October 2014

CBRNE NEWSLETTERRORISM

E-Journal for CBRNE & CT First Responders

10 years

www.cbrne-terrorism-newsletter.com

Turkey denies nuclear weapons plans

Source: http://www.dailysabah.com/politics/2014/09/25/turkey-denies-nuclear-weapons-plans

September 25 – Turkey has denied media claims that it is planning to develop nuclear weapons.
Following allegations in German newspaper Die Welt (red more at August 2014 issue) that Turkey is seeking to acquire enriched uranium, the Turkish Foreign Ministry spokesman Tanju Bilgiç said in a statement on Thursday: "The claims published in Die Welt on September 21 have nothing to do with the truth.

"Turkey attaches great importance to issues of arms control and disarmament and is a party to all relevant international treaties and conventions including, in particular, the treaty on non-proliferation of nuclear weapons. It is also an active participant in international efforts in these areas."
He added that Turkey strongly adhered to the peaceful use of nuclear energy within the framework of the treaty.
Due to Turkey's proximity to "regions posing high risks of proliferation of weapons of mass destruction" it has prioritized turning the Middle East into a "WMD-free zone," the statement added, calling for a conference on establishing the zone "at the earliest."
On Wednesday, Turkish Energy Minister Taner Yıldız said Turkey did not have the intention or technology, such as a nuclear research reactor or a uranium enrichment program, for nuclear weapons production.

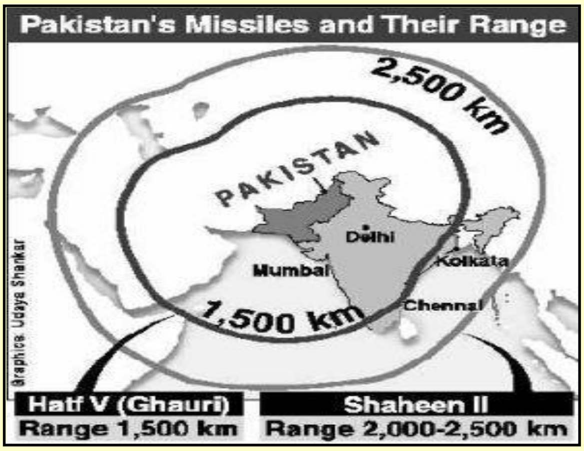
Pakistan is building smaller nukes, but they just might be more dangerous

Source: http://timesofindia.indiatimes.com/world/pakistan/Pakistan-is-building-smaller-nukes-but-they-just-might-be-more-dangerous/articleshow/43573197.cms

Pakistan is likely working to create tactical nuclear weapons, which are smaller warheads built for use on battlefields rather than cities or infrastructure. These weapons are diminutive enough to be launched from warships or submarines, which makes them easier to use on short notice than traditional nuclear weapons.

Pakistan test-fires short range missile Hatf IX

Developing tactical nuclear weapons calls for miniaturization of current weaponry (the "Davy Crockett," developed by the US in the '50s, was designed to launch from a simple tripod). But as The Washington Post reports, analysts are divided on whether Pakistan will be able to make warheads tiny enough for sea-launching.
There's less uncertainty about the military advantage gained with such weapons. A warhead-toting navy would allow Pakistan to stay



nuclear-capable regardless of what happens to its homeland, where its nuclear infrastructure is spread out.

The trade-off there, for both Pakistan and the world, is that nuclear missiles become more likely to fall into rogue hands, whether those of a maverick military commander or extremist groups. At a land-based facility, a hijacker would need "to commandeer two separate facilities, with two separate security procedures and local commanders," Jonah Blank, a political scientist with the RAND Corporation, wrote in an email to Business Insider. "For a sea-based nuclear device, a rogue operator would need only to commandeer one asset: A submarine or surface vessel." Other safeguards exist - US submarines, for instance, require complex codes before permitting a nuclear offensive - but faster access still simplifies one factor in a high-stake equation.

Pakistan's Hatf-V is a medium-range ballistic missile, capable of reaching targets in India.

Historically, deterrence and the stability it brings is often the salutary result of rivals with equal nuclear capability. It's also Pakistan's stated goal. Last September a statement from a meeting of the National Command Authority (which directs nuclear policy and development) said Pakistan is developing "a full-spectrum deterrence capability to deter all forms of aggression." The meeting was presