a speed below 50m/s**, state-run Xinhua news agency reported.
"Intercepting such drones is usually the work of snipers and helicopters, but their success rate is not as high and mistakes with accuracy can result in unwanted damage," said Yi Jinsong, a manager with China Jiuyuan Hi-Tech Equipment Corp, a group under the academy spearheading the project.
According to Yi, small-scale, unmanned drones are relatively cheap and easy-to-use, which makes them a likely choice for terrorists.
In addition, concerns have been raised over drones engaged in unlicensed mapping activities and the affect this could have on military and civil aerial activities.
The **new laser system**, which will either be installed or transported in vehicles, is expected to play a key role in ensuring security during major events in urban areas, the statement said, adding that a recent test saw the machine successfully shoot down more than 30 drones - a **100 per cent success rate.**
The academy said it was developing similar laser security systems with greater power and range.

Sandia Lab's mobile neutron imager shines in urban emergency response exercise

Source: http://www.homelandsecuritynewswire.com/dr20141103-sandia-lab-s-mobile-neutron-imager-shines-in-urban-emergency-response-exercise

November 03 – A nuclear device has been hidden in a high-rise building in a major metropolitan area. Emergency responders have intelligence that narrows down the location to a single city block, but it is not safe to search door-to-door. **Can they identify the exact location of the device quickly without the culprits realizing a search is on?**

The answer is a definite yes. Sandia National Laboratories' mobile imager of neutrons for emergency responders (MINER) system did just that at an emergency response exercise in downtown Chicago earlier this year. The exercise used a sealed laboratory radiation source that mimics the radioactive signature of more nefarious material.
"The system performed exactly as we expected," said Sandia physicist John Goldsmith. "With an unshielded source, we pinpointed the location within thirty minutes. With more shielding, it took a couple of hours."
A Sandia Lab release reports that MINER is a portable version of the neutron scatter camera (photo), which detects fast neutrons that emanate from special nuclear material to pinpoint the source, even at significant distances and through shielding. Funding for the development came from the Defense Nuclear Nonproliferation Office of Research and Development within the Department of Energy's National Nuclear Security Administration.
The original neutron scatter camera was quite large, standing about 5-feet tall and requiring a power source. MINER is about

half that size at 3-feet tall and 90 pounds.
MINER consists of sixteen proton-rich liquid scintillator cells arranged inside a large cylinder. The scatter aspect comes into play as neutrons travel through the scintillator cells and bounce off protons like billiard balls. Those interactions among the different detector cells enable the instrument to determine the direction of the radioactive source that emitted the neutrons.

Distinguishes between threatening and non-threatening radiation sources

As a neutron scatter camera, MINER (photo) has several advantages over other types of detectors, including the ability to discriminate the device signature from background radiation and to measure the spectrum of neutrons emitted by it.

"Simple neutron counters are unable to distinguish a threat source from an elevated neutron background. However, an imager such as MINER can do this by observing a 'hot spot' against the neutron background," Goldsmith said. "In addition, MINER's ability to measure the neutron spectrum enables it to distinguish plutonium, a threat source, from AmBe [americium-beryllium, the most common commercial source of neutrons], which is not a threat source. Among imaging approaches, this capability is unique to MINER."

MINER can be set up and taken down in ten minutes, and most importantly, operates on battery power. "Since MINER doesn't need to be tethered to a power source, it gives a lot of options to emergency responders," said Goldsmith.

The Chicago field exercise focused on neutron detectors, so MINER was one of three neutron imagers tested along with several neutron counters. It wasn't a competition, explained Goldsmith, but a test of each detector's capabilities.

"There are tradeoffs with every kind of detector. If you are trying to pinpoint a source, a backpack detector might be the fastest, but there are scenarios in which walking around isn't possible," he said.

One of MINER's strengths is its ability to provide omni-directional imaging. "Other imaging detectors have a very fixed field of view, so they look at a specific spot," said Sandia physicist Mark Gerling. "MINER images all the way around and up and down, or a full 4π steradians. We imaged part of one side of an entire high-rise building at once and narrowed the search to a specific room. It's extremely effective in this situation."

Two-for-one detector captures neutrons and gamma rays

MINER also is a two-for-one detector. The system was designed for neutron imaging and spectroscopy, but its proton-rich liquid scintillators also can capture gamma rays. While not the most efficient or effective gamma ray detector, MINER's design makes it suitable for several unusual applications.

"When used as a neutron scatter camera, MINER is closed. But if we open it up, we can position MINER near a radiation source and gather additional information about that source. This could be very useful in determining how to handle an object that is emitting radiation," explained Goldsmith.

The release notes that future work on MINER includes expanding and refining its measurement capabilities and participating in a search scenario at sea.

We Drove Saddam's Yellowcake to the Baghdad Airport

By Carter Andress

Source: http://www.frontpagemag.com/2014/carter-andress/we-drove-saddams-yellowcake-to-the-baghdad-airport/

As someone who led the company that transported 550 metric tons of yellowcake uranium—enough to make fourteen Hiroshima-size bombs—from Saddam's nuclear complex in the Iraq War's notorious "Triangle of Death"

for air shipment out of the country, I know Baathist Iraq's WMD potential existed**. In early 2008, we secretly moved over several nights 140 truckloads carrying 5500 barrels of extremely heavy radioactive material provided to Iraq as part of the French-supplied Osiraq reactor destroyed by Israeli fighter bombers in 1981.** The virulently anti-

Semitic Saddam had announced "here begins the Arab bomb" and the Israelis took him at his word.

The recent article in the New York Times, however, caught us all by surprise. Random caches of old chemical weapons found post-invasion were old news, but not "roughly 5,000" warheads and bombs, many filled with still active, nerve agent. That's an enormous quantity even if evidently left over from the 1980s Iran-Iraq War. Just "antiques," as the Washington Post's Karen DeYoung quaintly put it at a Center for Strategic and International Studies forum on Iraq.

At the least, this shocker (after so many years of repetitious "Bush lied [about WMD], people died") further points to the **world's inability to trust that the UN inspectors could ever realistically certify Saddam clean of his nuclear, chemical, and biological weapons programs.** He had to be

deposed, and the only way to do it was for us to invade and overthrow his dictatorship. Here was a genocidal, expansionist tyrant who had used chemical weapons on his own people and that of a neighboring nation (Iran), publically celebrated 9/11, and allowed a chemical weapons laboratory affiliated with al-Qaeda to operate within his security forces' reach inside his country's borders in contested Kurdistan (Khurmal).

The article in the Times references the Duelfer Report that summed up the official American

investigation of Iraq's WMD as definitive in that there were no ongoing WMD programs pre-invasion, yet fails to mention that every section of the report on the different types of weapons of mass destruction concluded that the evidence gathered by investigators clearly indicated that once sanctions were removed Saddam would reinstate his WMD programs. In addition, the article mentions that the chemical weapons program was not active for over ten years, but not the biological weapons program, which extended into 1996 and was only discovered because Saddam's son-in-law defected, even after five years of aggressive UN inspections.

There's no question in my mind, Saddamist Iraq would have reconstituted its WMD programs once UN sanctions faded away—a push Security Council veto-wielding members Russia and France were actively working toward because of oil field opportunities. (Petroleum companies from both countries signed huge, new contracts with Saddam pre-invasion.) And given the yellowcake inventory, nuclear weapons with available Pakistani and North Korean technology might not have been far off. After over ten years in effect, the sanctions system was actively degrading with banned flights landing in Baghdad, the Oil for Food program corrupted, and, as a result, would have collapsed if we had not invaded—thus leaving Saddam free to threaten the world again with WMD.

The greater problem, however, of significant quantities of chemical weapons hidden at some date prior to the US invasion points to a current and growing threat. The leader of the neo-Saddamists allied now with ISIS is Izzat al-Douri, a former Iraqi army general and last member of the senior Baathist leadership not executed or imprisoned. There is a distinct possibility that Saddam's minions hid these munitions with the intention of disinterring them for deterrent use once again. And in fact, this is why Saddam's military and secret police leaders never ceased to believe Iraq possessed WMD and could therefore project terror onto the Kurds and the rest of the region (Israel and Iran, specifically) until the end because Iraq did possess WMD, even after the dictator's death by hanging. The Iraqi army and security services did not handle "special" weapons without the knowledge of the regime's leaders. So to think that Saddam and his immediate circle, including al-Douri, did not know the locations of the WMD discussed in the Times article begs credulity.

Much of the area where the "antique," yet still potentially potent chemical weapons discovered by US forces is now in the hands of ISIS, the forces of al-Douri, and their allied Sunni Arab tribes undergirding the "caliphate" occupying almost a third of Iraq. With hundreds of Western passport holders fighting in Syria and Iraq, the most immediate threat to the United States is the spread of jihadi terrorism to Europe now that ISIS has a border with Turkey, a gateway to the EU.

Can one even imagine the impact of a weaponized sarin-gas attack in Paris?

Carter Andress *is president of AISG, Inc. (American-Iraqi Solutions Group) and the author, with Malcolm McConnell, of* Victory Undone: The Defeat of al-Qaeda in Iraq and Its Resurrection as ISIS *(Regnery, October 2014).*

Gulf countries concerned over possible fallout from Dimona

Source: http://i-hls.com/2014/11/gulf-countries-concerned-possible-fallout-dimona/

Israel's nuclear capabilities occupy the minds of many, not only Israel's direct enemies but also the countries in the Persian Gulf, which are heavily invested in comprehensive studies designed to obtain any information on this issue. Their purpose is, inter alia, to be better prepared for any eventuality. One of the more surprising agencies which publish detailed position papers on Israeli nuclear ability and its perils, is The Emirates Center for Strategic Studies and Research.

Recently, the center released interesting details on a possible source of hazard: the plant at Dimona, Israel.

Among the interesting arguments in the framework of a recent study by the center, takes up a warning issued by Bennett Ramberg, a policy analyst in the US State Department's Bureau of Politico-Military

Affairs under President George H.W. Bush (senior). Ramberg said as follows: in the case of an Israeli strike against Iran, not necessarily an Israeli nuclear strike, the possible counter-attack on Israel (by Iran and or Hezbollah) using conventional missiles may focus on the Dimona plutonium-based nuclear plant.

Ramberg underscored that according to estimates by American nuclear experts, the results of such a conventional attack on Israel could resemble those of a so-called 'dirty bomb'. An attack on the plant at Dimona could engulf neighboring Israeli towns, but due to the wind patterns in the area, the nuclear fallout might cross the Arab Desert all the way to the Persian Gulf, thereby affecting mass populations. The study's co-authors believe Israel gained a great deal from its policy of nuclear ambiguity. For instance, when three countries – Iran, Iraq and Syria – were perceived in the public's eye for years as attempting to develop nuclear capabilities, the result was that the global community turned against those three countries. Nevertheless, Israel was not the target of any sanctions, nor was any direct pressure brought to bear on Israeli to stop its alleged nuclear activity. Thus, behind this veil of ambiguity, claims the report, Israel has managed to produce an arsenal of 75-200 nuclear bombs. In addition, the world has never made a real effort to force Israel to sign the NPT, the Non-Proliferation Treaty, let alone ratify it.

Nuclear weapons convoy trucks 'should have been retired in 2003'

Source: http://news.stv.tv/west-central/298916-nuclear-weapons-convoy-trucks-should-have-been-retired-in-2003/

Trucks transporting nuclear materials through Scotland have suffered a series of breakdowns and faults since 2010, it has been revealed.

A freedom of information request by monitoring body Nukewatch uncovered a number of incidents when convoys have been delayed

or forced to turn back because of faults including fuel leaks, mechanical breakdowns and flat batteries.

The aging vehicles used to transport warheads and other nuclear material to RNAD Coulport in Argyll were originally supposed to have been taken out of service in 2003, with an MoD assessment stating they would become "increasingly unsupportable" by 2009.

Jane Tallents of Nukewatch said: "It's very clear that, as a result of bureaucracy and incompetence in the Ministry of Defence, deadly cargoes of highly radioactive materials are being driven round the country in unreliable, antiquated vehicles which cannot be guaranteed to deliver them safely to their destination.

"The military regularly tell the public that their nuclear programmes operate to the highest safety standards, but the evidence here shows that this is far from being the case."

Transport minister Keith Brown said he would raise the issue with the UK Government in the wake of the Nukewatch report.

He said: "It's no secret that I'm opposed to the presence of nuclear weapons in Scotland and that I'd like to see them permanently removed, but while they are there we should be doing all we can to make sure that safety is paramount.

"The revelations by the Nukewatch network that old vehicles are being used to transport warheads between Coulport and the maintenance facilities in England adds to existing worries.

"I already have concerns about these weapons being transported on our public roads at all and serious reservations about them travelling through our towns and cities. I look at the potential for damage to the road network, especially from the weight of the trucks on some of our smaller roads, as well; Scotland is carrying the risks and the costs of having these things lurking in our country and that has to stop.

"Finding out that the trucks the UK Government is using to transport its weapons of mass destruction through our communities are outdated has the smell of politicians who care little being prepared to do things on the cheap without thinking about the consequences.

"I'll be raising this with the UK Government and demanding some answers; we need to know, at the very least, that all practical steps are being to protect public safety while Scotland is burdened with hosting these weapons."

Missing radioactive material may pose 'dirty bomb' threat: IAEA

Source: http://www.reuters.com/article/2014/03/21/us-nuclear-security-iaea-idUSBREA2K10W20140321

About 140 cases of missing or unauthorized use of nuclear and radioactive material

were reported to the U.N. atomic agency in 2013, highlighting the challenges facing world leaders at a nuclear security summit next week.

Any loss or theft of highly enriched uranium, plutonium or different types of radioactive sources is potentially serious as al Qaeda-style militants could try to use them to make a crude nuclear device or a so-called "dirty bomb", experts say.

Denis Flory, deputy director general of the International Atomic Energy Agency (IAEA), (photo) said most of the reported incidents concerned small quantities of radioactive material.

But, "even if they can't be used for making a nuclear weapon, they can be used in radioactive dispersal devices, which is a concern," Flory told Reuters in an interview.

In a "dirty bomb", conventional explosives are used to disperse radiation from a radioactive source, which can be found in hospitals, factories or other places that may not be very well protected.

Holding a third nuclear security summit since 2010, leaders from 53 countries - including U.S. President Barack Obama - are expected to call for more international action to help

prevent radical groups from obtaining atomic bombs.
At the March 24-25 meeting in The Hague, they will say that much headway has been made in reducing the risk of nuclear terrorism but also make clear that more must be done to ensure that dangerous substances don't fall into the wrong hands.
The Dutch hosts say the aim is a summit communique "containing clear agreements" to prevent nuclear terrorism by reducing stockpiles of hazardous nuclear material, better securing such stocks and intensifying international cooperation.
Flory said member states had reported a total of nearly 2,500 cases to the IAEA's Incident and Trafficking Database since it was set up two decades ago. More than 120 countries take part in this information exchange project, covering theft, sabotage, unauthorized access and illegal transfers.

Nuclear security pact delayed

In 2012, 160 incidents were reported to the IAEA, of which 17 involved possession and related criminal activities, 24 theft or loss and 119 other unauthorized activities, its website says.
"It is continuing, which means there is still a lot of work to do to have that really decrease," Flory said with respect to the statistics. However, there are also "more and more countries which declare incidents. The number of incidents we don't know is probably decreasing."
Because radioactive material is less hard to find and the device easier to make, experts say a "dirty bomb" - which could cause panic and have serious economic and environmental consequences - is a more likely threat than a deadly atom bomb.
Radical groups could theoretically build a crude nuclear bomb if they had the money, technical knowledge and fissile materials needed, analysts say.
One of the biggest challenges ahead is to finally bring into force a 2005 amendment to the Convention on Physical Protection of Nuclear Materials (CPPNM), Flory said.
There are still 27 countries - including the United States - which need to ratify the amendment, which expands the coverage from only the protection of nuclear material in international transport to also include domestic use, transport and storage.
"It is extremely important because this amendment brings a lot of strengthening in the field of nuclear security," he said.
Harvard University professor Matthew Bunn said this month that a U.S. failure so far to ratify the amended convention "has made it far harder" for Washington to pressure others to do so.
"The problem appears to be a combination of lack of sustained high-level attention by both the administration and Congress and disputes over unrelated issues," Bunn said.
Flory, who heads the IAEA's nuclear safety and security department, said he knew that the U.S. administration was "very keen on finishing the process" as soon as possible.
"This is a country where you have a lot of nuclear material, a lot of nuclear facilities and they have a lot of influence on nuclear security."

Iran is going to be a nuclear power

Source: http://i-hls.com/2014/11/iran-going-nuclear-power/

Very soon, Israel would have to come to terms, so it seems, with a highly regrettable foregone conclusion: Iran will have become a nuclear power. Does this development mean that Iran would attack Israel? Or does it mean, perhaps, that Israel might use conventional weapons to attack Iran's nuclear facilities, in order to prevent it from joining the nuclear club? It would seem than none of these two options is about to materialize.
Iran is not going to attack Israel, as its leaders are all too familiar with the "Second Strike Capability" Israel's deep ocean fleet wields, which could deliver a serious blow to the regime's facilities, for example in Teheran. From Iran's point of view, belligerent Israel is a danger to world peace, so their nuclear program is designed to curtail this

threat and safeguard against it, rather than use nuclear weapons to destroy Israel.
According to foreign sources, Israel would not use nuclear weapons, if only since doing so would serve as an unwitting admittance, contrary to is long-enduring policy of "nuclear ambiguity", to having nuclear arms. Israel would not launch conventional means either, despite its leaders' confrontational statements, for this could be a prelude to an all-Islamic effort to develop nuclear weapons or acquire them, thereby turning the entire Middle East to a multi-nuclear region, as well as the hotbed for regional warfare.
Such a development raises the following fundamental question worldwide, in particular in the US: how is Iran going to conduct itself after it will have achieved nuclear weapons? Will Iran become a bellicose power bent on undermining the long-standing American clout among the Middle East's oil producing countries, thereby preempting a possible future Israeli strike? Or would Iran decide to dissipate these concerns among its neighbors and choose in turn to develop good relations with all fellow Muslim countries in the region, thereby clarifying it has no intention of seizing control of any of them.
Another source for concern in the US is the direction of Iran's relations with the burgeoning sector of Islamic terrorist organizations? Iran is currently a major financier of terrorist activity, but Teheran does not direct their actions nor sets targets for them. The West seems to believe this policy is not going to change once Iran crosses the nuclear threshold.
In view of the political upset in the US following the Mid-term elections and the Republican victory in Congress and the Senate, it seems that despite the President's reassurances to Prime Minister Netanyahu, that the US would never allow Iran to 'go nuclear', it is far from clear whether the Obama administration could at all back on the president's promises. Aside from promises not always being tantamount to actions, it would be very difficult for a 'lame duck president', especially after a Democratic Party defeat, to determine foreign policy exclusively. It may very well be incumbent upon the president to face facts and accept that the Republican Party would be calling the shots from now on.
It would appear as though for now, Israel might be the primary casualty of the Mid-term election results. After his debacle, Obama may become anti-Israeli with a vengeance, as he would no longer have to consider public opinion in the framework of his decisions in the case of being tough on Israel. Having lost the election, President Obama may find it difficult to execute operative measures that would be damaging to Israel, but during his remaining two years in office, he could still undermine Israel's international standing, cast a shadow over Israel's leaders and generally make Israel's life miserable.

Israeli nuclear weapons, 2014

By Hans M. Kristensen and Robert S. Norris
Source: http://bos.sagepub.com/content/70/6/97.full

Since the late 1960s, every Israeli government has practiced a policy of nuclear opacity that, while acknowledging that Israel maintains the option of building nuclear weapons, leaves it factually uncertain as to whether Israel actually possesses nuclear weapons and if so at what operational status. Since the mid-1960s, this policy has been publicly expressed—and recently reaffirmed by Prime Minister Benjamin Netanyahu—as the phrase "We won't be the first to introduce nuclear weapons into the Middle East" (Netanyahu, 2011).
This statement is widely seen as a deception, because it is a long-held conclusion among governments and experts that Israel has produced a sizable stockpile of nuclear warheads (probably unassembled) designed for delivery by ballistic missiles and aircraft. Common sense dictates that a country that has developed and produced nuclear warheads for delivery by designated delivery vehicles has, regardless of their operational status, introduced the weapons to the region. But Israeli governments have attached so many interpretations to "introduce" that common sense doesn't appear to apply.

Declassified documents from US–Israeli negotiations in 1968–1969 about the sale and delivery of F-4 Phantom aircraft show that the White House understood full well that "they [Israel] interpreted that ["introduction"] to mean they could possess nuclear weapons as long as they did not test, deploy, or make them public" (White House, 1969a: 1). In a memo prepared for President Nixon on the Israeli nuclear program, national security advisor Henry Kissinger stated: "This is one program on which the Israelis have persistently deceived us—and may even have stolen from us" (White House, 1969a: 7 of attachment).

Both the Johnson and Nixon administrations tried to get a clearer understanding of the Israeli interpretation of "introduction." During a meeting at the Pentagon in November 1968, Israel's ambassador to the United States, Yitzhak Rabin, who later succeeded Prime Minister Golda Meir as Israeli prime minister, said that "he would not consider a weapon that had not been tested to be a weapon." Rabin noted that this was his personal understanding as a former military leader. Moreover, he said, "There must be a public acknowledgement. The fact that you have got it must be known." Seeking clarity, US Assistant Secretary of Defense Paul Warnke asked: "Then in your view, an unadvertised, untested nuclear device is not a nuclear weapon?" Rabin responded: "Yes, that is correct." So, Warnke continued, an advertised but untested device or weapon would constitute introduction? "Yes, that would be introduction," Rabin confirmed (Department of Defense, 1968: 2, 3, 4).

In a follow-up exchange in July 1969, the Nixon administration plainly summarized its own understanding of the term "introduction": "When Israel says it will not introduce nuclear weapons it means it will not possess such weapons." The Nixon administration wanted Israel to accept the US definition, but the Meir government didn't take the bait and instead claimed: "Introduction means the transformation from a non-nuclear weapon country into a nuclear weapon country" (Department of State, 1969a). In other words, Israel construed its pledge not to be the first to introduce nuclear weapons to mean that that introduction was not about physical possession but about public acknowledgement of that possession.

Kissinger saw a way out of the disagreement: He informed President Nixon that what the Israelis had done was to "define the word 'introduction' by relating it to the NPT [Nuclear Non-Proliferation Treaty]." Kissinger's argument was that the "distinction between 'nuclear-weapon' and 'non-nuclear-weapon' states is the one which the NPT uses in defining the respective obligations of the signatories." By arguing that the NPT negotiations "implicitly left … it up to the conscience of the governments involved" by being "deliberately vague on what precise step would transform a state into a nuclear weapon state after the January 1, 1967, cut-off date used in the treaty to define the nuclear states," and by arguing that the NPT does not define what it means to "manufacture" or "acquire" nuclear weapons, Kissinger concluded that the new Israeli formulation "should put us in a position for the record of being able to say we assume we have Israel's assurance that it will remain a non-nuclear state as defined in the NPT" (White House, 1969b: 1).

Kissinger's disingenuous interpretation provided the United States with a way out of a diplomatic dilemma via a tacit understanding between Nixon and Meir that the United States would no longer pressure Israel to sign the Nuclear Non-Proliferation Treaty as long as the Israelis kept their program restrained and invisible—meaning that Israel would not test nuclear weapons and would not acknowledge in public its possession of such weapons.

The Nixon administration also tried to extract a pledge from Israel on the use of US-supplied aircraft. In the Israeli letter that requested the sale of 50 F-4 Phantoms, Rabin formally promised the United States that Israel "agrees not to use any aircraft supplied by the U.S. as a nuclear weapons carrier" (Embassy of Israel, 1968: 1). A similar promise was made in 1966 in connection with the sale of A-4 Skyhawk aircraft. It is not known if Israel made similar pledges when it acquired F-15 and F-16 aircraft in the 1980s and 1990s, or when it purchased F-35s—which will start to be delivered in 2017.

If a formal pledge was made also for the F-15 and F-16 aircraft, it would appear to rule out Israel currently using US-supplied aircraft in a nuclear strike role. But given the preconditions the Nixon administration discovered Israel had attached to the "no introduction" pledge, Israel may also have attached preconditions to the pledge not to "use any aircraft supplied by the U.S. as a nuclear weapons carrier." What do "use" and "carrier" mean? Do they refer to equipping an aircraft with the *capability* to deliver nuclear weapons or do they refer to the act of *employment* itself? Does the pledge apply to US aircraft modified by Israel? And what does "nuclear weapons" mean? Similar to the interpretation of "introduction," Israel may

consider that as long as a nuclear bomb is not assembled nor its existence announced, a US-supplied aircraft is not being used (by Israel's definition) as a carrier of nuclear weapons.
The tacit understanding that the Nixon administration reached with Israel about "introduction" may have resolved a diplomatic conundrum. But it failed to address the core issues: first, that Israel already possessed nuclear weapons, and second, that the United States would be seen as having a double standard when criticizing other Middle Eastern countries for pursuing nuclear weapons while turning a blind eye to Israel's arsenal. And those have been irritants regarding the NPT and Middle Eastern security issues ever since, helping provide excuses for other countries in the region to reject criticism of their own weapons of mass destruction.
On a few rare occasions, some Israeli officials have made statements implying that Israel already has nuclear weapons or could "introduce" them very quickly if necessary. The first came in 1974, when then-President Ephraim Katzir stated: "It has always been our intention to develop a nuclear potential … We now have that potential" (quoted in Weissman and Krosney, 1981: 105). Long after his retirement, in a 1981 *New York Times* interview, former defense minister Moshe Dayan also came close to violating the nuclear ambiguity taboo when he declared for the record: "We don't have any atomic bomb now, but we have the capacity, we can do that in a short time." He reiterated the official policy mantra "We are not going to be the first ones to introduce nuclear weapons into the Middle East," but his acknowledgement that "we have the capacity" and would quickly produce atomic bombs if Israel's adversaries acquired nuclear weapons was a hint that Israel had in fact produced all the necessary components to assemble nuclear weapons in a very short time (*New York Times*, 1981).
During a press conference in Washington with US President Bill Clinton and Jordan's President Hussein in 1994, Israeli Prime Minister Yitzhak Rabin made a similar statement, saying "Israel is not a nuclear country in terms of weapons" and has "committed to the United States for many years not to be the first to introduce nuclear weapons in the context of the Arab-Israeli conflict. But at the same time," he added, "we cannot be blind to efforts that are made in certain Muslim and Arab countries in this direction. Therefore, I can sum up. We'll keep our commitment not to be the first to introduce, but we still look ahead to the dangers that others will do it. *And we have to be prepared for it*" (Rabin, 1994; emphasis added).
The ambiguity left by Israel's refusal to confirm or deny the possession of nuclear weapons prompted the BBC in 2003 to bluntly ask former Prime Minister Shimon Peres whether the ambiguity was just another word for deception: "The term nuclear ambiguity, in some ways it sounds very grand, but isn't it just a euphemism for deception?" Peres did not answer the question but confirmed the need for deception: "If someone wants to kill you and you use deception to save your life, it's not immoral. If we wouldn't [sic] have enemies we wouldn't need deceptions" (BBC, 2003).
Three years later, in a December 2006 interview with German television, then-Prime Minister Ehud Olmert appeared to compromise the deception when he criticized Iran for aspiring "to have nuclear weapons, as America, France, Israel, Russia" (Williams, 2006). The statement, which he made in English, attracted widespread attention because it was seen as an inadvertent admission that Israel possesses nuclear weapons (Williams, 2006). A spokesperson for Olmert later said he had been listing not nuclear states but "responsible nations" (Friedman, 2006).
Ambiguity is not just about refusing to *confirm* possession of nuclear weapons but also about refusing to *deny* it. When asked during a 2011 CNN interview if Israel *does not* have nuclear weapons, Netanyahu did not answer directly but repeated the policy not to be the first to "introduce" nuclear weapons into the Middle East. Undeterred, the journalist followed up: "But if you take an assumption that other countries have them then that may mean you have them?" Netanyahu didn't dispute that but implied that the difference is that Israel doesn't threaten anyone with its arsenal: "Well, it may mean that we don't pose a threat to anyone. We don't call for anyone's annihilation … We don't threaten to obliterate countries with nuclear weapons but we are threatened with all these threats" (Netanyahu, 2011).

The nuclear alert

One of the scenarios where Israel might decide to "introduce" its nuclear arsenal is in a crisis that poses a threat to the very existence of the state of Israel. It is widely believed such an incident might have happened in October 1973 during the Yom Kippur War, when Israeli leaders feared Syria was about to defeat the Israeli army in the Golan Heights. The rumor first appeared in *Time* magazine in 1976, was greatly expanded upon in Seymour

Hersh's book *The Samson Option* in 1991, and several unidentified former US officials allegedly stated in 2002 that Israel put nuclear forces on alert in 1973 (see e.g., Sale, 2002).

But an interview conducted by Avner Cohen with the late Arnan (Sini) Azaryahu in January 2008 calls into question the validity of this rumor. Azaryahu was senior aide and confidant to Yisrael Galili, a minister without portfolio who was Golda Meir's closest political ally and privy to some of Israel's most closely held nuclear secrets. In the early afternoon of the second day of the war—October 7, 1973—when the Israeli military appeared to be losing the battle against Syrian forces in the Golan Heights, Azaryahu said that the defense minister, Moshe Dayan, asked Meir to authorize initial technical preparations for a "demonstration option"—that is, ready nuclear weapons for potential use. But Galili and Deputy Prime Minister Yigal Allon argued against the idea, saying Israel would prevail using conventional weapons. According to Azaryahu, Meir sided with her two senior ministers and told Dayan to "forget it" (Cohen, 2013. For analysis of the Azaryahu interview and its implications, see Cohen (n.d.).)

A study by the Strategic Studies division of the Center for Naval Analyses (CNA) in April 2013 appeared to confirm Meir's rejection of Dayan's "demonstration option" and that Israel's nuclear forces were not readied. The report states that even though the authors "did exhaustively scrutinize" the document files of US agencies and archives and interviewed a significant number of officials with firsthand knowledge of the 1973 crisis, "None of these searches revealed any documentation of an Israeli alert or clear manipulation of its forces," and "none of our interviewees, save one, recalled any Israeli nuclear alert or signaling effort" during the Yom Kippur War (Colby et al., 2013: 31–32).

Even so, the single former official who recalled seeing an "electronic or signals intelligence report" at the time that "Israel had activated or increased the readiness of its Jericho missile batteries"—and the extreme government secrecy that surrounds the issue of Israeli nuclear weapons in general—led the authors of the CNA study to conclude that "the United States did observe some kind of Israeli nuclear weapons-related activity in the very early days of the war, probably pertaining to Israel's Jericho ballistic missile force … ." (Colby et al., 2013: 34). The study's overall assessment was that "Israel appears to have taken preliminary precautionary steps to protect *or prepare* its nuclear weapons and/or related forces" (Colby et al., 2013: 2; emphasis added).

The conclusion that Israel did something with its nuclear forces in October 1973—although not necessarily place them on full operational alert or prepare for a "demonstration option"—seems similar to the assertion made by Peres in 1995, who in an interview with the authors of *We All Lost the Cold War* "categorically denied that Jericho missiles were made ready, much less armed. At most, he insisted, there was an operational check. The cabinet never approved any alert of Jericho missiles" (Lebow and Stein, 1995: 463, footnote 47).

Evidently, some uncertainty persists about the 1973 events. But then, presumably as well as now, the Israeli warheads were not fully assembled or deployed on delivery systems under normal circumstances but stored under civilian control. And since no official confirmation was made back then either via a test or an announcement, no formal "introduction" of nuclear weapons occurred—at least in the opinion of Israeli officials.

Six years later, on September 22, 1979, a US surveillance satellite known as the Vela 6911 detected what appeared to be the flash from a nuclear test in the southern parts of the Indian Ocean (for background on the 1979 Vela incident, see Richelson, 2006). Despite widespread rumors about Israeli involvement in the test, which would constitute "introduction" of nuclear weapons by the Israeli definition, Israeli governments have continued since to state that Israel would not be the first to introduce nuclear weapons in the region.

How many warheads?

Absent official public information from the Israeli government or intelligence communities of other countries, speculations abound about Israel's nuclear arsenal. Over the past several decades, news media reports, think tanks, authors, and analysts have sized the Israeli nuclear stockpile widely, from 75 warheads up to more than 400 warheads. Delivery vehicles for the warheads have been listed as aircraft, ballistic missiles, artillery tactical or battlefield weapons such as artillery shells and landmines, and more recently sea-launched cruise missiles. We believe many of these rumors are inaccurate and that the most credible stockpile number is on the order

of 80 warheads for delivery by aircraft, land-based ballistic missiles, and possibly sea-based cruise missiles (see Table 1).

TYPE	YEAR FIRST DEPLOYED	RANGE (KM)	COMMENT
AIRCRAFT			
F-16A/B/C/D/I Fighting Falcon	1980	1,600	Nuclear bombs posssibly stored at underground facility near Tel Nof Air Base
F-15I Ra'am (Thunder)	1998	3,500	Potential nuclear strike role
LAND-BASED MISSLES			
Jericho II	1984–1985	1,500+	Possibly 25–50 at Zekharia for TELs in caves
Jericho III	?	4,000 ?	In development
SEA-BASED MISSLES			
Dolphin-class submarines	2002 ?	?	Possibly modified cruise missile for land-attack

Table 1. Israeli nuclear forces, 2014

In 1969, the US State Department concluded: "Israel has moved as rapidly as possible since about 1963" in "developing a capability to produce and deploy nuclear weapons, and to deliver them by surface-to-surface missile or by plane" (Department of State, 1969b: 1; Department of State, 1969c: 3). By 1974, the CIA concluded: "Israel already has produced and stockpiled a small number of fission weapons" (CIA, 1974: 20). "Small" is a relative term; to some analysts it meant an arsenal of a dozen or two dozen weapons, but the public estimate would later balloon significantly.

Most publicly available estimates appear to be derived from a rough calculation of the number of warheads that could hypothetically be created from the amount of plutonium Israel is believed to have produced in its nuclear reactor at Dimona. The technical assessment that accompanied the 1986 *Sunday Times* article about former nuclear technician Mordechai Vanunu's disclosures about Dimona, for example, estimated that Israel had produced enough plutonium for 100 to 200 nuclear warheads (*Sunday Times*, 1986a, 1986b, 1986c).[2] In the public debate, this quickly became Israel *possessing* 100 to 200 nuclear warheads, the estimate that has been most commonly used ever since. There is uncertainty about the operational history or efficiency of the Dimona reactor's operation over the years, but plutonium production is thought to have continued after 1986, making for a total of roughly 840 kilograms of plutonium for military purposes.[3] That amount could potentially be used to build 168 to 210 nuclear weapons, assuming a second-generation, single-stage, fission-implosion warhead design with a boosted pit containing 4 to 5 kilograms of plutonium.[4]

Total plutonium production is a misleading indicator of the actual size of the Israeli nuclear arsenal, however, because Israel—like other nuclear-armed states—most likely would not have converted all of its plutonium into warheads. A portion is likely stored as a strategic reserve. And given that Israel probably has a limited portion of its aircraft and missiles that are equipped to deliver nuclear weapons, it would in any case not produce many more warheads than it can actually deliver.

And this is where the estimates of 200 to 400 warheads strain credibility. Assuming that Israel has no more than 25 single-warhead land-based ballistic missiles, such a large stockpile would imply as many as 150 to 350 air-delivered bombs, or a significant inventory of other types of nuclear weapons. In comparison, the 180 US bombs deployed in Europe have roughly 20 bombs allocated to each nuclear-capable fighter-bomber squadron. Israel's nuclear posture has not been determined by war-fighting strategy but by deterrence needs, so a more realistic estimate may be that Israel only has a couple of fighter-bomber squadrons assigned to the nuclear missions with perhaps 40 bombs in total.

The higher stockpile estimates appear to come from rumors that Israel has produced a significant number of other types of nuclear weapons, or tactical nuclear weapons. A variety of different sources over the years has claimed, without providing much evidence, that the other weapon types include artillery, landmines, suitcase bombs, nuclear electromagnetic pulse weapons to take out electronic circuits, and enhanced radiation weapons (neutron bombs).[5]

Seymour Hersh's 1991 best-seller, *The Samson Option*: *Israel's Nuclear Arsenal and American Foreign Policy*, claimed that Israel had manufactured "hundreds" (Hersh, 1993:

276) of low-yield neutron nuclear warheads and that at least three nuclear-capable artillery battalions were established after 1973 with self-propelled 175-mm cannons assigned more than 108 nuclear artillery shells. Additional nuclear artillery shells were supplied for Israel's 203-mm cannons. Moreover, Hersh claimed, the warhead that was tested in Israel's suspected nuclear test in 1979 "was a low-yield nuclear artillery shell that had been standardized for use by the Israeli Defense Force" (Hersh, 1993: 271). *The New York Times* reported these claims but also mentioned that the "formal" United States intelligence estimate was "fewer than 100" warheads, quoted the Carnegie Endowment as saying that most outsiders estimated as many as 200 warheads, but ended on Hersh's estimate of an Israeli stockpile of "300 or more" warheads (Brinkley, 1991).

Partly building on these claims, an article published in *Jane's Intelligence Review* in 1997 by photo-interpreter Harold Hough used commercial satellite photos to examine Israel's suspected missile base near the town of Zakharia. The article concluded that the base might house 50 Jericho II missiles and that five bunkers at a nearby depot were capable of storing 150 weapons. "This supports indications that the Israeli arsenal may contain as many as 400 nuclear weapons with a total combined yield of 50 megatons,") Hough (1997) asserted.[6]

The satellite photos were not very clear, however, and imagery experts later pointed out that "close examination of the published photos indicates that many of these identified features are not visually evident" leaving "large uncertainty associated with these identifications" (Gupta and Pabian, 1998: 97). Possibly indicating similar doubts, a *New York Times* article reminded readers that a Rand Corporation study commissioned by the Pentagon and reported by the Israeli daily newspaper *Haaretz* had concluded that Israel only had enough plutonium to make 70 nuclear weapons (Schmemann, 1998).

The Rand estimate was in the same range as the 60 to 80 nuclear warheads the US Defense Intelligence Agency (DIA) listed in a 1999 classified report (US Defense Intelligence Agency, 1999).[7] Leaked and later published in 2004, this report is to our knowledge the most recent publicly available document that provides an official estimate of how many nuclear warheads Israel has. The report, the timing of which coincided with the commissioning of the first of Israel's six Dolphin-class submarines, also contained a projection for the arsenal by 2020: 65 to 85 warheads.

During the 15 years that have passed since the DIA report, Israel presumably has continued production of plutonium at Dimona for some of that time (although the reactor is getting old) and probably also has continued producing nuclear warheads. Many of those warheads were probably replacements for warheads produced earlier for existing delivery systems, such as the Jericho II missiles and aircraft. Warheads for a rumored Jericho III ballistic missile would probably replace existing Jericho II warheads on a one-for-one basis. Warheads for the rumored submarine-based cruise missile, if true, would be in addition to the existing arsenal but probably only involve a relatively small number of warheads.

Warhead designs

The large variety of warhead designs that would be needed to arm the many different types of launchers rumored to exist—reentry vehicles for ballistic missiles, gravity bombs for aircraft, artillery, landmines, and a neutron bomb—would be a significant technical challenge for a nuclear weapons complex that has only conducted one nuclear test, or even a few tests, 35 years ago.

It took other nuclear weapon states dozens of elaborate nuclear test explosion experiments to develop such varied weapon designs—as well as the war-fighting strategies to justify the expense. According to some analysts, Israel had "unrestricted access to French nuclear test explosion data" in the 1960s (Cohen, 1998: 82–83), so much so that "the French nuclear test in 1960 made two nuclear powers not one" (Weissman and Krosney, 1981: 114–117). Until France broke off deep nuclear collaboration with Israel in 1967, France conducted 17 fission warhead tests in Algeria, ranging from a few kilotons to approximately 120 kilotons of explosive yield (*CTBTO*, n.d.; Nuclear Weapon Archive, 2001).

Based on interviews with Vanunu in 1986, Frank Barnaby, a nuclear physicist who worked at the British Atomic Weapons Research Establishment, later said that Vanunu's description of "production at Dimona of lithium-deuteride in the shape of hemispherical shells … raised the question of whether Israel had boosted nuclear weapons in its arsenal" (Barnaby, 2004: 4). Although he didn't think Vanunu had much knowledge about such weapons, Barnaby concluded that "the information he gave suggested that Israel had more advanced nuclear weapons than Nagasaki-type weapons" (Barnaby, 2004: 4).

Barnaby did not mention thermonuclear weapons in his 2004 statement, even though he concluded in his book *The Invisible Bomb* in 1989 that "Israel *may have* about 35 thermonuclear weapons" (Barnaby, 1989: 25). At the time, the director of the CIA apparently did not agree but reportedly indicated that Israel *may be seeking* to construct a thermonuclear weapon (Cordesman, 2005). Yet *The Samson Option* claims that US weapon designers concluded from Vanunu's information that "Israel was capable of manufacturing one of the most sophisticated weapons in the nuclear arsenal—a low-yield [two-stage] neutron bomb" (Hersh, 1993: 199). The authors of *The Nuclear Express* in 2009 echoed that claim, stating that the product of Israel's partnership with South Africa would be "a family of boosted primaries, generic H-bombs, and a specific neutron bomb" (Reed and Stillman, 2009: 174).

While a single-stage, boosted fission design warhead was probably within Israel's technical reach at the time, the claim that Israel also was capable of producing two-stage thermonuclear warhead designs, or even enhanced radiation weapons (which are also two-stage thermonuclear designs), is harder to accept, based on the limited information that is publicly available about Israel's nuclear testing and design history.

Whatever the composition of the Israeli nuclear arsenal, we neither see the indicators that Israel has sufficient nuclear-capable launchers for 200 to 400 nuclear weapons, nor understand why a country that does not have a strategy for fighting nuclear war would need that many types of warheads or warhead designs to deter its potential adversaries. In our assessment, a more credible estimate—taking into consideration plutonium production, testing history, design skills, force structure, and strategy—is an Israeli stockpile of approximately 80 boosted fission warheads.

Aircraft and airfields

Over the past 30 years, the Israeli Air Force (IAF) has had several types of US-produced aircraft capable of carrying nuclear gravity bombs. These include the A-4 Skyhawk, F-4 Phantom, and more recently the F-16 and F-15E. Moreover, Israel has purchased 20 F-35A Lightnings to replace older F-16s, and plans to buy more.

The A-4 and F-4 served long careers as nuclear strike aircraft in the US military, and their potential roles as similar nuclear weapons delivery vehicles within the IAF was the focus of much attention at the time they were in use. As noted earlier, when it bought these aircraft, Israel formally promised the United States that it "agrees not to use any aircraft supplied by the U.S. as a nuclear weapons carrier" (Embassy of Israel,1968: 1). But the experience with Israel's interpretation of its promise not to be the first to "introduce" nuclear weapons in the Middle East makes it hard to take its promise not to use American aircraft for nuclear missions without a pinch of salt.

Since the 1980s, the F-16 has been the backbone of the Israeli Air Force. Over the years, Israel has purchased well over 200 F-16s of all types, as well as specially configured F-16Is. Various versions of the F-16 serve nuclear strike roles in the US Air Force and among NATO allies, and the F-16 is the most likely candidate for air delivery of Israeli nuclear weapons at the present time.

Since 1998, Israel has also used the Boeing F-15E Strike Eagle for long-range strike and air-superiority roles. The Israeli version is characterized by greater takeoff weight—36,750 kg—and range—4,450 km—than other F-15 models. Its maximum speed at high altitude is Mach 2.5. The plane has been further modified with specialized radar that has terrain-mapping capability and other navigation and guidance systems. In the US Air Force, the F-15E Strike Eagle has been given a nuclear role. It is not known if the Israeli Air Force has added nuclear capability to this highly versatile plane.

Regardless of what happens with the F-15E, Israel has decided to replace a portion of its F-16 fleet with a new plane under development in the United States: the F-35A. In so doing, it will become the first non-US country to operate the aircraft. The first F-35A—the Israeli version will be known as the F-35I (named "Adir" for "awesome" or "mighty")—will arrive in 2017, with the first squadron expected to become operational at Nevatim Air Base in the Negev desert in 2018. Israel purchased 20 of an earlier F-35 design in 2012, and plans to buy over 100 of the new F-35Is, but the high cost of the F-35 might limit the plans. The F-35I will be adapted with Israeli weapons and has, unlike the F-15I and F-16I, the ability to fly long-range missions with internal weapons. The US Air Force is upgrading its F-35As to carry nuclear bombs, and Israel's Channel 2 reported that an unnamed "senior level US official" refused to say if Israel had requested such an upgrade for its F-35 s (Channel 2, 2014).

It is especially difficult to determine which Israeli wings and squadrons are assigned nuclear missions and which bases support them. The nuclear warheads themselves may be stored in underground facilities near one or two bases. Israeli F-16 squadrons are based at Ramat-David Air Base in northern Israel; Tel Nof and Hatzor air bases in central Israel; and Hatzerim, Nevatim, Ramon, and Ouvda air bases in southern Israel. Of the many F-16 squadrons, only a small fraction—perhaps one or two—would actually be nuclear-certified with specially trained crews, unique procedures, and modified aircraft. The F-15 s are based at Tel Nof Air Base in central Israel, and Hatzerim Air Base in the Negev desert. We cautiously suggest that Tel Nof Air Base in central Israel and Nevatim Air Base in the Negev desert have nuclear missions.

Land-based missiles

Israel's nuclear missile program dates back to the early 1960s. In April 1963, several months before the Dimona reactor began producing plutonium, Israel signed an agreement with the French company Dassault to produce a surface-to-surface ballistic missile. The missile system became known as the Jericho (or MD-620).

The first purchase of 30 missiles occurred in early 1966, but soon after the Six-Day War in June 1967 France imposed an embargo on new military equipment to Israel. Jericho production was transferred to Israel and the first two missiles delivered in 1968, with 10 more by mid-1969. The program was completed around 1970 with 24 to 30 missiles. Apparently not all were nuclear, with only 10 of the missiles "programmed for nuclear warheads," according to the White House (Department of State, 1968: 2; White House, 1969a: 1).[8] Apparently, the other missiles could be armed with chemical warheads, probably nerve gas (White House, 1969c). The short-range Jericho could deliver a 1,000-kilogram (2,200 pound) reentry vehicle, with a range of about 480 kilometers (298 miles). The accuracy was estimated to be roughly within 926 meters (approximately 0.6 miles) of its target (CIA, 1974: 22).

Most sources assert that Jericho was a *mobile* missile, transported and fired from a transportable erector launcher (CIA, 1974). But there have occasionally been references to possible silos for the weapon. A US State Department study produced in support of National Security Study Memorandum 40 in May 1969 concluded that Israel believed it needed a nearly invulnerable nuclear force to deter a nuclear first strike from its enemies, "i.e., having a second-strike capability." The study stated: "Israel is now building such a force—*the hardened silos of the Jericho missiles*" (Department of State, 1969d: 7; emphasis added). It is not clear that the claim of "hardened silos" constituted the assessment of the US intelligence community, and only a few subsequent sources—all non-governmental—have mentioned Israeli missile silos.[9] We did not find any public evidence of Jericho silos.

The Jericho range was sufficient to target Cairo, Damascus, and all of Jordan, but not the Soviet Union—which was gaining importance in Israel's planning. In collaboration with South Africa, Israel in the late 1980s developed the medium-range Jericho II that put the southern-most Soviet cities and the Black Sea Fleet within range. Jericho II, a modified version of the Shavit space launch rocket, was first deployed in the early-1990s, replacing the first Jericho.

Unofficial estimates of the Jericho II's range vary greatly and tend to be exaggerated—some even up to 5,000 kilometers (3,100 miles).[10] The Jericho was first flight-tested in May 1987 to approximately 850 km (527 miles). The trajectory went far into the Mediterranean Sea. Another test in September 1989 reached 1,300 km (806 miles). The US Air Force National Air Intelligence Center in 1996 reported the Jericho II range as 1,500 kilometers (930 miles) (NAIC, 1996).

Half of Iran, which has increased in importance to Israeli military strategy over the past two decades, is out of Jericho II's reach. That includes Tehran (barely). Rumors abound that

Israel has been developing a longer-range missile, publicly known as Jericho III, with an estimated range of 4,000 kilometers, or 2,480 miles. With such a missile, Israel would be able to target all of Iran, Pakistan, and all of Russia west of the Urals—including, for the first time, Moscow. Jericho III was first test-launched over the Mediterranean Sea in January 2008, again in 2011, and most recently in July 2013. Unidentified defense sources told *Jane's Defence Weekly* that Jericho III constitutes "a dramatic leap in Israel's missile capabilities" (*Jane's Defence Weekly*, 2008: 5), but many details and current status are unknown.

How many Jericho missiles Israel has is another uncertainty. Estimates vary from 25 to 100. Most sources estimate that Israel has 50 of these missiles, and place them at the Sdot Micha facility near the town of Zakharia in the Judean Hills approximately 27 kilometers, or about 17 miles, east of Jerusalem. (There are many alternative spellings and names for the base, including Zekharyeh, Zekharaia, Sdot Micha, and Sdot HaElla.)

Commercial satellite images show what appear to be two clusters of what might be caves for mobile Jericho II launchers. The northern cluster includes 14 caves and the southern cluster has nine caves, for a total of 23 caves. This number of caves roughly matches the 24 to 30 missiles mentioned in a 1969 White House memo (White House, 1969a). Each cluster also has what appears to be a covered drive-through facility, potentially for missile handling or warhead loading. A separate circular facility with four tunnels to underground facilities could potentially be for warhead storage. Consequently, we conclude that estimates of 50 to 100 missiles are exaggerated and estimate that Israel deploys about two dozen mobile launchers for Jericho missiles.

Most reports only mention one missile site, but a US State Department background paper from 1969 stated that there was "evidence strongly indicating that *several sites* providing operational launch capabilities are virtually complete" (Department of State, 1969c: 4; emphasis added). The Sdot Micha base is relatively small at 16 square kilometers, and the suspected launcher caves are located along two roads, each of which is only about one kilometer long. Although this layout would provide protection against limited conventional attacks, it would be vulnerable to a nuclear surprise attack. For the Jericho missiles to have military value, they would need to be able to disperse from their caves.

Sea-based missiles and submarines

Rumors abound that Israel has developed a nuclear warhead for a sea-launched cruise missile, which would be launched from diesel-electric Dolphin-class attack submarines that Israel has acquired from Germany. Some rumors say that the nuclear-capable sea-launched cruise missile is a modification of the conventional "Popeye Turbo" air-to-surface missiles, while others claim that Israel converted the US-supplied Harpoon—a long-standing US anti-ship missile—to nuclear capability.

It is difficult to say with certainty when the rumors first emerged or where, but one early candidate is a Center for Strategic and International Studies study from 1998, which listed: "Variant of the Popeye air-to-surface missile believed to have nuclear warhead" (Cordesman, 1998: 17). There was no source for the claim, but it quickly made its way into *The Washington Times* under the headline "Israel buying 3 submarines to carry nuclear missiles." The article also referenced a June 8, 1998 report in the Israeli paper *Haaretz* "that Israeli military planners want to mount nuclear-armed cruise missiles on the new submarines" (Sieff, 1998).

An article published by Gerald M. Steinberg from Bar Ilan University in *RUSI International Security Review* in 1999 described "unconfirmed reports that Israel is developing a cruise missile (known as the Popeye Turbo) with a range of 350 kilometers, to be operational in 2002," that "could become the basis of a sea-based second strike deterrent" (Steinberg, 1999: 215–224).

When the Clinton administration proposed returning the Golan Heights to Syria, the Israeli government responded with a $17 billion security package request that included 12 long-range BGM-109 Tomahawk sea-launched cruise missiles. (The US Navy possessed a nuclear-armed version of the Tomahawk between 1983 and 2012.) Israel argued that it would need the Tomahawk to compensate for the loss of strategic depth if it gave up the Golan Heights, although targeting Iran was clearly also a factor. But the Clinton administration turned down the Israeli request in March 2000.

Only three months later, in June 2000, an article in the *Sunday Times* quoted unnamed "Israeli defense officials" as saying that Israel had secretly tested a submarine-launched cruise missile to a range of more than 1,500 kilometers (930 miles) in the Indian Ocean (Mahnaimi and Campbell, 2000).

The reports about a nuclear Popeye cruise missile and a 1,500-kilometer cruise missile test were soon conflated into one missile, which has been referred to as fact in numerous publications ever since. After the widely respected book *Deadly Arsenals* printed this information in June 2002 (Cirincione et al., 2002), coverage in *The Washington Post* added unnamed former Pentagon and State Department officials who confirmed that Israel was arming three newly acquired diesel submarines with "newly designed cruise missiles capable of carrying nuclear warheads." The report said the US Navy monitored the Israeli cruise missile test, although a former Pentagon official cautioned: "It is above top secret knowing whether the sub-launched cruise missiles are nuclear-armed" (Pincus, 2002).

The lead author of the *Sunday Times* cruise missile test article, Uzi Mahnaimi, has written other articles about Israel's nuclear capabilities, some of which later turned out to be incorrect. A 2007 article claimed "several Israeli military sources" had told the *Sunday Times* that two Israeli air force squadrons were training to blow up an Iranian facility using low-yield nuclear "bunker-busters" (Mahnaimi and Baxter, 2007). In 2010, Mahnaimi claimed "the decision has now been taken" to continuously deploy at least one of Israel's "submarines equipped with nuclear cruise missiles … in the Gulf near the Iranian coastline." The article quoted an unidentified navy officer saying that the "1,500-km range of the submarines' cruise missiles can reach any target in Iran" (Mahnaimi, 2010). These and other articles have caused media critics, including Marsha B. Cohen on PBS's *Frontline*, to describe Mahnaimi as a "sensationalist" with "a long and consistent record—for being wrong" (Cohen MB, 2010).

Up until 2002, news media reports focused on a naval version of the air-launched Popeye Turbo missile. But in October 2003 the *Los Angeles Times* quoted unnamed US and Israeli officials saying that Israel had modified the US-supplied Harpoon cruise missile to carry nuclear warheads on submarines. "Two Bush administration officials described the missile modification and an Israeli official confirmed it," the paper stated (Frantz, 2003).

This added to the mystery because the range of the Harpoon is even shorter than the range of the Popeye Turbo (110-plus kilometers, or about 68 miles, versus 300-plus kilometers, or about 186 miles). Former Israeli Deputy Defense Minister Efraim Sneh dismissed the Harpoon story: Anyone with even the slightest understanding of missiles knows that the Harpoon can never be used to carry nuclear warheads. Not even [Israel's] extraordinarily talented engineers and its sophisticated defense industries can transform the Harpoon into a missile capable of doing this. It's simply impossible. (Haaretz, 2003)

Sneh's claim that "the Harpoon can never be used to carry nuclear warheads" is not entirely correct. Between 1973 and 1980, the United States considered equipping the Harpoon with a nuclear warhead, but the program was terminated (Cochran et al., 1984). Israel's nuclear weapons engineering capability is much less advanced than that of the United States, and the Pentagon's Defense Security Cooperation Agency, which oversees US military sales abroad, told *Arms Control Today* that although Israel's contract for Harpoon missiles does not explicitly prohibit Israel from modifying them to carry nuclear warheads, "we have had no reason to believe that the government of Israel had any intention to modify or substitute the warheads of these missiles" (Boese, 2003).

Contrary to the Harpoon rumor, the normally well-informed Avner Cohen writes in *The Worst-Kept Secret* that the submarine cruise missile developed for Israel's sea-based strategic leg of its nuclear deterrent has been "developed and built in Israel" (Cohen A, 2010: 83).

Israel plans to operate six Dolphin-class submarines. The last three submarines are 10 meters (approximately 33 feet) longer than the first three due to the addition of an improved air-independent propulsion system. After delivery of the first three submarines, rumors of nuclear capability reportedly prompted Germany to demand that Israel assure that the additional submarines it wanted would not be carrying nuclear weapons (Ben-David, 2005).

Whether the German demand was actually made remains unknown, but in 1999, after delivery of the first Dolphin submarine, then-Prime Minister Ehud Barak told the National Defense College that the submarines "add an important component to Israel's long arm" (Barak, 1999). And the Israeli defense force chief of staff made it clear in 2005 that Israel was modifying its military capabilities in response to Iran's suspected nuclear weapons ambitions. "We cannot sit indifferent in the face of the combination of an irrational regime with non-conventional weapons. We have to concentrate all our efforts to create different capabilities that would allow us both to defend and to react" (Ben-David, 2005: 4).

Colonel Yoni, the head of the Israeli submarine fleet, in 2006 refused to comment on reports about the submarines' rumored nuclear capability but added that "hitting strategic

targets is not always a task the Air Force or the infantry can carry out … a submarine can perform the mission," he explained. "The fact that foreign reports refer to the submarines as a deterring factor says something" (Greenberg, 2006).
In June 2009, Israeli defense sources reported that the INS *Leviathan*—one of the first three diesel-electric Dolphin-class submarines but *without* the air-independent propulsion of later purchases of submarine—had sailed through the Suez Canal on its way to a naval exercise. Some news media reported the submarine sailed for an exercise in the Persian Gulf, but instead it docked at the Israeli naval base at Eilat in the Red Sea. Speculations erupted about the deployment being a signal to Iran and therefore indirectly a confirmation of the Dolphin-submarine's rumored nuclear capability, and that Israel might deploy submarines permanently at Eilat. But an Israeli defense official said there would be no permanent submarine deployment in Eilat: "If anything, we are scaling down our naval operations in Eilat" (Haaretz, 2009).
Even so, an article published by the *Sunday Times*—written by the same reporter that wrote the article about the 1,500-km cruise missile test and the plans to bomb Iran with low-yield nuclear bombs—claimed that Israel had made a decision "to ensure a permanent presence of at least one" of the Dolphin-class submarines in the Persian Gulf "near the Iranian coastline" (Mahnaimi, 2010).
The German magazine *Der Spiegel* reported in 2012 that the German government had known for decades that Israel planned to equip the submarines with nuclear missiles. Former German officials said they always assumed Israel would use the submarines for nuclear weapons, although the officials appeared to confirm old rumors rather than provide new information. The article quoted another unnamed ministry official with knowledge of the matter: "From the beginning, the boats were primarily used for the purposes of nuclear capability" (*Der Spiegel*, 2012).

Setting the record straight

From these examples, it should be apparent that there is much that is unclear about what kind of nuclear weapons Israel has, how many there are, under what circumstances they would be used, or how they would be delivered to their targets. All Israeli governments have preferred to keep this information secret. Nevertheless, from our examination of the publicly available information, we conclude that widespread claims of an Israeli nuclear stockpile of 200 to 400 warheads and 50 to 100 Jericho missiles are exaggerated.

In our assessment, based on analysis of available sources and examination of commercial satellite imagery, we estimate that Israel has a stockpile of approximately 80 nuclear warheads for delivery by two dozen mobile Jericho missiles, a couple of squadrons of aircraft, and perhaps a small inventory of sea-launched cruise missiles. Much uncertainty remains, however, about the structure and diversity of Israel's nuclear arsenal because of Israel's policy of keeping its nuclear capability ambiguous and because other countries don't reveal some of what their intelligence communities know.
Despite Israel's stated policy that it will not be the first to introduce nuclear weapons in the Middle East, there is little doubt that Israel has already introduced nuclear weapons in the region and that only a deception based on a narrow interpretation of what constitutes "introduction" keeps Israel from officially being a nuclear weapon state. Thanks to invaluable research by researchers such as Avner Cohen and William Burr, previously unknown nuances of Israel's opaque nuclear policy have become available to the public.

▶ **Links, notes and references are available at source's URL.**

Hans M. Kristensen *is the director of the Nuclear Information Project with the Federation of American Scientists (FAS) in Washington, DC, USA. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a co-author of the world nuclear forces overview in the SIPRI Yearbook (Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has co-authored Nuclear Notebook since 2001.*

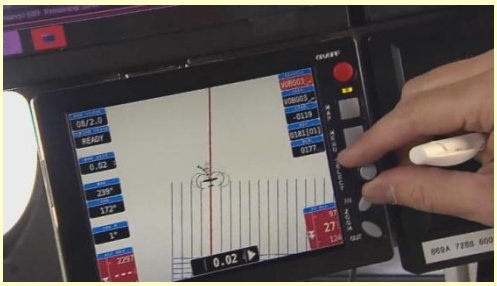
Robert S. Norris *is a senior fellow with the Federation of American Scientists in Washington, DC, USA. A former senior research associate with the Natural Resources Defense Council, his principal areas of expertise include writing and*

research on all aspects of the nuclear weapons programs of the United States, the Soviet Union and Russia, the United Kingdom, France, and China, as well as India, Pakistan, and Israel. He is the author of Racing for the Bomb: General Leslie R. Groves, the Manhattan ProjectÕs Indispensable Man (Steerforth, 2002) and co-author of Making the Russian Bomb: From Stalin to Yeltsin (Westview, 1995). He co-authored or contributed to the chapter on nuclear weapons in the 1985"2000 editions of the SIPRI Yearbook (Oxford University Press) and has co-authored Nuclear Notebook since 1987.

CTBTO is conducts largest ever Weapons of Mass Destruction exercise

Source: http://en.cihan.com.tr/news/CTBTO-is-conducts-largest-ever-Weapons-of-Mass-Destruction-exercise_4067-CHMTU5NDA2Ny80

November 18 – **The Comprehensive Test Ban Treaty Organization (CTBTO) is conducting the "largest ever" Weapons of Mass Destruction (WMD) exercise in Jordanian dessert to develop its "On Site Inspection" capabilities for when the Treaty comes into force.**



The organizers have made the exercise as close a simulation to a real On Site Inspection as possible. The environment is very challenging, with a very rugged terrain ranging from 400m below sea level to 1000m above.

"On Site Inspection is a specific verification element. It is really the last verification measure which will allow member states to verify if an ambiguous event that happened is of a nuclear nature or not." CTBTO On Site Inspection Coordinator Matjaz Prah says.

The exercise has involved transporting approximately 150 tonnes of equipment from the CTBTO headquarters in Vienna, Austria, to the base of operations near the Dead Sea in Jordan.

Over 200 individuals are taking part, 40 of them playing the part of inspectors, and the remainder supporting or evaluating the project. Individual participants will apply the various techniques that would be used in a real life inspection.

The inspection team can deploy up to five independent field missions each inspection day. They must investigate an area of 1000 square kilometers with the aim of finding a ground zero that might be no more than a couple of meters across.

The Comprehensive Nuclear-Test-Ban Treaty (CTBT) bans nuclear explosions by everyone, everywhere, and it has been ratified by 163 states including the three of nuclear states: France, UK and Russian Federation. However, for the Treaty to enter

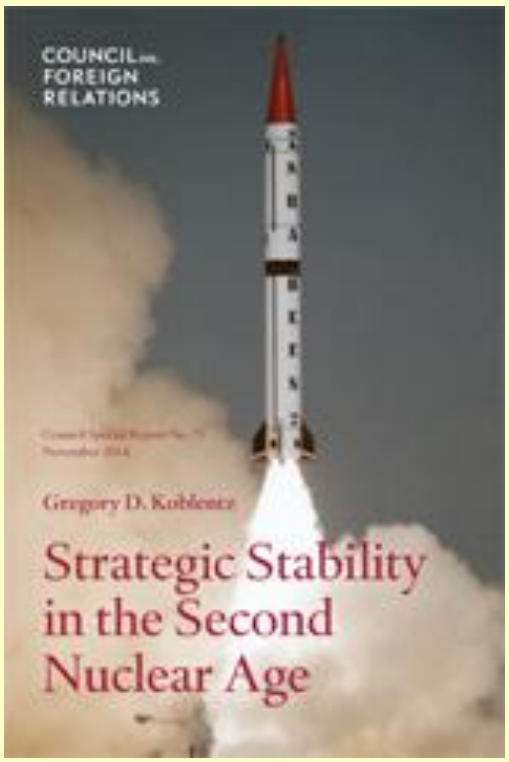
into force, further 44 states with nuclear technology need to sign and ratify the Treaty.

Strategic Stability in the Second Nuclear Age

By Gregory D. Koblentz

Source: http://www.cfr.org/arms-control-disarmament-and-nonproliferation/strategic-stability-second-nuclear-age/p33809

Since the end of the Cold War, a new nuclear order has emerged, shaped by rising nuclear



states and military technologies that threaten stability, writes George Mason University's **Gregory Koblentz** in a new Council Special Report.

During the Cold War, the potential for nuclear weapons to be used was determined largely by the United States and the Soviet Union. Now, with 16,300 weapons possessed by the seven established nuclear-armed states—China, France, India, Pakistan, Russia, the United Kingdom, and the United States—deterrence is increasingly complex. Since most of these countries face threats from a number of potential adversaries, "changes in one state's nuclear policy can have a cascading effect on the other states."

Though many states are downsizing their stockpiles, Asia is witnessing a buildup; Pakistan has the fastest-growing nuclear program in the world. By 2020, it could have a stockpile of fissile material that, if weaponized, could produce as many as two hundred nuclear devices. The author identifies South Asia as the region "most at risk of a breakdown in strategic stability due to an explosive mixture of unresolved territorial disputes, cross-border terrorism, and growing nuclear arsenals."

Emerging technologies such as missile defenses, cyber and antisatellite weapons, and conventional precision strike weapons pose additional risks, Koblentz warns, and could potentially spur arms races and trigger crises.

"The United States has more to lose from a breakdown in strategic stability than any other country due to its position as a global leader, the interdependence of its economy, and the network of security commitments it has around the world," he asserts. The United States and Russia still possess more than 90 percent of the world's nuclear weapons. Despite the increasing chill in U.S.-Russia relations, Washington's highest priority should be to maintain strategic efforts with Russia and China, the two states with the capability and potential intent to launch a nuclear attack on the American homeland.

The United States should work with other nuclear states to address sources of instability in the near term and establish processes for multilateral arms control efforts over the longer term, writes Koblentz. **He urges the Obama administration to**

- enhance initiatives that foster transparency, confidence-building, and restraint to mitigate the risk that emerging technologies will trigger arms races, threaten the survivability of nuclear forces, or undermine early warning and nuclear command and control systems;
- deepen bilateral and multilateral dialogues with the other nuclear-armed states; and
- create a forum for the seven established nuclear-armed states to discuss further steps to reduce the risk of deliberate, accidental, or unauthorized use of nuclear weapons.

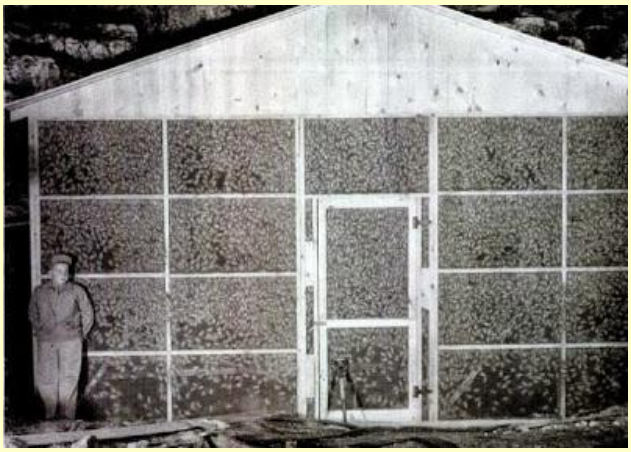
▶ **Read the full report from source's URL** (under the cover photo)

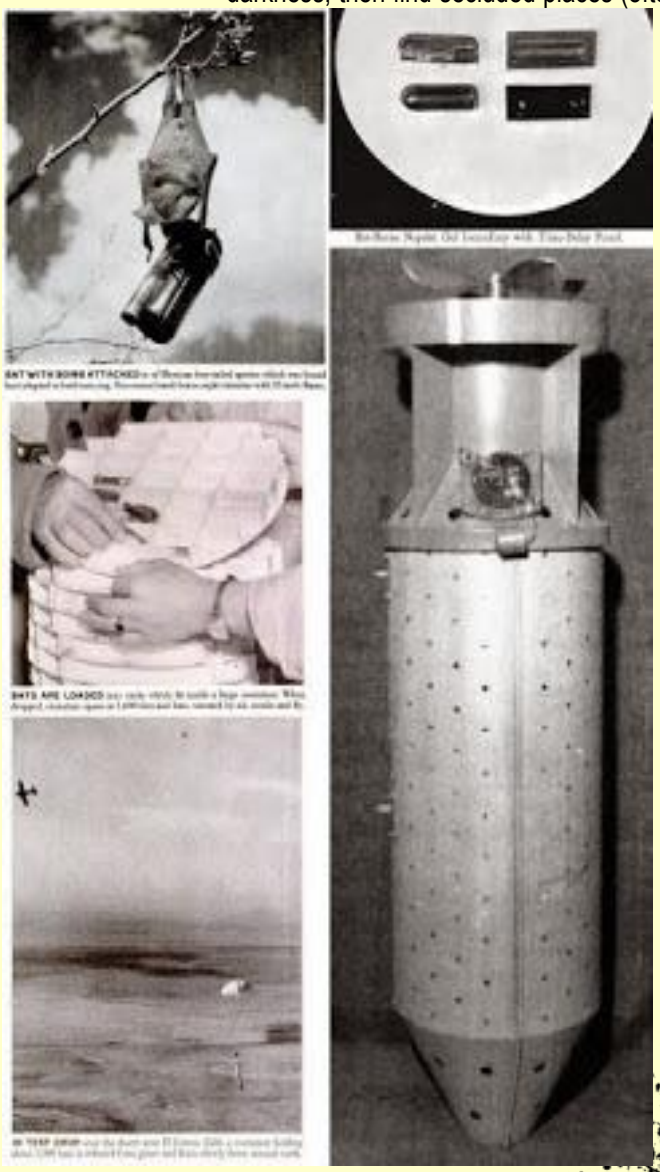
Gregory D. Koblentz *is an associate professor in the School of Policy, Government, and International Affairs and deputy director of the biodefense graduate program at George Mason University. Koblentz is a research affiliate with the security studies program at the Massachusetts Institute of Technology and a member of the scientist working group on chemical and biological weapons at the Center for Arms Control and Non-Proliferation in Washington, DC. During 2012–2013, he was a Stanton Nuclear Security Fellow at the Council on Foreign Relations. Previously, he worked at Georgetown University, Harvard University's Kennedy School of Government, and the Carnegie Endowment for International Peace. Koblentz has published in international security journals including* International Security, Survival, Contemporary Security Policy, International Affairs, Bioterrorism and Biosecurity, *and* Nonproliferation Review. *He is the author of* Living Weapons: Biological Warfare and International Security *and coauthor of* Tracking Nuclear Proliferation: A Guide in Maps and Charts. *He received an MPP from the John F. Kennedy School of Government at Harvard University and a PhD from the Massachusetts Institute of Technology.*

Bat bomb

Source: http://en.wikipedia.org/wiki/Bat_bomb

Bat bombs were an experimental World War II weapon developed by the United States. **The bomb consisted of a bomb-shaped casing with numerous compartments, each containing a Mexican Free-tailed Bat with a small timed incendiary bomb attached.** Dropped from a bomber at dawn, the casings would deploy a parachute in mid-flight and open to release the bats which would then roost in eaves and attics. The incendiaries would start fires in inaccessible places in the largely wood and paper construction of the Japanese cities that were the weapon's intended target.





Overview

The Bat Bomb was originally conceived by a Pennsylvania dentist named Lytle S. Adams, a friend of First Lady Eleanor Roosevelt. Dr. Adams submitted it to the White House in January 1942, where it was subsequently approved by President Roosevelt on the advice of Donald Griffin.

Adams observed that the infrastructure of Japan was especially susceptible to incendiary devices as many of the buildings were made of paper, bamboo, and other highly flammable material. The plan was to release bat bombs over Japanese cities having widely-dispersed industrial targets. The bats would spread far from the point of release due to the relatively high altitude of their release, then at dawn they would hide in buildings across the city. Shortly thereafter built-in timers would ignite the bombs, causing widespread fires and chaos.

The United States decided to develop the Bat Bomb during World War II as four biological factors gave promise to this plan. First, bats occur in large numbers (four caves in New Mexico are each occupied by several million bats). Second, bats can carry more than their own weight in flight (females carry their young—sometimes twins). Third, bats hibernate, and while dormant they do not require food or maintenance. Fourth, bats fly in darkness, then find secluded places (often

in buildings) to hide during daylight.

Project details

Errant bats from the experimental Bat Bomb set the Carlsbad Army Airfield Auxiliary Air Base, New Mexico on fire.

By March 1943 a suitable species had been selected. The project was considered serious enough that Louis Fieser, the inventor of military napalm, designed 0.6 ounce (17 g) and one ounce (28 g) incendiary devices to be carried by the bats. A bat carrier similar to a bomb casing was designed that included 26 stacked trays, each containing compartments for 40 bats. **The carriers would be dropped from 5,000 feet (1,525 m). Then the trays would separate but remain connected to a parachute that would deploy at 1,000 feet (305 m). It was envisioned that ten B-24 bombers flying from Alaska, each carrying a hundred shells packed with bomb-carrying bats could release 1,040,000 bat bombs over the target—the industrial cities of Osaka Bay.** A series of tests to answer various operational questions were conducted. In one incident the Carlsbad Army Airfield Auxiliary Air Base 32°15'39"N 104°13'45"W near Carlsbad, New Mexico, was set on fire on May 15, 1943, when armed bats were accidentally released. The bats incinerated the test range and roosted under a fuel tank.

Following this setback, the project was relegated to the Navy in August 1943, **who renamed it Project X-Ray**, and then passed it to the Marine Corps that December. The Marine Corps moved operations to the Marine Corps Air Station at El Centro, California. After several experiments and operational adjustments, the definitive test was carried out on the "**Japanese Village**" a mockup of a Japanese city built by the Chemical Warfare Service at their Dugway Proving Grounds test site in Utah.

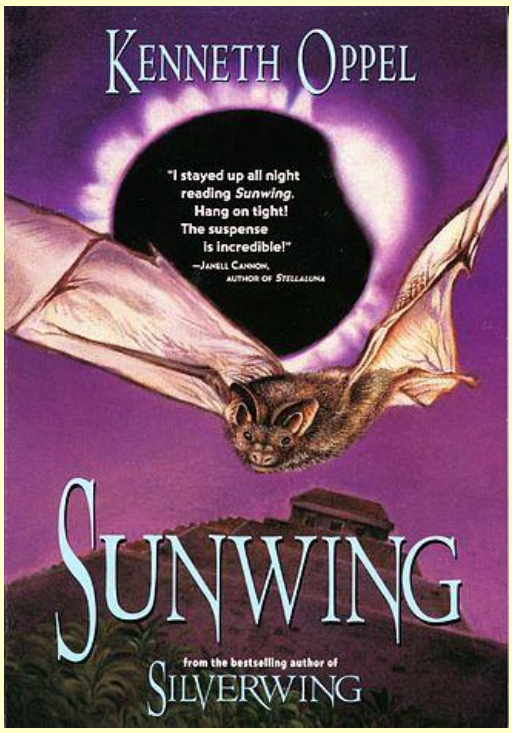
Observers at this test produced optimistic accounts. The chief of incendiary testing at Dugway wrote: "A reasonable number of destructive fires can be started in spite of the extremely small size of the units. The main advantage of the units would seem to be their placement within the enemy structures without the knowledge of the householder or fire watchers, thus allowing the fire to establish itself before being discovered." The National Defense Research Committee (NDRC) observer stated: "It was concluded that X-Ray is an effective weapon." The Chief Chemist's report stated that on a weight basis X-Ray was more effective than the standard incendiary bombs in use at the time. **"Expressed in another way, the regular bombs would give probably 167 to 400 fires per bomb load where X-Ray would give 3,625 to 4,748 fires".**

More tests were scheduled for the summer of 1944 but the program was cancelled by Fleet Admiral Ernest J. King when he heard that it would likely not be combat ready until mid-1945. By that time it was estimated that $2 million had been spent on the project. It is thought that development of the bat bomb was moving too slowly, and was overtaken in the race for a quick end to the war by the atomic bomb project.

Dr. Adams maintained that the bat bombs would have been effective without the devastating effects of the atomic bomb.

He is quoted as having said: ***Think of thousands of fires breaking out simultaneously***

over a circle of forty miles in diameter for every bomb dropped.
Japan could have been devastated, yet with small loss of life.



The infamous "Invasion by Bats" project was afterwards referred to by Dr. Stanley P. Lovell, director of research and development for Office of Strategic Services (OSS), whom General Donovan ordered to review the idea, as "Die Fledermaus Farce". Lovell also mentioned that bats during testing were dropping to the ground like stones.

Cultural influence

- The book ***Sunwing*** written by Kenneth Oppel was inspired by this plan.
- The song "The Story Of The Japanese Bat Bomb" from the 2008 LP *Doris, Buzz and Friends*, written by John Krane, is also based on this plan, though it projects that its inventor was saddened by the bombs imminent detonation (there is no evidence of such conflict).
- Adams and his bat bomb project are the subject of Derrick C. Brown's poem, "The Project Known as X-Ray," collected in *Scandalabra.*
- Alan Scott's novel *The Anthrax Mutation* (original title, *Project Dracula*) used the "Bat Bomb" concept, but had the bats carrying volatile pouches full of powdered anthrax bacilli—a genetically-engineered strain of anthrax made to be very infective and very resistant to the effects of sunlight and temperature. The pouches fall free of the bomb casing and disintegrate once free of the low-oxygen environment inside the bomb; once in the air, the bats fly free and find niches to sleep in during the day, presumably in homes and offices.

Lobster's Sense of Smell Could Help Detect Explosives: UF Researchers

Source: http://www.nbcmiami.com/news/local/Lobsters-Sense-of-Smell-Could-Help-Detect-Explosives-250628481.html

Researchers at the University of Florida say a lobster's sense of smell could one day help protect soldiers from landmines and other explosives.

UF researchers have discovered that a type of olfactory neuron in lobsters constantly discharges small bursts of electronic pulses that may help them find an odor's location when they search for food or try to avoid danger.

Now the researchers say that ability, which they call "lobster radar" could help them develop improved electronic "noses" to detect explosives.

"An electronic nose has to recognize an odor and locate its source. Finding the source has often been the job of the person handling the electronic nose," said Barry W. Ache, director of the Center for Smell and Taste in UF's Evelyn F. and William L. McKnight Brain Institute.

The "lobster radar" can pinpoint a smell the same way a human can hear a train moving left to right. The finding by UF's researchers could also help scientists better understand the sense of smell in all animals, including humans.
"The involvement of bursting sensory neurons in olfactory processing is not unique to the lobster," Yuriy Bobkov, of the UF Whitney Laboratory for Marine Bioscience, said in a statement. "It's likely to be a fundamental aspect of olfaction."

IUPUI study reveals how dogs detect explosives, offers new training recommendations

Source:http://www.sciencecodex.com/iupui_study_reveals_how_dogs_detect_explosives_offers_new_training_recommendations-128779

A research team at Indiana University-Purdue University Indianapolis (IUPUI) has helped determine the science behind how canines locate explosives such as Composition C-4 (a plastic explosive used by the U.S. military). **The study found the dogs react best to the actual explosive, calling into question the use of products designed to mimic the odor of C-4 for training purposes.** These findings are the culmination of a four-year contract funded by the U.S. Department of Defense (DOD).

"Appropriately, dogs that are trained to find real explosives are going to find real explosives and not much else," said John Goodpaster, Ph.D., associate professor of chemistry and chemical biology and director for the Forensic and Investigative Sciences Program in the School of Science at IUPUI.

In this photo, a law enforcement dog participates in a field trial led by the School of Science at Indiana University-Purdue University Indiana-polis. The study found the dogs react best to actual explosive, calling into question the use of products designed to mimic the odor of C-4 for training purposes. (Photo Credit: Image courtesy of the Indiana University-Purdue University Indianapolis School of Science)

The effectiveness of trained detector dogs is well established, but the study sought to determine which chemical compounds cause a dog to recognize a particular explosive and alert to it. Previous studies have suggested that certain non-explosive chemicals emitted by Composition C-4 cause dogs to alert, and that these specific chemicals could be used as mimic substances to train the dogs in place of real explosives.

In the first phase of the study, IUPUI researchers discovered that the non-explosive chemicals given off by C-4 mimics also are present in a variety of everyday plastic objects. Objects tested included PVC pipes, electrical tape, movie tickets, a plastic grocery bag and plastic food wrapping. Several of the tested items emitted appreciable levels of a mimic compound recommended by some vendors for training canines.

The second phase exposed 33 trained canines from the DOD, Department of Justice, Amtrak and other agencies to these vapors to see if the dogs would respond. The field trials demonstrated that the dogs failed to respond in any significant way to specific odor compounds found in C-4. The results indicate that if the dogs are trained on the full scent, they will only detect real explosives.

"The canines are not easily fooled—you can't pick and choose components of explosive odors and expect the dog to respond," Goodpaster said. "Dogs are specific and it's the full scent that causes them to alert."

The study also sought to better establish the scientific facts needed for canine detection to be legally admissible evidence—an effort that found using mimic compounds could present challenges in court. By training with real explosives, false positives are unlikely in the field. Overall, the team recommended that dogs be trained with actual, not mimic, explosives.

While there is technology available to search for explosives, canines remain the best option because of their speed, sensitivity and ability to search large numbers of items, Goodpaster said. Co-authors on the study include current and former IUPUI School of Science undergraduate and graduate students: William Kranz, Kelley Kitts, Nicholas Strange, Joshua Cummins and Erica Lotspeich.

Fake bomb belt woman has reduced jail term upheld at Dubai Cassation Court

Source: http://www.thenational.ae/uae/courts/fake-bomb-belt-woman-has-reduced-jail-term-upheld-at-dubai-cassation-court

November 03 – The woman who wore a fake bomb belt to prosecution headquarters and threatened to detonate it has had her reduced jail term upheld.

Zulvia Hamraeva, 33, was sentenced to seven years by Dubai Criminal Court but then had the sentence reduced to two years on appeal.

The woman, from **Uzbekistan**, then appealed again but Dubai Cassation Court on Monday morning ruled that the two-year sentence will stand.

Her Emirati accomplice, M Y A, 28, who also appealed his two-year sentence for aiding and abetting Hamraeva by making the belt had his term reduced to one year by the appeal court, a term upheld by the cessation court on Monday.

Hamraeva was convicted of threatening to detonate the bomb belt at the prosecution building on September 1 last year. She was also convicted of threatening police and prosecution workers to force them into conducting a DNA test to prove that an Emirati man is the father of her 10-year-old son. In addition, she was found guilty of deliberately endangering the lives and safety of people and spreading terror among them by making bomb threats.

Before the terror alert, the Uzbek sent a picture of the fake bomb to J S A, 49, the man she claimed was the father of her son. Then she threatened to set it off if the DNA test was not carried out to prove his paternity.

The Emirati man testified that her met Hamraeva in 2003 and, 10 days later, she claimed she was pregnant by him.

An Ajman court acquitted him and jailed Hamraeva for one month for adultery. Three years later, she filed another case, this time at a Sharjah court, but again J S A was acquitted.

"On August 20 last year she sent me the picture of the belt but I didn't take the threat seriously," said J S A, adding that she asked for him to admit he is the father, as well as demanding Dh3 million and a villa.

Both the Uzbek and her accomplice denied all charges in all three courts.

Records stated that when Hamraeva opened up her abaya in the centre of the prosecution building and made the bomb threats, people were terrified and started rushing outside.

"Her belt looked very much real with its wire hooked to a detonator. This happened for the first time in the UAE and it's so grave — others may try to do like she did," said M A A, a negotiator who worked with the woman.

After nearly 13 hours of negotiations, she surrendered and the belt was found to be an elaborate fake.

Hamraeva will still be deported after serving her sentence, a decision upheld by both the appeal and cassation courts.

U.S. strike kills Khorasan Group's chief bomb-maker

Source: http://www.homelandsecuritynewswire.com/dr20141106-u-s-strike-kills-khorasan-group-s-chief-bombmaker

November 06 – **U.S. airstrikes in Syria overnight successfully hit a group of al-Qaeda-affiliated militants, killing the group's top bomb-maker.**

David Drugeon, a French Islamist militant, was killed along with other Khorasan Group members near Saramada, a town eighteen miles northeast of Idlib in Syria's northwest. Drugeon escaped an earlier U.S. airstrike, on 22 September, which was aimed to take him out.

Gen. Lloyd Austin, the Central Command commander in charge of U.S. military operations in the Middle East, speaking in an unrelated forum in Washington earlier today, said he would not discuss the strikes, but suggested Drugeon may have been targeted.

"He is clearly one of the leadership elements and one of the most dangerous elements in that organization," Austin said. "And so any time we can take their leadership out, it's a good thing."

***Al Arabiya* reports that one U.S. official said Drugeon's bomb-making skills were nearly as worrisome as those of Ibrahim al-Asiri, a member of al-Qaeda's Yemen affiliate who has built three nonmetallic devices which were smuggled onto U.S.-bound commercial planes. None detonated.**

Drudgeon was born in 1989 in Vannes on the Atlantic coast of Brittany. He grew up in a blue-collar and immigrant neighborhood on the outskirts of town, where social housing dominated the landscape. Eric Pelletier, a reporter with *L'Express*, reports that Drugeon had a normal childhood. His father was a bus driver and his mother a secretary and committed Catholic.

His life became less steady when his parents' divorce when he was 13, an experience many of his friends describe as traumatic for the young Drudgeon. He began acting out, and his grades at school nosedived. He began hanging out with a group of young Muslims in the neighborhood who adopted a fundamentalist interpretation of Islam. Before he turned 14 he converted to Islam, changing his name to Daoud.

He traveled to Egypt to study Arabic, and traveled to Afghanistan and Pakistan several times. According to Pelletier, French intelligence established that Drugeon joined a small al-Qaeda subgroup known as Jund-al-Khilafah based in the Miran Shah area of Pakistan.

In late 2013, together with several members of Jund-al-Khilafah, he moved to Syria to help form the Khorasan Group, becoming the group's top bomb-maker.

CNN reports that the innovative Drudgeon was designing bombs made out of clothing dipped in explosive solution and explosives concealed in personal electronics.

In July, the Transportation Security Administration (TSA) banned cell phones without electronic charge from airplane cabins in response to the intelligence coming in about Drudgeon's designs, much of it fragmentary.

Army Col. Steve Warren said at the Pentagon that the strikes hit five targets at two locations. Warren said that the Khorasan Group was the pre-planned target of the strikes. The Khorasan Group, he said, "is a group of personnel, some of whom are also al-Nusra affiliated, some of whom are al-Qaeda affiliated, some of whom are affiliated with other organizations. But these strikes weren't specifically targeting any of those other organizations. They were targeting the Khorasan group. If a

terrorist happens to be a member of both groups, so be it."
Gen. Austin noted said none of the airstrikes was aimed at al-Nusra.
U.S. officials said the targets hit last night included bomb-making facilities, training areas, and meeting locations.
The Khorasan Group is made up of al-Qaeda veterans of the wars in Afghanistan and Pakistan. They traveled to Syria to join forces the Jabhat al-Nusra Front, the Islamist group al-Qaeda favors over ISIS. U.S. intelligence officials say the Khorasan Group has been actively plotting attacks against Western targets.
One of the very first airstrikes on the first day – 8 August — of the U.S. anti-ISIS campaign, consisted of twenty Tomahawk cruise missiles and other smart bombs directed at eight Khorasan Group targets near Aleppo in northwestern Syria.

Albanian Army Reports 12000 Sticks of TNT Missing

Source: http://colle-log-en.w.ezic.info/298297.html

November 08 – Albanian Army has informed that 12.000 pieces of TNT explosives, each weighing 200 grams, have been stolen from an Army depot in the village of Nuaj, near the city of Kruja. The theft may have been done for lucrative purposes, as the TNT can be used in quarries, but it also may be used for terrorism.

MINA correspondent from Tirana reports that the value of the stolen explosives are estimated at 200 million lek, or about 1,4 million EUR. The police arrested one warehouse employee.
It is possible that the explosives were sold to quarries, but the prosecution can't overrule the possibility that it has gone in the hands of criminals who might use it for terror attacks in our region, or outside Albania, Albanian daily Shekulli reports.
This is not the first recent case of theft from an army depot in Albania, which famously saw its depots looted after the financial meltdown of 1997. Shekulli writes that there has been a spate of attacks on businessmen, but also electric pylons, with explosives in Albania.

EDITOR'S COMMENT: 12,000 sticks? And nobody noticed anything? You need time and manpower to accomplish such an "operation"! Were they just freely stored in the open without protection, guarding and all necessary security measures? Come on people! Be a bit serious with explosives!

400 kg explosive, 1700 detonators seized in poll-bound Jharkhand

Source: http://www.dnaindia.com/india/report-400-kg-explosive-1700-detonators-seized-in-poll-bound-jharkhand-2033681

In a major haul, security forces seized 400 kg of local explosives and over 1,700 detonators during an anti-Naxal operation in poll-bound Jharkhand on Monday.
The operation was carried out by the elite CoBRA commando troops of CRPF alongwith the Jharkhand 'Jaguars' police unit in the Bokakhar-Ranidah area of Latehar district early this morning.
According to officials, the seized items include 1,745 detonators, three gas cylinder based Improvised Explosive Devices of 50 kg each, a 5kg cane bomb, 400kg of urea mixed with petrol, 10kg of

gun powder, nitro sulphide wighing approximately 1 kg, two large cutter machines, two drill machines, 400 syringes, tool boxes, electronic gadgets and 200 pressure cookers used to prepare IEDs.

"It is suspected that the Naxals would have used these explosives to target security forces and polling parties during the forthcoming Assembly polls in the state," a senior security officer said.

The joint forces have launched a search operation around this Naxal hideout, the officer said.

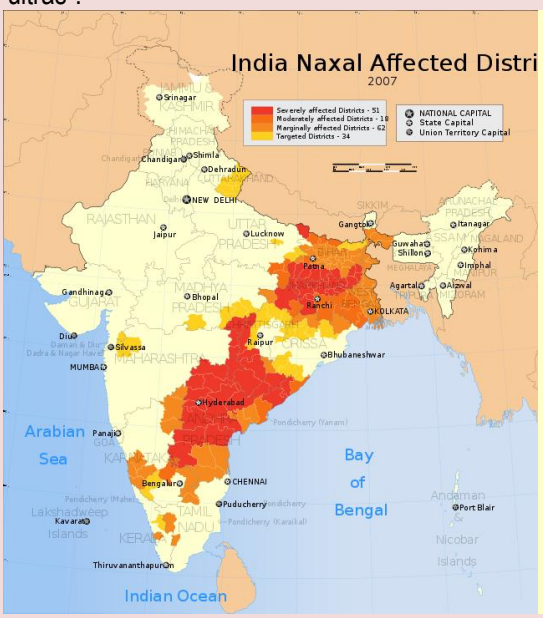
The state will go to polls in five phases starting November 25 and counting of votes will take place on December 23.

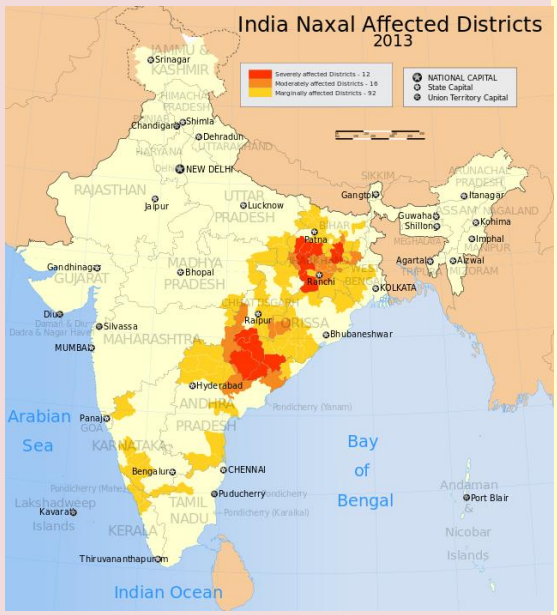
Naxal

Source: http://en.wikipedia.org/wiki/Naxalite

A **Naxal** or **Naxalite** is a member of any of the Communist guerrilla groups in India, mostly associated with the Communist Party of India (Maoist). The term *Naxal* derives from the name of the village Naxalbari in West Bengal, where the movement had its origin. Naxalites are considered far-left radical communists, supportive of Maoist political sentiment and ideology. Their origin can be traced to the split in 1967 of the Communist Party of India (Marxist), leading to the formation of the Communist Party of India (Marxist–Leninist). Initially the movement had its centre in West Bengal. In later years, it spread into less developed areas of rural southern and eastern India, such as Chhattisgarh, Odisha and Andhra Pradesh through the activities of underground groups like the Communist Party of India (Maoist).

In 2006 India's intelligence agency, the Research and Analysis Wing estimated that 20,000 armed-cadre Naxalites were operating in addition to 50,000 regular cadres and their growing influence prompted Indian Prime Minister Manmohan Singh to declare them to be the most serious internal threat to India's national security. Naxalites, and other anti-government militants, are often referred to as "ultras".





In February 2009, the Indian Central government announced a new nationwide initiative, to be called the "Integrated Action Plan" (IAP) for broad, co-ordinated operations aimed at dealing with the Naxalite problem in all affected states (namely Karnataka, Chhattisgarh, Odisha, Andhra Pradesh, Maharashtra, Jharkhand, Bihar, Uttar Pradesh, and West Bengal). Importantly, this plan included funding for grass-roots economic development projects in Naxalite-affected areas, as well as increased special police funding for better containment and reduction of Naxalite influence in these areas.

In 2009, Naxalites were active across approximately 180 districts in ten states of India. In August 2010, after the first full year of implementation of the national IAP program, Karnataka was removed from the list of Naxalite-affected states. In July 2011, the number of Naxalite-affected areas was reduced to 83 districts in nine states (including 20 additional districts). In December 2011, the national government reported that the number of Naxalite-related deaths and injuries nationwide had gone down by nearly 50% from 2010 levels.

New facility to help in fight against IEDs opens in the Netherlands

Source: http://www.eda.europa.eu/info-hub/news/2014/11/04/new-facility-to-help-in-fight-against-ieds-opens-in-the-netherlands

A new facility designed to help in the fight against Improvised explosive devices (IEDs) was officially opened today in the Netherlands. The Joint Deployable Exploitation and Analysis Laboratory (JDEAL) provides a permanent technical exploitation training capability in the Dutch town of Soesterberg. Under the project a further two deployable laboratories could be procured for use in future operations.

JDEAL, which was facilitated by the European Defence Agency (EDA) and lead nation the Netherlands, focuses on training the full range of skills needed for technical exploitation. This involves the recording and analysing of information related to events, scenes, technical components, and material used in IED attacks.

The project makes use of equipment and knowledge gained from the EDA developed Counter-IED Technical Exploitation Laboratory previously deployed with ISAF in Kabul.

Alongside the Netherlands, ten other EDA Member States – Austria, Belgium, France, Germany, Hungary, Italy, Luxembourg, Portugal, Spain, and Sweden – plus Norway have joined the project. Denmark, the United Kingdom, the United States and the NATO Counter-IED Centre of Excellence have also sent observers.

Warrant Officer Bert Westers, from the Dutch armed forces, was previously stationed at the laboratory in Afghanistan and will now act as a trainer at JDEAL. He commented: "This new facility allows us to maintain and build on the skills and experiences that we gained in Kabul. It also helps to improve our forces' ability to deal with threats from IEDs in the future."

Education, research, and deployable capabilities

The training facility will host both national and multinational training events, tailored to the needs of the Member States involved. Alongside the training aspect, JDEAL is intended to be a platform for research and development and is specifically designed for subprojects to be launched under its framework. It will also work closely with other actors and cooperative bodies working in the counter-IED field.

In a second step the establishment of two deployable laboratories is planned, in order to have at least one available for upcoming

operations/missions by the second half of 2015.

Background

The JDEAL project will work across the entire scope of IED exploitation. This includes detailed visual examination and high quality image capture; technical exploitation reporting; biometric analysis (latent finger print recovery); electrical circuitry (primarily radio parts); document and media recovery (focused on the mobile phones often used as IED triggering devices); chemical analysis; mechanical exploitation as well as other material exploitation. This is done in close cooperation with intelligence services, which can use the results to attack the networks involved in manufacturing the IEDs.

The JDEAL project was born out of the EDA developed multinational counter-IED Exploitation Laboratory (MNTEL), which was deployed in Kabul under French management. During the laboratory's three year deployment in Afghanistan more than 6 000 IEDs were forensically examined, providing invaluable support to law enforcement and leading to numerous terrorist prosecutions.

Japanese researchers develops liquid bomb detector that works in seconds

Source: http://www.counteriedreport.com/news/japanese-researchers-develops-liquid-bomb-detector-that-works-in-seconds

Japanese researchers have developed a counterterrorism device that can quickly determine if the liquid inside a bottle or can is explosive or flammable, which could greatly speed up baggage inspections at airports.

The bomb-detecting apparatus, developed by a team led by Hideo Itozaki, a professor of engineering at **Osaka University**, is also compact and can be installed anywhere.

"The device should prove useful not just in airports, but also in a variety of event venues and museums, including the Olympic Games," Itozaki said.

Its detection accuracy meets the global standards set by the European Civil Aviation Conference.

The developers, who conducted a month-long trial of the device at Narita Airport's international terminal, hope to collaborate with private companies to sell their detector next spring.

To operate the detector, a bottle of liquid is placed between two cylinders that emit light. The device cross-references the light-absorption properties of the liquid with information stored in a database.

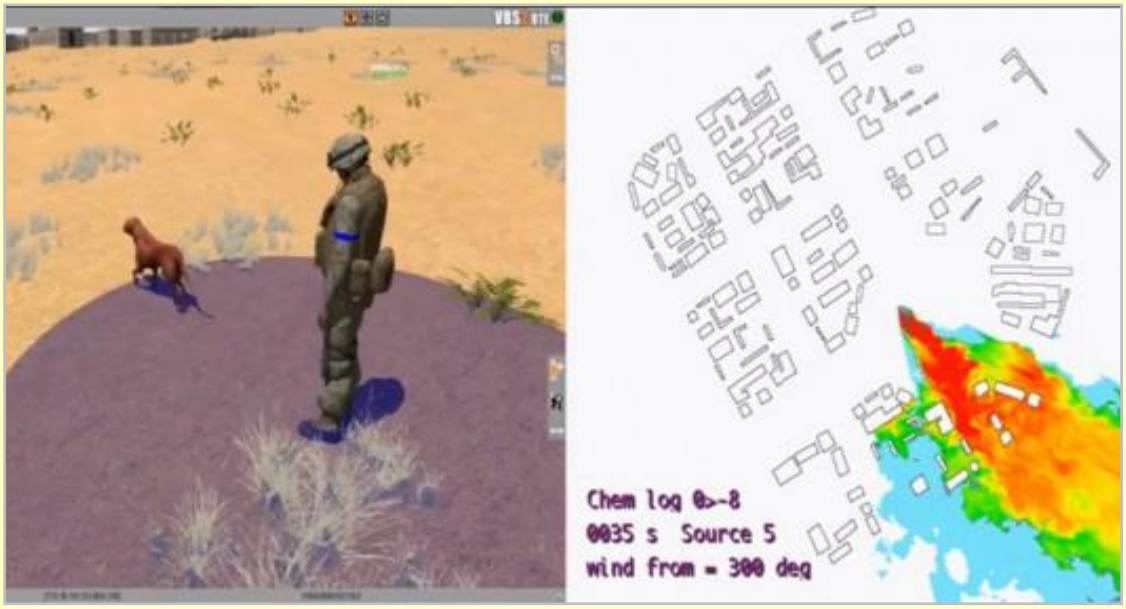
Depending on the safety of the content, a lamp glows either red or green. Results take less than a second if the content of the bottle is an ordinary fluid such as water. With less common liquids, the machine will determine their safety in about five seconds. The findings can also be displayed on a portable device.

Liquids in opaque containers such as aluminum cans are inspected using a different method whereby sensors touch the surface of the containment vessel.

Many of the devices that currently examine fluid content in airports around the world are cumbersome and take time to give results. In addition, in Japan, fluids brought onto domestic flights are checked only for their flammability.

Video game gives soldiers better skills to handle bomb-sniffing dogs

Source: http://www.gizmag.com/rover-dog-ied-finder/34674/



Rover is a video game developed by the US military that uses an Xbox Kinect to help train dog handlers to detect subtle cues from bomb-sniffing canines

For centuries, dogs have served in a variety of roles alongside humans, including faithful companion and guardian. The latter function is one that's seen more focus in recent times as canines have been trained to sniff out buried improvised explosive devices (IEDs) before they are detonated. The dog's handler also needs to be trained to detect subtle cues from the animal, which is where a video game developed by the US military comes into play.

Rover, as it is called, was created by a team including Adam Moses, a computer scientist at the U.S. Naval Research Laboratory (NRL), who were challenged by the Office of Naval Research (ONR) to come up with a tool for training dog handlers. **The program helps soldiers practice commands and, perhaps even more importantly, read a dog's silent cues, such as seeing the animal glance a little longer at, or briefly stop in front of, an alley that might hold danger.**

According to the NRL, IEDs subtly leak gas plumes that pretty much no human-built sensor can detect because its particles are so small, however, dogs' noses are much

more sensitive, allowing them to pick up the scent of these plumes. Moses spent a lot of time researching dog behavior, including spending hundreds of hours watching tapes of dogs and their handlers from Iraq. This research, plus ten years spent working with first responders on modeling how airborne toxins spread through a city after an accident or attack, gave him the tools and know-how necessary to create the software.

Rover works in conjunction with an Xbox Kinect and a "skeleton tracker" program Moses wrote

to allow handlers to practice virtual dog command gestures with their on-screen companions. A soldier and his virtual Labrador bomb-sniffing sidekick might, for example, explore an empty desert village together as they try to locate hidden IEDs. The program itself is a module of a US Army training tool known as Virtual Battlespace.

One chief concern Moses aimed to address in creating *Rover* was making sure the handler understands the dog's psychology so that those subtle cues in its behavior aren't missed and the handler can safely guide the dog to its origin.

"A dog is trying to please the handler, so if the handler keeps the dog moving instead of looking at what's caught the dog's attention, the dog is less likely to display that cue again," says Moses. "An inexperienced handler can un-train a dog by accident, so better that they could spend a week on one of these and, if they make a mistake here, it's no big deal."

Future plans for *Rover* could include creating a wider range of dog personalities that might all handle distractions, such as crowds and noises, differently. It might also find its way into the hands of law enforcement agencies, who could adapt it to handlers working with drug-sniffing dogs. Moses is also considering the potential benefits of adding a scoring system based on things like how many cues from the dog the handler noticed or if they kept the dog on track.

Westinghouse, SNPTC team up for Turkish nuclear plant

Source: http://www.neimagazine.com/news/newswestinghouse-snptc-team-up-for-turkish-nuclear-plant-4449742

November 25 – Westinghouse Electric Company, China's State Nuclear Power Technology Corporation (SNPTC) and Turkey's state-owned electric power company, EÜAS, have agreed to enter into exclusive negotiations to develop and construct a four-unit nuclear power plant in Turkey.

The project, which would be Turkey's third nuclear power plant, will 'be based on AP1000 reactor technology,' Westinghouse said. The agreement also covers operations, nuclear fuel, maintenance, engineering, plant services and decommissioning.

Westinghouse has been working with SNPTC on AP1000 technology transfer and the localisation of AP1000 technologies in China since December 2007. In October 2009, the companies signed an agreement to co-develop and refine the AP1000 to create the CAP1400, a bigger (1530 MWe) version of the AP1000 (1250 MWe) with independent intellectual property.

While Westinghouse is expected to have limited involvement in CAP1400 projects within China, it will still have a stake in CAP1400 export projects, Tim Collier, Westinghouse vice president and managing director for China said in April.

In addition to the proposed third nuclear power plant, Turkey is planning a four-unit nuclear power plant at Akkuyu, based on Russia's VVER-1200 reactor technology. This project, which could start construction in 2015, will be build by Rosatom under its build, own, operate model. Four more AREVA/MHI's Atmea 1 reactors are also proposed for construction at Sinop. No site has been specified for the proposed third nuclear plant.

Die Welt: the Turkey Promotes atomic bomb?

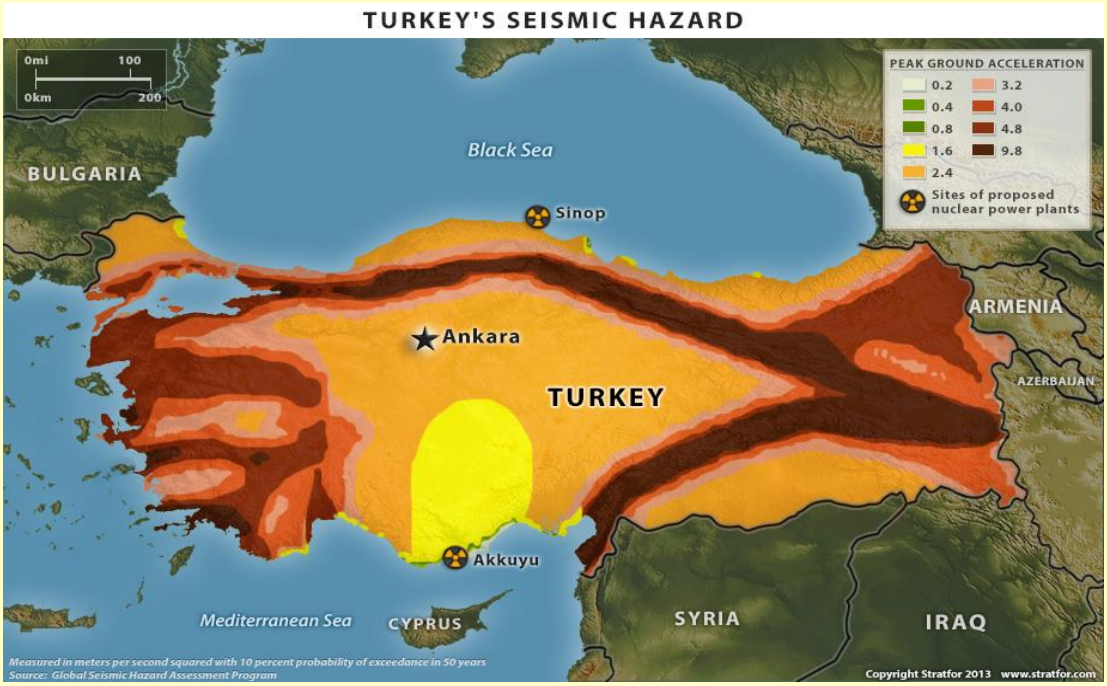
Source: http://thepressportal.com/die-welt-the-turkey-promotes-atomic-bomb/

Berlin: in the current publication, the German newspaper Die Welt writes that one of the reasons that the BND, the German intelligence service, monitor the Anchor, it could be a Turkish nuclear weapons program, which secretly evolves the Turkey.

As stated in the report, the BND has indications (growing according to the publication) that Recep Tayyip Erdogan wants to equip nuclear his country.

Up to date info like the BND to spy on the anchor for other reasons: for the influx of Islamic militants in Iraq and Syria, for smuggling, drug trafficking and the presence of Kurdish fighters, reported the newspaper.

The Welt reported that Turkey commissioned in 2011 in the Russian firm Rosatom to build a large plant on the Mediterranean coast, about 300 kilometers east of the tourist center of Antalya. Two years later, there was a similar agreement with a French-Japanese consortium.



The newspaper reported that usually in the case of a nuclear power plant for peaceful purposes, companies end up in agreement with the Government to provide the necessary uranium and obtain nuclear waste after the end of the process.

However, Ankara failed to agree to this condition, wanting to check the same issue of uranium enrichment and the disposal of nuclear waste. The Welt writes that this piece of the nuclear process is crucial for every country that wants to build nuclear weapons.

"If Turkey wants to keep spent nuclear fuel rods, it has only one logical explanation: wishes to gather material for a plutonium bomb" stresses the newspaper.

According to the newspaper, the gaps in Turkey's nuclear agreements leave gaping loophole and for uranium-enrichment necessary to build a nuclear weapon.

The same anchor, however, denies that it wants uranium enrichment.

According to Germany's Federal Intelligence Service, the Turkish Prime Minister Erdogan has already arranged in 2010, to prepare the Turkey for the construction of uranium enrichment plants, the newspaper reported. In accordance with other findings of the Agency, Turkey reportedly already has a significant number of centrifuge machines.

From coming? The newspaper stresses that it is easy to guess: from Pakistan. The Welt also speaks, and for exchanges of scientific evidence on nuclear Pakistan.

At the same time, refers to the Turkish manufacturing missile program saying that from 2011 the Erdogan had asked for long-range missile development. The journal adds that at the beginning of 2012 the anchor started developing medium-range missile and stresses that a medium range missile with 2,500 km range can be ready in 2015.

According to the Welt, these plans are a strong indication of a continuing nuclear weapons construction programme.

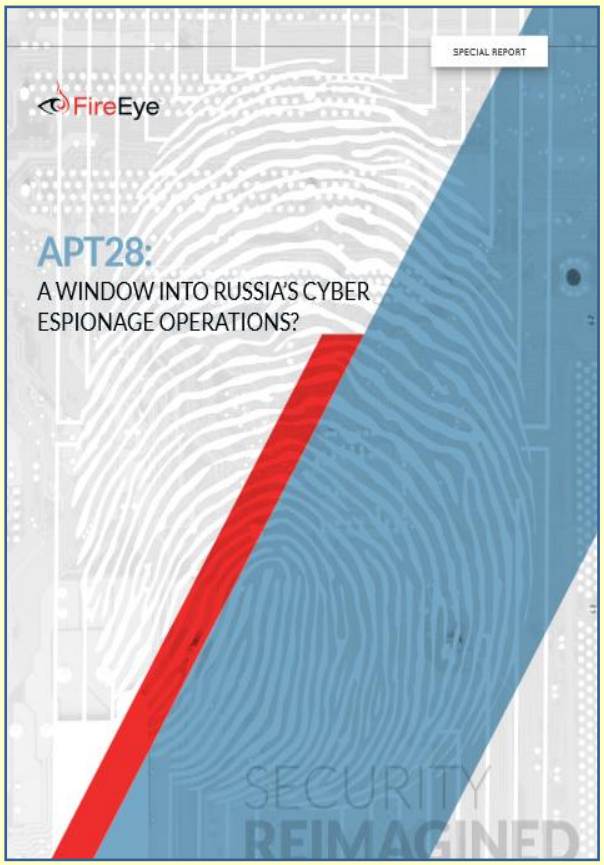
The newspaper also refers to earlier statements by Turkish officials as Abdullah Gul as Foreign Minister that "Turkey can not leave one neighbouring country (r.r. reference to Iran) to have nuclear weapons itself (the Turkey) does not have".

The author of the article, Hans Rile, former head of policy planning at the Defense Ministry, claims that with Israel's nuclear power and the nuclear program of Iran, Erdogan will not be met unless developed and anchor the possibility of nuclear weapons.

New report details Russia's cyber-espionage activities

Source: http://www.homelandsecuritynewswire.com/dr20141030-new-report-details-russia-s-cyberespionage-activities

October 30 – Researchers at FireEye, a Silicon Valley-based computer security firm, are connecting the Russian government to cyber espionage efforts around the world. **According to a report released on Tuesday by FireEye, hackers working for the Russian government have for seven years been hacking into computer networks used by the government of Georgia, other Eastern European governments, and some European security organizations.**



The attacks have not been directly linked to any Russian government office or asset such as a Web server address, instead researchers at FireEye made the government connection because the malicious software used in the attacks was written during Moscow and St. Petersburg working hours on computers that use Russian language settings and because the targets align with Russian intelligence interests. "The malware indicates a seven-year espionage effort, operating and developed over time," Laura Galante, FireEye's manager of threat intelligence, said. "This is a professional, well-resourced effort that has been going on for years."

FireEye adds that it is often difficult to distinguish between Russian government attacks and attacks by Russian hackers. "You only exist as a significant Russian cybercriminal if you abide by three rules," said Tom Kellermann, chief cybersecurity officer at Trend Micro, a security firm based in Irving, Texas "You are not allowed to hack anything within the sovereign boundary; if you find anything of interest to the regime you share it; and when called upon for 'patriotic activities,' you do so. In exchange you get 'untouchable status.' "

The *New York Times* reports that FireEye is one of several global security firms that have connected the Russian government to cyber espionage. Earlier this year, Symantec, F-Secure, and CrowdStrike tied a series of coordinated attacks on Western petroleum and gas companies to the Russian government. "This is state espionage," Galante said on Tuesday. "This is Russia using its network operations to bolster their key political goals."

American officials have blamed Russian hackers for a series of distributed denial-of-service (DDoS) attacks on Kyrgyzstan in January 2009 that, according to analysts, was meant to persuade Kyrgyzstan's president to evict an American military base in the country. Shortly after the attacks, Kyrgyzstan announced plans to remove the U.S. base and received $2 billion in aid and loans from Russia.

Galante said FireEye's researchers discovered the espionage campaign, called APT28 by the firm's researchers, on computer networks of some of its clients. Targets of the campaign include the Ministry of Internal Affairs of Georgia and its Ministry of Defense, the governments of Poland and Hungary, the North Atlantic Treaty Organization, and other European security organizations.

▶ **You can read the full report at:** http://www.fireeye.com/resources/pdfs/apt28.pdf

Georgia Tech releases 2015 Emerging Cyber Threats Report

Source: http://www.homelandsecuritynewswire.com/dr20141030-georgia-tech-releases-2015-emerging-cyber-threats-report

In its latest Emerging Cyber Threats Report, Georgia Tech warns about loss of privacy; abuse of trust between users and machines; attacks against the mobile ecosystem; rogue insiders; and the increasing involvement of cyberspace in nation-state conflicts.

Such topics are discussed at length in the annual report, which is published by the Georgia Tech Information Security Center (GTISC) and the Georgia Tech Research Institute (GTRI).

The report was released yesterday at the 12th Georgia Tech Cyber Security Summit (GT CSS), which has become one of the Atlanta IT community's key event on cyber security.

A Georgia Tech release notes hat in the report, Georgia Tech covers five major areas. **Observations that summarize findings in each area are as follows:**

- Technology enables surveillance, while policy lags behind.
- Attackers continue to target the trust relationship between users and machines.
- Mobile devices fall under increasing attack, stressing the security of the ecosystem.
- Rogue insiders cause significant damage, but solutions are neither simple nor easy.
- Low-intensity online nation-state conflicts become the rule, not the exception.

"We must continue to invest in research and develop technology, processes and policies that help society deal with these developments," said GTISC director Wenke Lee. "Researchers from academia, the private sector, and government must continue to work together and share information on emerging threats, make improvements to policy, and educate users."

— Read more in Emerging Cyber Threats Report 2015 (Georgia Tech Information Security Center [GTISC] and thee Georgia Tech Research Institute [GTRI], 2014) at: http://www.gtcybersecuritysummit.com/2015Report.pdf

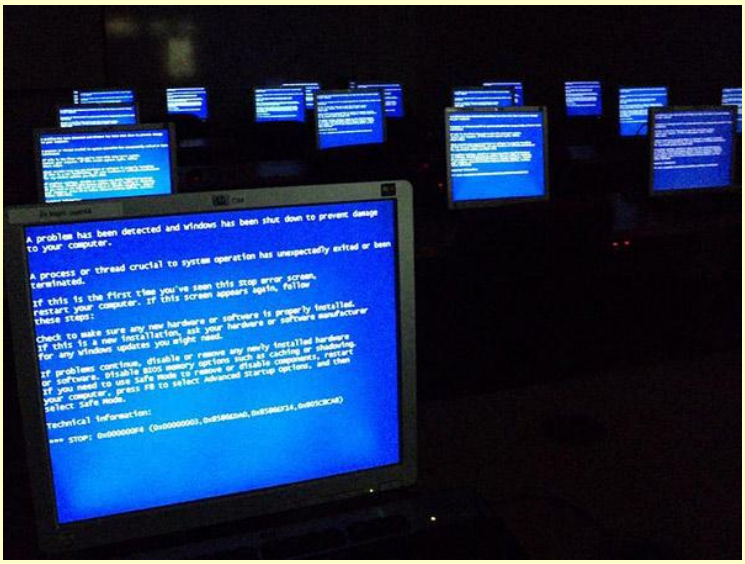
A major cyberattack causing widespread harm to national security is imminent: Experts

Source: http://www.homelandsecuritynewswire.com/dr20141103-a-major-cyberattack-causing-widespread-harm-to-national-security-is-imminent-experts

A new report from the Pew Research Center and Elon University's Imagining the Internet Center found that more than 60 percent of the roughly 1,600 computer and Internet experts surveyed on the future of cyberattacks believe a nationwide cyberattack is imminent. They did so in response to the question: "By 2025, will a major cyberattack have caused widespread harm to a nation's security and capacity to defend itself and its people?" The experts also warn about the risks to privacy which will accompany a growing focus on cybersecurity.

The *Inquirer* reports that some survey respondents believe that the worst cyber threats would be containable. "While, in principle, all systems are crackable, it is also possible to embed security far more deeply in the future Internet than it is in the present Internet environment," said Lee McKnight, a professor at Syracuse University's School of Information Studies.

Many experts cited the Stuxnet worm as an example of how a cyberattack could damage critical infrastructure such as power grids, air-



traffic controls, and financial networks. Stuxnet, believed to have been engineered by U.S. or Israeli intelligence to damage Iran's nuclear program, infected the software of at least fourteen industrial sites in Iran and helped destroy roughly 20 percent of the centrifuges being used to enrich radioactive fuel. "The majority opinion here is that these attacks will increase and that lots of institutions, including major government institutions, will be at risk," said Lee Rainie, director of the Pew Research Internet Project and co-author of the report.

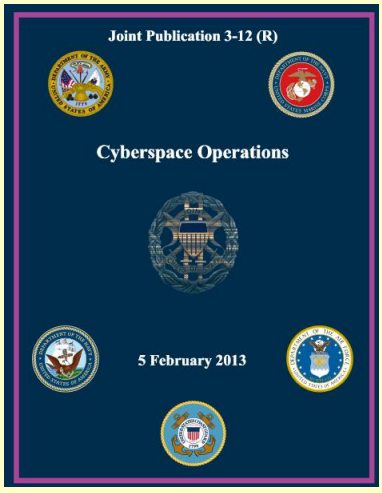
Jason Pontin, editor and publisher of the *MIT Technology Review*, likened Stuxnet to "a Pearl Harbor event."

"Do we really believe that the infrastructure of a major industrial power will not be so attacked in the next 12 years?" he asked. "The Internet is an insecure network; all industrialized nations depend on it. They're wide open."

Some experts believe the threat of "mutually assured destruction" could discourage state-sponsored cyber warfare. "Right now, cyberattacks are too costly," one survey respondent said. "The bigger risk will be when cyber crooks drain Wall Street of all its cash."

Report co-author Janna Anderson of Elon University warns, however, that some threats are being exaggerated for profitability, adding that privacy would continue to suffer as a result. According to Jonathan Grudin, a principal researcher at Microsoft Research, concerns about cyberattacks "seem exaggerated by the political and commercial interests that benefit from us directing massive resources to those who offer themselves as our protectors." In reference to President Dwight Eisenhower's 1961 warning about the influence of a "military-industrial complex," Grudin said lawmakers seem "powerless to rein in the military-industrial-intelligence complex, whose interests are served by having us fearful of cyberattacks."

Pentagon has declassified 2013 Joint Cyberspace Operations Doctrine



Source: http://stefanomele.it/news/dettaglio.asp?id=421

This publication provides US joint doctrine for the planning, preparation, execution, and assessment of joint cyberspace operations across the range of military operations.

Prepared under the direction of the Chairman of the Joint Chiefs of Staff, this publication sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners.

It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs), and prescribes joint doctrine for operations and training. It provides

military guidance for use by the US Armed Forces in preparing and executing their plans and orders.

▶ **Read the full document at:** http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Greece - Europe runs largest cyber-security exercise to date

Source: http://eandt.theiet.org/news/2014/oct/cyber-europe-2014.cfm

October 31 – More than 200 cyber-security agencies, energy and telecoms companies, financial institution and Internet service providers have taken part in Cyber Europe 2014, the largest cyber-security exercise to have been run in Europe to date in Athens, Greece.

Organised by the European Network and Information Security Agency (ENISA), the drill simulated 2,000 separate cyber incidents including denial of service attacks on online

services, intelligence and media reports on cyber-attack operations, website defacements and attacks on critical national infrastructure including energy and telecommunication networks.

Testing Europe's preparedness, cooperation and procedures, the exercises, involving over 400 cyber security experts, has been run simultaneously from multiple cyber research centres across Europe.

"The sophistication and volume of cyber-attacks are increasing every day," said European Commission Vice-President Neelie Kroes. "They cannot be countered if individual states work alone or just a handful of them act together. I'm pleased that EU and EFTA Member States are working with the EU institutions with ENISA bringing them together. Only this kind of common effort will help keep today's economy and society protected."

ENISA runs such pan-European simulations every two years. However, the 2014 exercise has been the most complex and the largest so far.

"Five years ago there were no procedures to drive cooperation during a cyber-crisis between EU Member States," said executive director of ENISA, Professor Udo Helmbrecht. "Today we have the procedures in place collectively to mitigate a cyber-crisis on European level. The outcome of the exercise will tell us where we stand and identify the next steps to take in order to keep improving."

According to ENISA's Threat Landscape report (2013), the sophistication of attacks and complexity of the tools used by various cyber criminals or state-backed agents is steadily increasing. Multiple countries are known to have developed capabilities that can be used to infiltrate all kinds of targets, governmental and private in order to achieve their objectives.

In 2013, global web-based attacks

increased by almost a quarter and the total number of data breaches was 61 per cent higher than 2012. Each of the eight top data breaches resulted in the loss of tens of millions of data records while 552 million identities were exposed. According to industry estimates cyber-crime and espionage accounted for

between $300bn and $1tr in annual global losses in 2013.

ENISA will release results of the latest exercise in the upcoming months.

Is social media responsible for your safety during a disaster?

By Andrew Quodling and Emma Potter

Source: http://www.homelandsecuritynewswire.com/dr20141111-is-social-media-responsible-for-your-safety-during-a-disaster

November 11 – **Given the popularity of Facebook and Twitter, it's not surprising so many people use social media in crises such as floods, fires, and earthquakes.**

Facebook has introduced **Safety Check**, a new tool for users in disaster-affected areas to notify their network of "friends" of their safety and check on their family and friends.

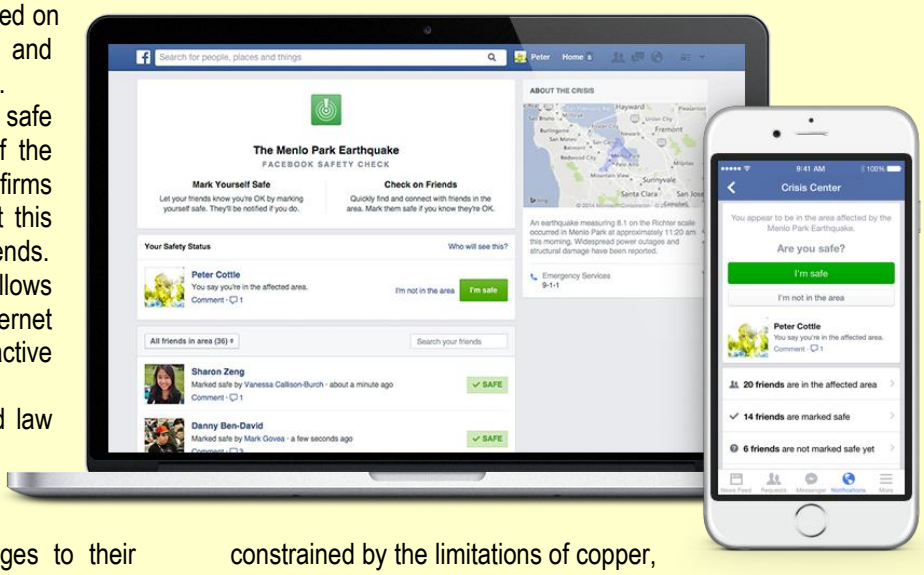
Facebook will send a notification to users who may be affected by a disaster, based on the location in their profile and geolocation data collected by apps.

People can then confirm they are safe or report that they are outside of the affected area. When a user confirms they are safe, Facebook will post this on their timeline and notify their friends.

This service from Facebook follows similar moves by other internet companies to become more proactive in crisis communications.

Twitter Alerts allows pre-approved law enforcement, emergency management, and government agencies, as well as selected NGOs to send important messages to their followers via push notifications and text messages.

Google has also developed tools to streamline official communication from emergency responders to the public during disasters.



Social media in disasters

Sites such as Facebook and Twitter have become key sources that people turn to for help and information in natural disasters. Our experience in recent disasters, including the 2010-11 Queensland floods and 2013 Tasmanian bushfires, is proof of this.

Emergency management organizations often stress the importance of emergency preparedness for people who live in places that are prone to natural disasters.

But while social media can be a handy resource in crises, people must be careful not to take their access for granted during emergencies. Floods, fires, and earthquakes often disrupt the power and communications infrastructures that smartphones rely upon.

Granted, Internet companies such as Facebook and Google are keenly aware of this problem and are working to provide internet access remotely through arrays of unmanned drones, stratospheric balloons and satellites.

But for the time being, our access is constrained by the limitations of copper, fiber, hybrid, and cellular internet technologies, and their vulnerability to the elements.

New media, new concerns

In a crisis, it is critically important that governments are able to communicate information to citizens that is both accurate and up to date.

With traditional systems, such as radio and television, this is a relatively simple process — emergency management organizations cooperate with media producers to ensure that the information broadcast is current and correct.

This is a more challenging process with new media platforms, because of the different ways that users share information. While traditional media would stop broadcasting

any outdated information, social media posts can still be shared well after their accuracy has expired.
Some research has suggested that users have been able to police each other's social media and hashtag usage during disasters.
But the cost of failure — whether it is the sharing of false or outdated information — can be tragic if it results in a diversion of resources from where they are truly needed.
Facebook's lack of transparency makes it difficult to know how its social algorithms are geared to facilitate accurate communication in times of crisis.
As tempting as it may be to trust Facebook's service, we do not know if posts from users in emergency zones are treated any differently by its algorithm than posts about ice bucket challenges or Kardashians, or how widely-read a user's call for help might be.
There may also be legal ramifications if a platform's algorithms favor posts that are outdated or misleading. Courts in Australia and Germany have held Google responsible for defamation. Will platforms that engage in crisis communications also be liable for their technological failings?
If Facebook aims to become a go-to service for its users during natural disasters, the effectiveness of its algorithms must be a key concern.

Trial by fire?

So while we're yet to see how Safety Check works in action, some of its features seem potentially problematic.
Safety Check doesn't seem to allow users to report themselves as unsafe, only that they are safe or outside of the affected area
At first blush, this bears resemblance to the social media guides of emergency management organizations, emphasizing more traditional communication methods where there is immediate danger.
It also helps position Facebook in a way that minimizes its users' expectations of Facebook's role as an emergency service provider.
The system also has a basic, on/off-style understanding of safety. The design of the system might be focused around the types of disasters that Facebook's developers see more of, such as earthquakes, where safety can often be quickly and easily established after a tremor or series of tremors.
Fires, floods and cyclones, on the other hand, can be long and unpredictable events. Floods can last over a number of days or weeks, or in the case of bush fires and cyclones, their path may change as the disaster evolves.
This raises questions about how and when Facebook will disseminate safety notifications. If a bushfire is occurring near a major population, for example, at what point do users in the affected area receive a notification?
Safety Check's main problem is that in spite of its celebrated launch, it seems to be a hobby-style project for Facebook — as the tool was designed at a "hackathon," not in consultation with any emergency management organizations.
In spite of our concerns, it is encouraging to see an organization such as Facebook taking responsibility for its users and entering the crisis communication space.
A tool that helps family and friends during a crisis, and facilitates easy communication is a welcome development.

Andrew Quodling *is Ph.D.Candidate at Queensland University of Technology.*

Emma Potter *is Ph.D. Candidate at Queensland University of Technology.*

Using Big Data To Fight Pandemics

By Nuria Oliver

Source: http://techcrunch.com/2014/11/08/using-big-data-to-fight-pandemics/?ncid=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29

Last year, I gave a talk at WIRED 2013 on how anonymous and aggregated mobile phone data can be used to understand and combat the spread of infectious diseases. I described a study that we carried out in my research team a few years ago, where we analyzed

aggregated and anonymized mobile data from Mexico during the H1N1 flu outbreak in the spring of 2009.

Thanks to the massive adoption of mobile phones and the power of anonymized and aggregated data, we were able to quantify the impact that the measures taken by the Mexican government had on the mobility of the population and hence on the spread of the disease. We, and similarly researchers at the Karolinska Institute and Harvard University among others, have demonstrated how the analysis of large-scale mobile data can be used to deliver significant benefits to society.

Little did I know that today we would be fighting the worst Ebola outbreak in our history, with already almost 5,000 deaths and over 13,000 infections. Unfortunately, a few months after the outbreak of the pandemic we are only now

starting to put into place coordinated efforts towards the analysis of mobile phone network data and what this tells about the spread of Ebola.

People's efforts have understandably been focused elsewhere. This week at the ITU Plenipotentiary Conference in Busan, the International Telecommunication Union (ITU), the GSMA and the Internet Society (ISOC) announced that they are joining forces in the fight against Ebola. This unity is an essential step forward, but along with the GSMA, United Nations Global Pulse, and a number of other data scientists, I really want to make sure we, and most importantly the African mobile operators, address this opportunity and truly harness the potential of the data available.

Of course mobile data analytics cannot directly assist the heroic work of doctors and nurses who are on the ground, but it could prove extremely helpful when it comes to planning resource allocation or understanding the effectiveness of different mobility containment measures.

Mobility is one of the key factors that contributes to the spread of a human-transmitted infectious disease, such as Ebola. Therefore, understanding and quantifying human mobility in the areas affected by the Ebola virus could make a crucial difference to contain it. And population mobility is precisely one of the characteristics that can be analyzed and predicted using large-scale anonymized mobile data.

In addition, levels of activity of the cell towers over a specific time period could be seen as a proxy of the amount of people in the geographical area served by that tower. Modeling the changes in the levels of activity in the towers of areas affected by Ebola would provide insights into population changes due to the outbreak.

While this data is far from perfect, it provides valuable information that would otherwise be prohibitively expensive and time consuming to collect.

Understandably, there might be concerns, particularly in West Africa, about the impact on privacy. The good news is that extensive research conducted by a range of academic teams demonstrates that it is possible to both analyze human mobility patterns and preserve privacy. All data is typically anonymized using state-of-the-art encryption algorithms. In addition, data is usually analyzed in a highly secure and protected environment (e.g. the mobile operator premises) by authorized personnel. No analysis is undertaken that would ever identify individuals. In addition, only the resulting aggregated, non-sensitive analyses (e.g. population mobility estimates, aggregate statistics…) would be made available to relevant aid agencies or government agencies.

Technical difficulties should not be a barrier either, as there is a body of work illustrating how to carry out this type of analysis. Moreover, there is a group of highly skilled data scientists — including ourselves — and strong support from organisations, such as the ITU, ISOC, GSMA and

United Nations Global Pulse — who are ready and willing to assist African operators in the process, particularly to ensure that all data handling is carried out in an ethical and anonymous manner, always respecting local data privacy laws.

The potential to have positive impact and help save lives is immense. I truly hope that we can quickly find a way to realize this the full potential of big data for social good. It's an opportunity that we cannot afford to miss.

__Nuria Oliver__ is a scientific director at Telefonica looking at how the use of big data can help to fight pandemics such as Ebola and bird flu.

U.S. government networks vulnerable despite billons spent on protecting them

Source: http://www.homelandsecuritynewswire.com/dr20141112-u-s-government-networks-vulnerable-despite-billons-spent-on-protecting-them

Experts say that cybersecurity has leaped over terrorism as the top threat to U.S. security, and with the awareness of the threat comes funding better to secure government systems. **There are currently 90,000 information technology security professionals working for the government, 33 percent of them are contractors.** The federal government is projected to hire more cyber professionals and spend $65 billion on cybersecurity contracts between 2015 and 2020, but today, federal cybersecurity officials are still struggling to keep sensitive data from hackers and cyber criminals, according to an APanalysis of records.

The AP has filed dozens of Freedom of Information Act requests, interviewed hackers and cybersecurity experts, and obtained records describing vulnerabilities within government networks to learn that after forty years and more than $100 billion spent since the first federal data protection law was enacted, the U.S. government still lacks the manpower and proper measures to secure its network systems. "It's a much bigger challenge than anyone could have imagined twenty years ago," said Phyllis Schneck, deputy undersecretary for cybersecurity at DHS.

Systems at more than a dozen agencies, including the Pentagon and the National Weather Service, have been infiltrated via phishing e-mails, malware, and physical theft of data storage devices. **Last year, the U.S. Computer Emergency Readiness Team (US-CERT) responded to 228,700 cyberincidents involving federal agencies and critical infrastructure firms; that figure is more than twice the number of incidents that occurred in 2009, and according to the*Mercury*, federal employees are responsible for at least 50 percent of federal cyber breaches.** One federal employee was redirected to a hostile site after clicking on a link that led to a video of tennis star Serena Williams. In September 2011, a parked car belonging to a Pentagon contractor was broken into by a thief who stole unencrypted computer backup tapes containing about five million Social Security numbers along with medical information of Pentagon employees. The federal contractor was tasked with securing those records.

According to an annual White House cybersecurity review, **in 2013, 21 percent of all federal breaches originated from government workers who violated policies; 16 percent of breaches were linked to employees who lost devices or had them stolen; 12 percent to workers who improperly handled sensitive information printed from computers; 8 percent to workers who ran or installed malicious software; and 6 percent to employees who were enticed to share classified information.**

Outsider and accidental threats are not the only risk federal computer systems face. Only a few intentional insider hacks like the one committed by former National Security Agency contractor Edward Snowden, have been reported or discovered. Since 2006, more than eighty-seven million sensitive or private federal records have been exposed by hackers or leakers, according to the Privacy Rights Clearinghouse, which tracks cyberincidents at all levels of government. The*Washington Post* reported last month on a breach targeted at unclassified White

House computers by hackers believed to be working for the Russian government. The Obama administration has not provided details of the attack, but many analysts consider it to be one of the many daily attacks that occur within the federal government. "Certainly a variety of actors find our networks to be attractive targets and seek access to sensitive information," a White House official said. "We are still assessing the activity of concern.

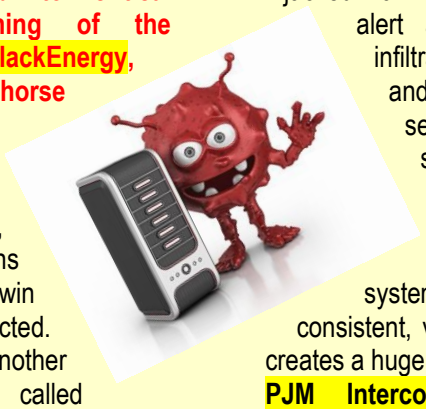
Only a small percent of cyber criminals are caught. In 2013, the Justice department filed 146 cases under the government's computer hacking statue. Former DHS chief Tom Ridge has called on Congress quickly to pass legislation that would better allow the private and public sector to share intelligence on cyber breaches, which will help catch cyber criminals in their early stages of planning an attack. "The constant drumbeat of headlines makes it clear that perhaps the greatest vulnerability this nation faces lies in cyberspace," Ridge said.

Some have warned of a **"Cyber Pearl Harbor"** — but Pearl Harbor was a surprise. No one in business or government today can continue to plead surprise when it comes to the possibility of cyberattack. It is imperative that our political and private sector leaders work together to secure critical infrastructure and other networked systems from cyberpredators."

Security experts worry BlackEnergy technology could soon be available to bad non-state actors

Source: http://www.homelandsecuritynewswire.com/dr20141113-security-experts-worry-blackenergy-technology-could-soon-be-available-to-bad-nonstate-actors

November 13 – **On Monday, the *Homeland Security News Wire* reported on a DHS cyber threat alert issued to critical infrastructure firms warning of the malicious software called BlackEnergy, a variant of a Trojan horse believed to have originated from Russian government-sponsored hackers.** Several industrial control systems, including GE Cimplicity, Siemens WinCC, and Advantech/Broadwin WebAccess, have been affected. BlackEnergy is similar to another Russian issued malware called Sandworm, which was used in a 2013 Russian cyber-espionage campaign against NATO, the European Union, and overseas telecommunication and energy assets. DHS believes the attack on U.S. critical systems is "part of a broader campaign by the same threat actor."



The link to Russia makes BlackEnergy dangerous, but security experts fear that the technology could soon be available to other bad actors. "I think we should be scared and take this very seriously because it could be a nation-state issue. But the fact is, once the tools are there they could just leave it out and anyone could do (the attack)," said James Joshi, a University of Pittsburgh associate professor and lead faculty member of the school's Information Assurance Program.

The *Pittsburgh Post-Gazette* reports that there are no signs that affected systems have been hijacked via BlackEnergy, but DHS is on high alert as the malware could have infiltrated yet-to-be discovered files and systems. "It's really a very serious issue and the fact that sometimes it's very difficult to detect (this type of malware) and sometimes the places that house industrial control systems may or may not follow very consistent, very rigorous, security practices creates a huge problem," said Joshi.

PJM Interconnection, a grid operator responsible for the largest grid in the U.S., covering Pennsylvania and twelve surrounding states, said the organization is aware of the threats, "however, like all cybersecurity threats, we continually monitor and arm ourselves with the best strategies to protect the grid and our market," said spokesman Paula DuPont-Kidd. **Peoples Natural Gas**, which manages 14,000 miles of pipeline in its network, does not use any of the software identified as the target of BlackEnergy and the company operates its critical assets through offline systems. "This eliminates over 99 percent of these malicious threats," said spokesman Barry Kukovich.

Scott Aaronson, senior director of national security policy for the Edison Electric Institute, has been aware of BlackEnergy

for about a month, and urges all critical firms to review the safety of their systems regularly. DHS believes there are several entities that are unaware that they have been hacked. "There are two kinds of companies: those that have been attacked and those that don't know it yet," Aaronson said. He added that there is no such thing as 100 percent security, "what we're doing is not risk elimination; it's risk management."

Anderson notes that while companies may not be able to guard against all threats, more emphasis needs to be placed on how to recover after an attack on critical systems. "How do you make sure that any damage that is done is not catastrophic, but is simply a nuisance?" he asked. The National Institute of Technology recommends best practices for critical infrastructure firms to guard and recover from cyberattacks, but some companies may fail to follow standards as rigorously as they should.

First Victims of Stuxnet Served as Gateway to Natanz

Source: http://www.hstoday.us/single-article/first-victims-of-stuxnet-served-as-gateway-to-natanz/418063b520f1bea8b89c42a7b8b6f7a9.html

More than four years after Stuxnet—the notorious computer worm that ravaged Iran's Natanz nuclear facility—was first discovered, researchers have just now identified the worm's original victims: five Iranian companies working in the industrial control systems (ICS) area.

Researchers at Kaspersky Lab, the world's largest privately held vendor of endpoint protection solutions, combed through 2,000 Stuxnet files collected over a two-year period in an effort to unearth the goals of the Stuxnet operations.

"Analyzing the professional activities of the first organizations to fall victim to Stuxnet gives us a better understanding of how the whole operation was planned," said Alexander Gostev, chief security expert at Kaspersky Lab. "At the end of the day this is an example of a supply-chain attack vector, where the malware is delivered to the target organization indirectly via networks of partners that the target organization may work with."

All five of the organizations worked in industrial control systems. In particular, the fifth organization attacked produced uranium enrichment centrifuges, among other products for industrial automation, confirming the kind of equipment that is believed to have been the main target of Stuxnet.

"Apparently, the attackers expected that these organizations would exchange data with their clients – such as uranium enrichment facilities – and this would make it possible to get the malware inside these target facilities. The outcome suggests that the plan was indeed successful," Kaspersky Lab said in a statement.

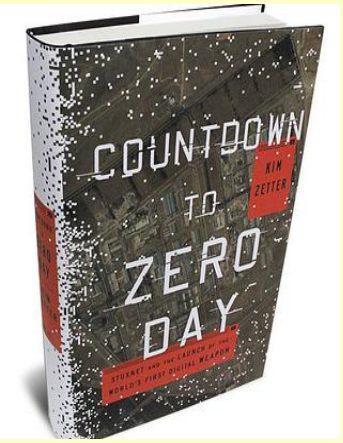
Although initial theories suggest Stuxnet spread via infected USB memory sticks plugged into PCs, researchers at Kaspersky discovered that the first worm's sample (Stuxnet.a) was compiled just hours before it appeared on a PC in the first attacked organization. In this case, since it's difficult to imagine that the attacker had enough time to compile the sample and deliver it to the target organization, **researchers believe a more plausible theory is that those behind Stuxnet used other techniques instead of a USB infection.**

How Stuxnet wormed its way into Natanz

Kaspersky's findings corroborate a February 2011 report published by Symantec, an American technology firm that analyzed more than 3,000 files of the worm and found that Stuxnet was distributed via five organizations, some of which were attacked twice – in 2009 and 2010.

Widely considered the first known cyber weapon, it is believed that the US partnered with Israel to create the virus in order to attack and slow down Iran's nuclear program. **Estimates indicate the worm destroyed up to 1,000 uranium enrichment centrifuges at Natanz, Iran's primary nuclear plant.** The attackers ended up losing control of the worm, which infected hundreds of thousands of computers in addition to its designated targets.

"The concentration of infections in Iran likely indicates that this was the initial target for infections and was where infections were initially seeded," the Symantec report stated. "While Stuxnet is a targeted threat, the use of a variety of propagation techniques (which will be discussed later) has meant that Stuxnet has spread beyond the initial target. These additional infections are likely to be 'collateral damage'—unintentional side-effects of the promiscuous initial propagation methodology utilized by Stuxnet."



Citing ***Countdown to Zero Day***, a book about Stuxnet by journalist Kim Zetter based on interviews with researchers who investigated the threat, Symantec researcher Liam O Murchu stated in a blog post that every Stuxnet sample originated outside of Natanz and can be traced back to specific companies involved in industrial control systems-type work.

An analysis of the breadcrumb log files revealed that Stuxnet did not escape from Natanz to infect outside companies but instead spread into Natanz from other organizations.

"Based on the analysis of the breadcrumb log files, every Stuxnet sample we have ever seen originated outside of Natanz," Murchu said. "In fact, as Kim Zetter states, every sample can be traced back to specific companies involved in industrial control systems-type work. This technical proof shows that Stuxnet did not escape from Natanz to infect outside companies but instead spread into Natanz."

The Kaspersky Lab researchers reached the same conclusion. By examining the trail of breadcrumbs left behind in each Stuxnet sample, the researchers were led to the five companies they believe might have served as the "patients zero"—the original victims of the attacks.

"For Stuxnet to be effective and penetrate the highly guarded installations where Iran was developing its nuclear program, the attackers had a tough dilemma to solve: how to sneak the malicious code into a place with no direct internet connections? The targeting of certain 'high profile' companies was the solution and it was probably successful," Kaspersky stated in a Securelist blog post.

'Patients zero' of Stuxnet attacks

The five Iranian organizations initially targeted in the attacks include industrial automation systems companies Foolad Technic Engineering, Behpajooh, Neda Industrial Group and Control-Gostar Jahed Company, as well as Kala Electric, which manufactures Iran's uranium enrichment centrifuges.

Foolad Technic Engineering Co., an Iranian company with headquarters in Isfahan, had plans for many of Iran's largest industrial enterprises on its network. The malware found at Foolad was compiled June 22, 2009 and had infected its first computer within hours, completely ruling out infection via a USB drive.

The company was attacked again on April 2010 by a third version of Stuxnet. Researchers believe that the persistence of the attackers indicates that Foolad may have been considered one of the shortest paths to the worm's final target.

Behpajooh Co. Elec & Comp. Engineering, located in Isfahan, was also attacked multiple times. Stuxnet spread most actively as a result of the March 2010 Behpajooh infection because of the second organization in the chain of infections that started from Behpajooh: Mobarakeh Steel Company (MSC), Iran's largest steel maker.

MSC was implicated in a US investigation of a Dubai firm smuggling bomb components into Iran. Its connection to Iran's largest steel maker, Mobarakeh Steel Company, is of particular significance, Kaspersky researchers said. The company was infected shortly after Behpajooh and could be the answer as to why Stuxnet burst out of containment.

"Stuxnet infecting the industrial complex, which is clearly connected to dozens of other enterprises in Iran and uses an enormous number of computers in its production facilities, caused a chain reaction, resulting in the worm spreading across thousands of systems in two or three months," Kaspersky researchers wrote.

The Neda Industrial Group -- an organization slapped with sanctions and charged with the illegal export of prohibited entities into Iran with potential military applications -- was only attacked once and the infection never spread outside the organization.

"However, to leave the organization may have not been

its purpose in this case," the researchers said. "As noted earlier, the capability of stealing information about STEP 7 projects from infected systems was of special interest to the creators of Stuxnet."

The fourth victim, Control-Gostar Jahed Company, was attacked only once in 2006. Researchers believe it was chosen as a target because of its extensive ties with the largest Iranian businesses in oil production, metallurgy and energy supplies.

Kala Electric, the fifth victim, especially stands out. Kaspersky indicated that, "Unlike in all above cases, the attack in this case started from three computers at once, on the same day (May 11, 2010), but at different times."

As the main manufacturer of the Iranian uranium enrichment centrifuges, Kala Electric presented the ideal target for an attack.

Given Stuxnet's main objective to render uranium enrichment centrifuges inoperable, the researchers concluded that, "It appears quite reasonable that this organization of all others was chosen as the first link in the infections chain intended to bring the worm to its ultimate target. It is in fact surprising that this organization was not among the targets of the 2009 attacks."

Consequences of Stuxnet attacks

After infecting the Natanz uranium enrichment complex in Iran and later spreading to other organizations, Stuxnet became known as a harbinger of a new era of highly sophisticated state-sponsored attacks on industrial control systems.

"Stuxnet remains one of the most interesting pieces of malware ever created," Kaspersky Lab said. "In the digital world, one might say it is the cyber equivalent of the atomic attacks on Nagasaki and Hiroshima from 1945."

Although the US and Israel are widely believed to be behind Stuxnet, the researchers do not pose any new theories about the perpetrators of the attacks.

Kaspersky indicated that one of the biggest remaining questions is whether there were any other malware like Stuxnet released, or whether it was a one-of-a-kind experiment. Only time will tell.

Researchers identify sophisticated Chinese cyberespionage group

By Ellen Nakashima

Source: http://www.washingtonpost.com/world/national-security/researchers-identify-sophisticated-chinese-cyberespionage-group/2014/10/27/de30bc9a-5e00-11e4-8b9e-2ccdac31a031_story.html

October 18 – A coalition of security researchers has **identified a Chinese cyberespionage group that appears to be the most sophisticated of any publicly known Chinese hacker unit and targets not only U.S. and Western government agencies but also dissidents inside and outside China.**

News of the state-sponsored hacker group dubbed **Axiom** comes a week before Secretary of State John F. Kerry and two weeks before President Obama are due to arrive in Beijing for a series of high-level talks, including on the issue of cybersecurity.

In a report to be issued Tuesday, the researchers said Axiom is going after intelligence benefiting Chinese domestic and international policies — an across-the-waterfront approach that combines commercial cyberespionage, foreign intelligence and counterintelligence with the monitoring of dissidents.

Axiom's work, **the FBI said in an industry alert this month, is more sophisticated than that of Unit 61398, a People's Liberation Army hacker unit that was highlighted in a report last year.** Five of the unit's members were indicted this year by a U.S. grand jury. The researchers concur with the FBI's conclusion, noting that, unlike Unit 61398, Axiom is focused on spying on dissidents as well as on industrial espionage and theft of intellectual property.

"Axiom's activities appear to be supported by a nation state to steal trade secrets and to target dissidents, pro-democracy organizations and governments," said Peter LaMontagne, chief executive of Novetta Solutions, a Northern Virginia cybersecurity firm that heads the coalition. "These are the most sophisticated cyberespionage tactics we've seen out of China."

Chinese Embassy spokesman Geng Shuang said in an e-mail

that "judging from past experience, these kinds of reports or allegations are usually fictitious." He repeated Beijing's position that Chinese law prohibits cybercrime and that the government

"has done whatever it can to combat such activities."

Senior Obama administration officials have over the past year and a half publicly called on China to halt its practice of stealing U.S. commercial secrets to benefit its own industries. China, especially in the wake of disclosures last year of widespread U.S. government surveillance by former National Security Agency contractor Edward Snowden, has pushed back, arguing that it is the United States that needs reining in.

Geng said in his e-mail: "China is a victim of these kinds of attacks, according to the Snowden revelations." Following the PLA indictments in May, Beijing pulled out of bilateral talks aimed at easing tensions in cyberspace.

In recent weeks, the research consortium has detected Axiom malicious software on at least 43,000 computers around the world belonging to law enforcement and other government agencies, journalists, telecommunication and energy firms, and human rights and pro-democracy groups.

The group said there also are indications that Axiom may be behind a high-profile cyberattack on Google, announced in 2010, which compromised the tech giant's source code and targeted Chinese dissidents using Gmail.

At least one Chinese-language computer in the United States was targeted, the report said, without specifying to whom the computer belonged.

Novetta senior technical director Andre Ludwig also said Axiom is seeking to hack personnel management agencies to obtain the personal data of people who have access to classified information that it can use for future targeting.

Axiom has been active for at least six years and employs techniques that make it stand out from other hacker groups, the researchers said. For one thing, it is highly skilled at burying malware within legitimate computer traffic so that a company or agency analyst who is studying traffic logs cannot detect it, Ludwig said.

The malware, called Hikit, can create multiple points of presence — what Ludwig called "breadcrumbs" inside the network to help Axiom move around and steal data, all without arousing suspicion.

Axiom also appears to have a "maintenance cycle" in which it periodically switches out malware, Ludwig said. "They have an advanced playbook," he said.

Unlike the security firm Mandiant, which reported on Unit 61398, the researchers were unable to identify the locations in China where Axiom operates from or identify its members. Axiom's members, Ludwig said, are better at covering their tracks than those of Unit 61398. They did not, for example, keep e-mail accounts or have an online presence that could be traced back to them.

China military expert Mark Stokes said it was "not surprising" to find that Unit 61398 was not as sophisticated as Axiom. That unit is part of the second bureau of the PLA's Third Department, which is the rough equivalent of the NSA. "Cyber seems a really small part of second bureau's broader mission, which is signals intelligence," said Stokes, executive director of Project 2049 Institute, an Arlington think tank. "There are other parts of 3 PLA that reasonably could be expected to have a much more dedicated cyber mission."

Some security experts said the report carries valuable remediation advice not often seen in such reports. The researchers created custom "signatures," ways to detect Axiom malware in users' computers. This is the sort of data more traditionally exchanged in

private intelligence-sharing groups, the experts said.

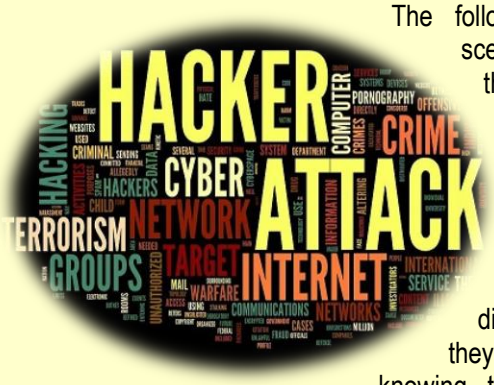
"This is the beginning of what will hopefully be a long line of industry-coordinated efforts to expose these threat groups, and to do so without having to use law enforcement, to help corporations and governments around the world combat" hackers, said Stephen Ward, senior director of iSight Partners, another coalition member. "This is a big first step."

Other coalition members include Microsoft, Bit9, Cisco, FireEye, F-Secure, Symantec, Tenable, ThreatConnect, ThreatTrack Security, Volexity and threat researchers who did not wish to be identified.

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.

Cyber warfare: it is already possible to prevent hostile hijacking of nuclear facilities' computers and systems

Source: http://i-hls.com/2014/11/command-control-unmanned-platforms-based-rugged-systems/



The following is a realistic scenario, not fictional: the enemy succeeds in taking over the computers at a nuclear power station's command center. The operators' screens display no alert and they have no way of knowing the facility had just been remote-breached. The production array and critical parameters, including the reactor's core cooling, are changing in an alarming way, but the perpetrators carefully saw to it that the monitoring system would not update technicians. The time it takes the on-site staffs to realize they are under attack, to track the hackers and avert disaster is way too long, posing a risk to both the reactor and to national security.

How realistic is this scenario? With 90% of all targeted cyber-attacks aiming at critical infrastructure sectors, there is no doubt a real change is called for in the overall cyber security doctrine of such facilities, along with a transition to innovative technologies to ensure more advanced security for computerized, operational and communications systems. The cyber warfare arena has been heating up in recent years. Sophisticated hackers, hostile countries, disgruntled employees within organizations, terror groups and the like, are each capable of posing a major threat. The situation each CEO is concerned with nowadays, is someone taking over the organization's central computing/operational systems and wreaking havoc in them. This challenge of securing critical infrastructure has intensified considerably, since beyond integrating advanced computing, the industrial world is fast approaching a new age in which machines interface with online command and control systems. Progress indeed entails numerous advantages, but at the same time it exposes such organizations to cyber threats and real dangers on both the virtual and physical levels.

Traditional security measures used by almost any organization do not amount to much of a solution. They rely upon known elements an assailant can use: signatures of malware files, rules, pattern identification, behavioral modes and so on, in hope that given the opponent's modes and means, they could be neutralized in advance. Such methods have worked in the past, and may still constitute some defense against foreseeable threats or ones which can be anticipated. Nevertheless, in a world undergoing a third industrial revolution and is already at an age when machines 'talk' with each other and make decisions – how do you deal with unprecedented attacks and schemes, ones we cannot even fathom?

In order to defend critical infrastructure efficiently, it is important to begin by realizing that sophisticated, targeted hacks would not use run of the mill means. They will investigate and a coordinate ZeroDay breaches or launch APTs (Advanced Persistent Threats) in such manner that they will never be detected prior to achieving

their objectives. Such orchestrated attacks require proactive defense as they abuse the unknown vulnerabilities which cannot be traced using existing solutions. What makes the situation all the more complex is the bringing of mechanical systems, hitherto offline, into the online world, when today's known data security means cannot provide a solution to the system differentiations in these environments, in the framework of which old machinery generate communication and data, alongside cutting edge computing and smart control systems.

The groundbreaking solution introduced by the Israeli startup, ThetaRay, solves the problems of this multiplex, unfathomable threat to computerized and mechanical systems by linking up to the organization's entire data array, operative systems and machinery, monitoring all the data they generate and analyzing all the sources at the same time.

This innovative ability allows ThetaRay to leverage organizational Big Data in order to discover anomalies, which would lead within seconds to uncovering threats and attacks on the organization, whether they originate from within or outside, as well as those unfolding secretly, as they had not been detected upon their initial infiltration into the organization. The solution, which is applied using cutting edge mathematical algorithms, has been patented following joint development by scientists from Yale and Tel Aviv Universities for over a decade.

This innovative approach is expressed in the company's methodology: no more deduction based on changes in patterns and signatures or rules and alerts concerning deviations from pre-defined thresholds, but rather, system-level and global level connection to all organizational data generators, including networks and machinery. The company's methodology further relies on applying mathematical tools to the organizational Big Data, without any prior knowledge regarding the data itself or any reliance on understanding potential threats.

The combination of technological, academic and industrial disciplines allows ThetaRay to carry out multi-dimensional analysis of data streaming in from various sources, in various formats and different timing, and issue effective, accurate and primarily rapid analysis, complete with an especially low level of false alarms. It is estimated that all this allows for the discovery of sophisticated attacks, or undiagnosed operational damages, to be drastically accelerated from several weeks to mere seconds.

No less important: the system filters the false alerts and even groups together all the instances related to the same single incident rather than issue numerous alerts, thereby enabling the organization's security staff to increase response efficiency and prevent disasters.

China Developing Holographic UAV Control Center

Source: http://i-hls.com/2014/11/china-developing-holographic-uav-control-center/

China's biggest aviation manufacturer, Aviation Industry Corporation of China (AVIC), is developing a holographic ground control system (GCS) for UAVs.

Unveiled at Airshow China here, the "nerve center" or GCS displays the UAV as a holographic image. It allows the controller to command the aircraft, obtain flight parameters and information on navigation and guidance through a "human-machine interface."

According to *Defense News*, the controller experiences the entire process of the mission via this interface, including mission payload, route planning, flight control, identification of friend/foe, precision strikes and task assessment of the UAV operational environment.

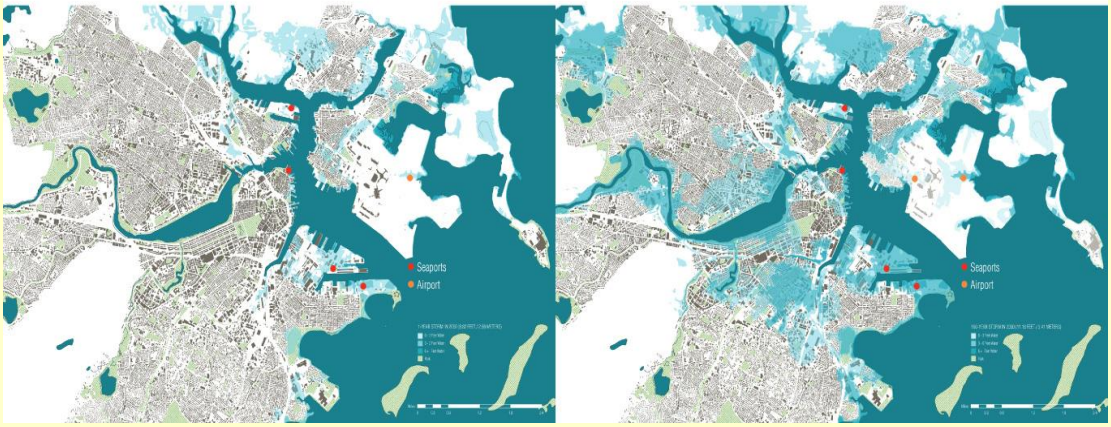
Building a network of canals to save Boston from sea level rise

Source: http://www.homelandsecuritynewswire.com/dr20141028-building-a-network-of-canals-to-save-boston-from-sea-level-rise

By the end of the century, sea-level rise on the U.S. east coast is predicted to reach six feet, so city planners in Boston recently met to discuss how to live with rising waters along the city's historic streets. **One suggestion is to turn Boston's Back Bay district into a network of canals.** "Much of the model has been how do we keep the water out? Everybody's afraid of the water," says Dennis Carlberg, sustainability director at Boston University and co-chair of Boston's sea-level rise committee. "So we wanted to turn that conversation on its head and say, well what if we let water in? How can we make life better in Boston by bringing water in?"

According to BBC News, the idea for turning streets into canals came about in May when national real estate association, the Urban Land Institute, held brainstorming sessions involving architects, developers, real estate experts, and business owners to discuss ways of preserving the city's buildings as sea-levels rise. "It can't be that we provide a giant

Figure 1: Major Massport Facility Locations and Flooding During 1-Year Storms [Left] and 100-Year Storms [Right] in 2050



dam at the Boston harbor and solve all our problems that way," says Boston's Chief of Environment, Energy and Open Space, Brian Swett. "The way we solve this has to be vibrant, liveable, exciting and enhance our quality of life."

Back Bay, a neighborhood which was actually a tidal bay before it began to be filled in and built on 150 years ago, now houses rows of five story brownstone homes arranged in a grid pattern. "Currently the Back Bay streets are about four feet above high tide, so if the sea level rises as predicted, they would be underwater part time by the end of the century," says Harvard Business School's John Macomber, who helped assess the financial implications of the canal concept.

The canals would alleviate sea-level rise by draining water into lower-lying back alleys and some main streets, but the proposed plan would have to contend with freezing temperatures in the winter. "The question is whether in a climate where it can snow for six months of the year you want canals that are always open and partly full of slush, sand and salt," says Macomber.

Other options for coping with sea-level rise include re-introducing natural wetland habitats that would soak in excess water. "As sea level rises, we are going to be losing this natural sponge globally, so trying to add some of it back is an important thing to be paying attention to," says Carlberg.

Architect Amy Korte, who is working on building design in Boston's Innovation District, has proposed increasing the foundation height for vulnerable structures and make sure critical infrastructure, such as electrical and mechanical equipment, are placed above flood levels. "We've looked at raising the ground floor elevation as much as possible," Korte said. "We asked how do we raise critical equipment and create a new vision for what good urban design can be."

Swett compares the recommendations for coping with sea-level rise to Venice and Amsterdam. **"Boston's been around for 400 years and we're going to be around for another 400. Amsterdam is already more than 700 years old, and Venice more than 1,500. So canals can work - even if they do make it more difficult to park."**

EDITOR'S COMMENT: This is a good idea! But if I could expand it a bit more, I would suggest thinking about creating new rivers, expand old ones and interconnect rivers. Big costly projects you might say! But big problems require big (out of the box) solutions!

EMS drone dramatically increases survival chances of heart attack patients, accident victims

Source: http://www.homelandsecuritynewswire.com/dr20141029-ems-drone-dramatically-increases-survival-chances-of-heart-attack-patients-accident-victims

Graduate student Alec Momont of TU Delft in the Netherlands has designed an unmanned, autonomously navigating mini airplane that can quickly deliver a defibrillator to where it is needed. A network of such drones could significantly increase the chance of survival following a cardiac arrest: from 8 percent to 80 percent.

Momont, of TU Delft's Faculty of Industrial Design Engineering, designed his prototype for an ambulance drone together with the Living Tomorrow innovation platform as part of his graduation program. A Delft TU release reports that when the emergency services receive a cardiac arrest call, this unmanned, autonomously navigating plane can quickly deliver a defibrillator to the emergency scene. Via a livestream video and audio connection, the drone can also provide direct feedback to the emergency services and the persons on site can be instructed how to treat the patient. The drone finds the patient's location via the caller's mobile phone signal and makes its way there using GPS. **The drone can fly at around 100 km/h, weighs 4 kg, and can carry another 4 kg.**

"It is essential that the right medical care is provided within the first few minutes of a cardiac arrest," says Momont. "If we can get to an emergency scene faster we can save many lives and facilitate the recovery of many patients. This especially applies to emergencies such as heart failure, drowning, traumas, and respiratory problems, and it has become possible because life-

saving technologies, such as a defibrillator, can now be designed small enough to be transported by a drone."

So Momont set to work and designed a new type of drone: a compact flying "medical toolbox," which carries essential medical equipment that anybody can use. This first prototype has been designed to transport a defibrillator.

"Some 800,000 people suffer a cardiac arrest in the EU every year, and only 8 percent survive," Momont explains. "The main reason for this is the relatively long response time of the emergency services (approximately ten minutes), while brain death and fatalities occur within four to six minutes. The ambulance drone can get a defibrillator to a patient inside a twelve km2 zone within one minute. **This response speed increases the chance of survival following a cardiac arrest from 8 percent to 80 percent.'**

The communications channel (a Webcam) built into the drone is also very important. This allows the emergency operators to see what is going on and provide instructions to the person applying the defibrillator, who in their turn can also ask the emergency operator questions. "Currently, only 20 percent of untrained people are able to successfully apply a defibrillator," says Momont. "This rate can be increased to 90 percent if people are provided with instructions at the scene. Moreover, the presence of the emergency operator via the drone's loudspeaker helps to reduce the panic of the situation."

Momont proposes expanding the existing emergency medical infrastructure with a network of fast and compact drones that have communication capabilities and can carry medical auxiliary equipment. "The costs should not be an issue; I have calculated these at approximately €15,000 per drone, which is clearly a reasonable amount if you consider the number of lives that could be saved."

"There are still a number of obstacles in the way of the development of the ambulance drone," says Momont. The drone can fly autonomously, however, and this is still not permitted by law. New Dutch legislation in this area is expected to be passed in 2015. Moreover, the drone has not yet been tested on "real" patients, and the object avoidance system for avoiding obstacles in the drone's path needs improvement.

Momont, however, still thinks his invention could be implemented within five years. A number of parties in the medical sector have

already registered their interest in the project. **Momont developed the ambulance drone in collaboration with the Belgian innovation platform Living Tomorrow, which helped to fund the project.** The next steps towards the development and implementation of the prototype are presently being considered together with Ghent University Hospital and Ghent University, both partners in Living Tomorrow. Momont is also working together with the Amsterdam Ambulance Service.

Rapid response team on motorcycles in the center of Israel

Source: http://i-hls.com/2014/10/rapid-response-team-motorcycles-center-israel/

Israel's Fire and Rescue Services will soon deploy a motorcycled search and rescue rapid response team which will operate in the center

of Israel. The team will focus on search and rescue missions following car crashes and car fires.

Israel's fire brigade training school has recently began a special training program comprising 10 firefighters who have been carefully chosen to constitute the Fire and Rescue Services' rapid response team to handle traffic-related events. They will primarily rescue people from car accidents and burning vehicles.

The first stage will feature 3 BMW 650 GS motorcycles (photo) which were recently purchased complete with firefighting and search and rescue kits.

The unique feature of this new unit is that customarily, firefighting motorcycles are deployed separately from rescue motorcycles throughout the world, whereas in Israel, the unit will carry out both duties. These motorcycles have been fitted and customized ahead of their planned designation, primarily in terms of their safety means.

Firefighting Officer Ehud Ben Ezra, who is in charge of training, said the course will last four weeks and consist of both theoretic and practical motorcycle driving as well as lessons on operating the dedicated equipment.

The officers will train in the following:

Emergency protocols vis-à-vis various types of vehicles, such as an electric vehicles, buses and hazardous materials' carriers

Search & rescue from cars and from commercial vehicles

Operating the dedicated equipment, the firefighting kit and motorcycle rescue devices

The current course is planned as a pilot program for assessment and evaluation. There are plans for future acquisition of additional motorcycles, per funding from Israel's National Road Safety Authority.

Sound-steered cyborg cockroaches could help save human lives

Source: http://www.gizmag.com/sound-steered-biobot-rescue-cockroaches/34630/?utm_source=Gizmag+Subscribers&utm_campaign=8e6ea6574f-UA-2235360-4&utm_medium=email&utm_term=0_65b67362bd-8e6ea6574f-90124985

If you're ever trapped in a collapsed building and are calling for help, you might want to think twice before squashing any cockroaches that wander your way – one of them might have been sent to find you. Researchers from North Carolina State University are currently laying the groundwork for such a scenario, by getting cyborg-like "biobot" cockroaches to move towards sounds. Down the road, such insects may be used to locate victims at disaster sites.

We first heard about the biobots a couple of years ago. Developed by a team led by Dr. Alper Bozkurt, each one consists of a Madagascar hissing cockroach equipped with a "backpack" that contains an inexpensive microchip, a wireless receiver/transmitter, and a microcontroller.
That microcontroller is wired into the cockroach's antennae and cerci. The cerci are sensory organs in the abdomen, that detect air movement in order to warn of approaching predators. When the cerci are instead stimulated by the microcontroller, the cockroach still thinks that something is coming at it from behind, and scuttles forward.

In order to direct that forward movement, either one of the antennae are stimulated. Ordinarily, they're activated when they brush against unyielding objects, letting the cockroach know that it can't move in that direction. In this case, when the stimulation comes not from an object but from a small electrical charge, the insect still reacts by changing course.
Previously, both human operators and a Kinect-equipped computer have used that system to steer the biobots by wireless remote control. In the most recent study, however, an array of three-directional microphones was added to each cockroach's backpack. By analyzing the sound detected by each of those mics, software was able to determine the location of the source of that sound. It then activated the biobot's microcontroller accordingly, in order to steer the insect toward that location.
Some cockroaches were also equipped with just a single high-resolution mic. It is hoped that eventually, biobots with those mics could be used to differentiate victims' voices from other noises at disaster sites. Once a voice was detected, the multi-mic biobots could be activated to seek out its source. Although the cockroaches couldn't do much to help those people themselves, rescuers could track them via their transmitters, to establish the whereabouts of the victims. A previous study has already indicated that the biobots can be used to map disaster sites.

New technology increases awareness of landslide risks

Source: http://www.homelandsecuritynewswire.com/dr20141120-new-technology-increases-awareness-of-landslide-risks

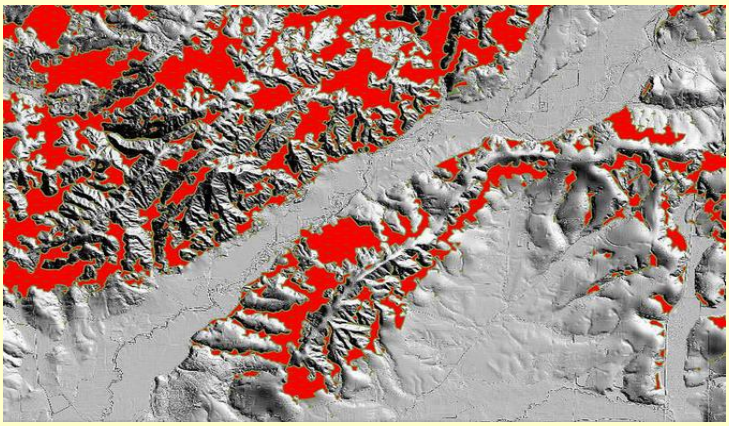
Engineers have created a new way to use lidar technology to identify and classify landslides on a landscape scale, which may revolutionize the understanding of landslides in the United States and reveal them to be far more common and hazardous than often understood.

The new, non-subjective technology, created by researchers at Oregon State University and George Mason University, can **analyze and classify the landslide risk in an area of fifty or more square miles in about thirty minutes — a task that previously might have taken an expert several weeks to months**. It can also identify risks common to a broad area rather than just an individual site.
An OSU release reports that with such speed and precision, it reveals that some landslide-prone areas of the Pacific Northwest are literally covered by landslides from one time or another in history.
The system is based on new ways to use light detecting and ranging, or lidar technology, that can seemingly strip away

vegetation and other obstructions to show land features in their bare form.

"With lidar we can see areas that are 50-80 percent covered by landslide deposits," said Michael Olsen, an expert in geomatics and the Eric HI and Janice Hoffman Faculty Scholar in the OSU College of Engineering. "It may turn out that there are 10-100 times more landslides in some places than we knew of before.

"We've always known landslides were a problem in the Pacific Northwest," Olsen said.



"Many people are just now beginning to realize how big the problem is."

An outline of the new technology was recently published in *Computers and Geosciences*, a professional journal.

Oregon and Washington, especially in the Coast Range and Cascade Range, are already areas commonly known to have landslides, and as a result Oregon's Department of Geology and Mineral Industries has become a national leader in mapping of them, Olsen said. But previous approaches are slow, and the new technology, called a Contour Connection Method, could radically speed up widespread mapping, and build both professional and public awareness of the issue.

Despite the prevalence and frequency of landslides, they are not generally covered by most homeowner insurance policies; coverage can be purchased separately, but most people do not. And with increasing population growth, more and more people are moving into more remote locations, or building in scenic areas near the hills around cities where landslide risk might be high.

Mapped landslide inventory

"A lot of people don't think in geologic terms, so if they see a hill that's been there for a long time, they assume there's no risk," said Ben Leshchinsky, a geotechnical engineer in the OSU College of Forestry. "And many times they don't want to pay extra to have an expert assess landslide risks or do something that might interfere with their land development plans."

Lidar is already a powerful tool, but the new system developed at OSU offers an automated way to improve the use of it, and could usher in a new era of landslide awareness, experts say. Information could be more routinely factored into road, bridge, land use, zoning, building and other decisions.

With this technology, a computer automatically looks for land features, such as suddenly steeper areas of soil that might be evidence of a past landslide. It then searches the terrain for other features, such as a "toe" of soils at the base of the landslide. And in minutes it can make unbiased, science-based classifications of past landslides that consistently use the same criteria.

The release notes that the technology was applied to the region surrounding the landslide of March, 2014, that killed 43 people near the small town of Oso, Washington (photo below). In about nine minutes it was able to analyze more than 2,200 acres and many prehistoric landslide features that are readily apparent in lidar images, in this region known for slope instability.

Eventually, adaptations of the technology might even allow for real-time monitoring of soil movement, the researchers said.

— Read more in Ben A. Leshchinsky et al., "Contour Connection Method for automated identification and classification of landslide deposits," Computers & Geosciences *74 (January 2015): 27-38*

NASA facilities across U.S. vulnerable to climate change

Source: http://www.homelandsecuritynewswire.com/dr20141106-nasa-facilities-across-u-s-vulnerable-to-climate-change

November 06 – The National Aeronautics and Space Administration (NASA) has been at the forefront of climate science, launching satellites that take the pulse of Earth's land, oceans, and atmospheric systems, gathering data on climate, weather, and natural hazards. The agency, however, is itself increasingly vulnerable to the effects of a changing climate. Hurricane Isabel partially flooded the Langley Research Center in Virginia in 2003; Hurricane Frances damaged the Kennedy Space Center in Florida in 2004; and Hurricane Katrina damaged buildings at the Stennis Space Center in Mississippi in 2005, among recent incidents. Other facilities have been damaged or threatened by tornadoes and wildfires.

A NASA release reports that a new study in the latest issue of the *Bulletin of the American Meteorological Society* found that NASA facilities and its overall mission could be threatened by an increase in extreme weather events and expected sea level rise. Using weather data and climate models, the study looked at how NASA facilities have been affected by climate change, including extreme weather events, and how the agency is preparing for the future.

With major facilities located along coastlines, NASA is particularly vulnerable to sea level rise. The study found that sea level rise could lead to an increase of 50 percent or more in coastal flooding frequency by the 2050s.

"It's a great experience working at NASA Centers across the country to enhance climate resilience. They are explicitly taking increasing risks due to climate change into account in their operations and planning," said Cynthia Rosenzweig, lead author of the study and a scientist at NASA's Goddard Institute for Space Studies in New York, which is affiliated with Columbia University's Earth Institute.

Rosenzweig heads the Climate Adaptation Science Investigator working group, which brings together climate scientists, mission operations personnel, human resource managers and ecosystem specialists to study and plan for the management of climate risks. NASA operates some $32 billion in facilities and has about 64,000 employees, contractors and partners.

At the Kennedy Space Center in Florida, home of NASA's premiere launch facility, launch pads and other facilities could experience inundation due to rising sea level and coastal flooding, according to one in a series of reports on NASA facilities prepared by the working group.

The added flooding and an increase in heavy precipitation events could mean increased erosion of coastline and changes in shoreline habitats, and challenges to stormwater and wastewater management systems. Higher average temperatures would add to cooling costs, increased restrictions on outdoor labor and damage to infrastructure materials, the report says. On the plus side, the prediction of fewer days before freezing would mean reduced

heating costs and possible expansion of launch windows.

"Actual weather data collected over the past 100 years in Florida point to one undeniable fact: average temperatures and sea level are rising," the report says. "In addition, climate models project accelerated temperature and sea level rise and an increase in extreme weather events — including heat waves, coastal flooding, and intense precipitation — for the Space Coast in the future.

"Already, the area shows signs of climate vulnerability: Outdoor work schedules must accommodate increasing temperatures, storm surges regularly breach the dunes near the launch pads, and sea turtles were rescued during a January 2010 cold stun event," the report says.

The area also encompasses the Cape Canaveral Air Force Station and large swaths of coastal habitat that is home to many types of wildlife. The federal aerospace facilities — and associated businesses and tourism — add substantially to the state's economy. NASA alone contributes an estimated $4.1 billion, according to one state-sponsored report.

The Space Center's launch facilities provide "a critical asset for the nation — access to orbits that cannot be obtained from launches anywhere else in the U.S.," the NASA report says.

The release notes that while the Goddard Institute for Space Studies studies the solar system, stars, and planets, it also has focused on Earth systems, including atmosphere and climate, and has become a key center for the development of atmospheric modeling and understanding climate change.

For details on specific impacts at many NASA facilities, see here.

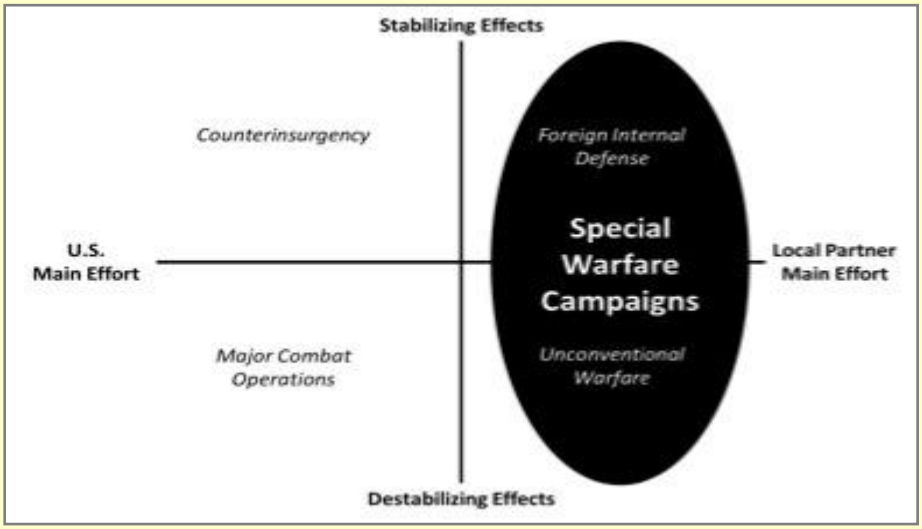
— Read more in Cynthia Rosenzweig et al., "Enhancing Climate Resilience at NASA Centers: A Collaboration between Science and Stewardship," Bulletin of the American Meteorological Society, *95, no. 9 (September 2014): 1351-63*

Special Warfare: The Missing Middle in U.S. Coercive Options

By Dan Madden, Dick Hoffmann, Michael Johnson, Fred T. Krawchuk, John E. Peters, Linda Robinson and Abby Doll

Source: http://warontherocks.com/2014/11/special-warfare-the-missing-middle-in-u-s-coercive-options/

In the face of adversaries exploiting regional social divisions by using special operations forces and intelligence services, and dwindling American appetite for intervention, the United States needs to employ a more sophisticated form of *special warfare* to secure its interests. Special warfare campaigns stabilize or destabilize a regime by operating "through and with" local state or nonstate partners, rather than through unilateral U.S. action. Special operations forces are typically the primary U.S. military forces employed, but successful campaigns depend on bringing to bear a broad suite of U.S. government capabilities. The figure below differentiates special warfare from more familiar forms of conflict. Special warfare has particular relevance to the current global security environment as policymakers seek options short of large-scale intervention to manage both acute crises (e.g., ISIL, Ukraine) and chronic challenges (e.g., insurgency in the Philippines). Special warfare fills the missing middle for exerting influence between the costly commitment of conventional forces and precision-



strike options provided by drones, aircraft, missiles, and special operations forces' direct action. The potential for escalation associated with precision-strike capabilities may render them too risky to employ in some circumstances, while in cases where the targeted regime's core interests are involved, precision-strike options may be too little to compel desired changes in behavior. Despite policymaker antipathy toward the costs and risks of intervention, observed and forecasted instability around the world will continue to create situations in which policymakers are forced to act to protect U.S. interests. Special warfare provides these decisionmakers with an additional option that can help protect American interests and manage risks in some important cases.

Special warfare is not new. The United States has a long (and somewhat checkered) history of special warfare operations. Classic cases from the 1980s include U.S. support to the government of El Salvador against the Farabundo Martí National Liberation Front Marxist insurgents and to the Mujahedeen in Afghanistan against the Soviets. In the former case, the U.S. military was restricted to providing no more than 55 advisors, who did not participate in combat operations. In the latter case, operations were conducted almost entirely from and through a third country, Pakistan. However, more than a decade of focus on counterterrorism, Iraq, and Afghanistan has atrophied U.S. special warfare campaign design skills in the military and appreciation for special warfare's employment as a strategic tool in the policy community. Efforts are being made, however, to reinvigorate special warfare capabilities.

The United States is not the only country with special warfare capabilities, as explored by other analysts and practitioners on War on the Rocks, including Dave Barno, Nadia Schadlow, and Lawrence Freedman. Russia has recently been successfully exploiting a mix of coethnic sentiment, special operations activities, and conventional deterrence to annex Crimea and destabilize eastern Ukraine. Some Baltic officials, sensitive to the presence of substantial Russian minorities in their own countries, are anxious over what might come next.

Iran has skillfully employed its own special warfare capabilities as part of a long-term regional strategy, using state tools and nonstate proxies to advance its regional interests. Iran's actions in Syria, for example, have contributed to a vexing dilemma for the United States, in which both action and inaction threaten policy disaster—the former an Iraq-style quagmire and the latter an uncontrolled regionalization of Sunni-Shia sectarian conflict. The Syria dilemma is symptomatic of Iran's broader efforts to establish a sphere of influence in the Middle East through mechanisms that ingrain instability in the structure of sectarian interrelations, which are similarly exemplified by its patronage of clients such as Hezbollah and its Quds Force activities in Iraq and other Arab states. Coupled with its quest for nuclear capability, Iran's activities risk a cascading proliferation of nuclear weapons in a deeply divided region. In the longer term, if Iran's quest for, and Russia's exercise of, nuclear deterrence and irregular influence are seen as successful asymmetric strategies for circumventing U.S. conventional dominance, other regional or aspiring global powers might adopt similar approaches to securing their interests.

The United States should consider employing special warfare campaigns to counter the aggressive employment of proxies by states competing for regional influence. Though there is no obligation for the United States to fight its adversaries symmetrically, adversaries are challenging the nation in ways difficult to credibly deter with conventional campaigns or precision strikes alone. If the United States were to rebalance its dependence on precision-strike, conventional, and special warfare capabilities, and how they are used to complement one another, it might

constitute a change in strategic posture analogous to the shift from Eisenhower's New Look dependence on massive nuclear retaliation for deterrence to Kennedy's Flexible Response policy for deterring aggression at multiple levels of the escalation ladder.

Our findings and recommendations are based on semi-structured interviews with special warfare practitioners and researchers, observed military exercises, a review of relevant literature, country and theater campaign plans, case studies, and analysis of a dataset of special warfare operations that our team constructed for this study.

Characteristics of Special Warfare

Special warfare campaigns, properly conducted, are far more than an activity for Special Operations Forces. They involve the comprehensive orchestration of U.S. government capabilities to advance policy objectives. Special warfare campaigns have six central features:

- Their goal is stabilizing or destabilizing targeted regimes;
- Local partners provide the main effort;
- U.S. forces maintain a small (or no) footprint in the country;
- They are typically of long duration and may require extensive preparatory work better measured in months (or years) than days;
- They require intensive interagency cooperation in which DOD may be subordinate to the State Department or Central Intelligence Agency (CIA); and
- They mobilize, neutralize, or integrate individuals or groups from the tactical to strategic levels.

Special warfare might be thought of as the art of making or breaking coalitions. Historically, U.S. Special Operations Forces have found their comparative advantage at the tactical level, while other government agencies have found theirs at the strategic level. It is this political element at this strategic level of special warfare campaigns that requires intensive interagency collaboration, creating situations where the joint force may be supporting an effort led by the State Department or CIA.

Strategic Advantages

Some advantages of special warfare include:

- **Improved understanding and shaping of the environment**. Special warfare, executed through intelligence or select military activities, can improve U.S. contextual understanding of potential partners and the situation on the ground before the United States commits to a course of action.
- **Cost-imposing strategies**. Special warfare's small-footprint approach allows the United States to pursue cost-effective, cost-imposing strategies, forcing opponents to spend disproportionate amounts to defend against friendly capabilities.
- **Sustainable solutions**. Special warfare's small-footprint approach can be more fiscally and politically sustainable than alternatives when underlying sources of conflict cannot be resolved in the short term, preserving core U.S. interests at costs that the nation is willing to bear. From a host nation or coalition political perspective, commanders can also use special warfare's partner-centric approach to design campaigns around a partner's core interests, rather than hoping to transform those interests in ways that have frequently proven to be ephemeral.
- **Managed escalation and credibility risk**. Given a decision to intervene, policymakers could use special warfare to avoid making commitments beyond U.S. interests. However, decisionmakers must carefully assess the escalation criteria and the options of adversaries and their external partners. Assessing the adversary's (and America's own) likely escalation behavior is fraught with uncertainty, not least because adversaries may not understand how their own preferences may change as the situation evolves (e.g., jingoistic pressure from domestic constituencies).

The notion that special warfare campaigns' escalation dynamics are simpler to manage than conventional or distant-strike campaigns is context dependent, but we offer the following evidence and arguments. Distant-strike campaigns against a peer competitor suffer from both a crisis instability problem, where each side has an incentive to strike first, and an ambiguity problem, where a lack of knowledge over the disposition of strategic weapons (e.g., mobile nuclear ballistic missiles) may cause the targeted state to believe that the United States is escalating vertically beyond what is intended. Because special warfare

campaigns unfold over a protracted time horizon, the same crisis instability problem does not hold. Time and space exists for political deliberation and negotiations.
Conventional campaigns (here either major combat operations or counterinsurgency) suffer from much larger political sunk costs that create incentives for the gambling for resurrection phenomenon, which has been used to describe President Lyndon Johnson's decision to escalate in Vietnam. Our analysis of special warfare campaign data found most outcomes indeterminate, meaning neither a decisive win nor loss at the operational level, and yet only in the case of South Vietnam was the conflict escalated into a conventional conflict. In the 1980s, Congress actually passed a law shutting down U.S. support to the Contras, indicating how different the political dynamics governing special warfare campaigns are when compared with other unpopular wars in which efforts in Congress to halt funding for the conflict became conflated with the emotive issue of support for U.S. troops (e.g., Iraq). Conversely, a U.S. unconventional warfare campaign supporting Tibet lasted decades without serious escalation risk or domestic political contestation.

Limits and Risks

As noted earlier, special warfare campaigns are characterized by operations in which the local partner provides the main effort. This dependency on partners carries a set of risks and limitations, as do other characteristics of special warfare. These include:

- **Divergent partner objectives**. A U.S. partner may have core objectives that conflict with those of the United States, or the partner may simply prioritize them differently.
- **Ineffective partner capability**. The opponent's level of capability and operational tempo relative to the partner's may render special warfare solutions ineffective within the required time horizon.
- **Unacceptable partner behavior**. Some partners may behave in ways that transgress America's normative standards (e.g., respect for human rights) and undermine their own sources of legitimacy.
- **Policy fratricide**. If special warfare campaigns are not carefully integrated into a holistic U.S. policy toward the targeted country (e.g., through geographic combatant command, country team, and NSS coordination), U.S. efforts can either turn into direct conflict (e.g., between diplomatic and military lines of effort) or become out of balance.
- **Disclosure**. The global proliferation of information technology erodes the ability to keep covert activities covert.

Though the United States might avoid some of these risks by acting unilaterally, doing so would likely come at the cost of at least some of the strategic advantages identified earlier.

Conclusion

When the United States seeks to achieve its goals through special warfare, it will require a different conceptual model to design and conduct campaigns than what it is accustomed to. This is because special warfare works principally through local actors, employs political warfare methods, and requires the integration of a much broader suite of U.S. government agency capabilities than are typically envisioned in conventional campaigns. Special warfare is a way of achieving strategic goals, and given recent trends in security threats to the United States and its interests, it may often be the most appropriate way of doing so. **As a result, the U.S. national security community needs to begin thinking seriously about special warfare capabilities, authorities, and options in strategic and operational planning.** We recommend that DoD strengthen its special warfare planning capacity and culture, conduct institutional reforms to facilitate unified action among relevant U.S. government agencies, and place greater emphasis on developing capabilities required to prevail in the human domain.

Dan Madden *is a project associate at the RAND Corporation. His research focuses on irregular warfare, force modernization, and strategic and campaign planning. He is a former Marine, and has served as a defense advisor to members of Congress.*

Dick Hoffmann *is a defense research analyst at the RAND Corporation. His research covers human performance in extreme environments, joint special*

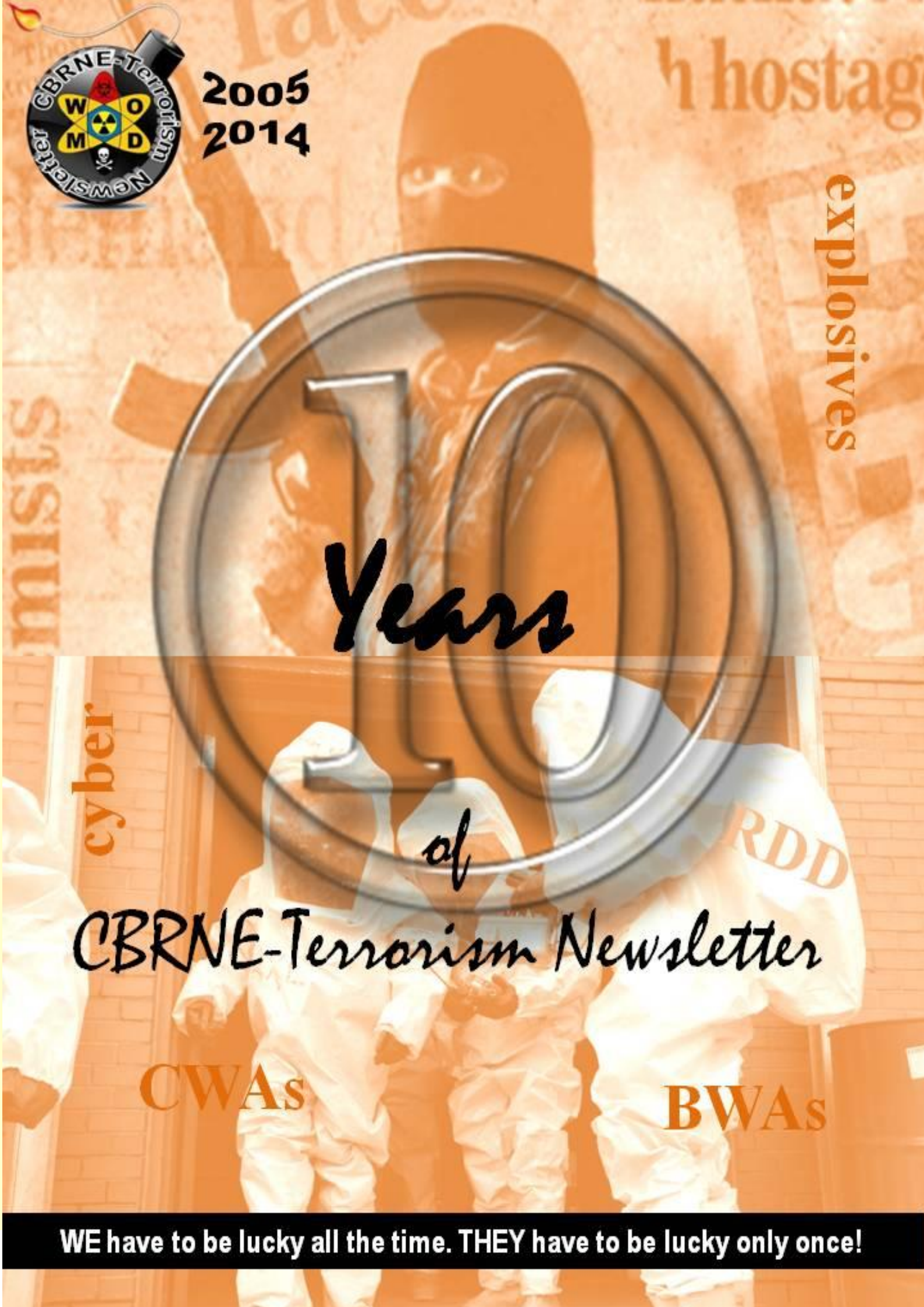
operations, and counterterrorism strategy. Before RAND, he served 20 years in the Navy as a SEAL.

***Michael Johnson** is a former U.S. Army strategic plans and policy officer with expertise in military strategy, risk assessment, joint campaign planning, joint and Army operations, military transformation, network-enabled battle command, and doctrine and force development.*

***Fred T. Krawchuk** is a consultant, visiting professor at IESE Business School, and retired U.S. Army special forces colonel who served in Iraq and Afghanistan. Fred specializes in organizational design, leadership and management, cross-cultural collaboration, complex problem solving, negotiations, and conflict resolution.*

***John E. Peters** is a senior political scientist at the RAND Corporation and a professor at the Pardee RAND Graduate School. He joined RAND in 1994 after a career in the U.S. Army. His background includes work in arms control and international security policy.*

***Linda Robinson** is a senior international policy analyst at the RAND Corporation. Her areas of expertise include national security strategy, international affairs, U.S. foreign policy, security force assistance, joint force development, special operations forces, irregular warfare, and stability operations.*
***Abby Doll** is a research assistant at the RAND Corporation and focuses on military capabilities assessment, scenario development, and escalation dynamics. She is currently pursuing a PhD in war studies from King's College, London.*


CBRNE-Terrorism Newsletter
W
O
M
D
2005
2014
10
Years
of
CBRNE-Terrorism Newsletter
explosives
cyber
RDD
CWAs
BWAs
WE have to be lucky all the time. THEY have to be lucky only once!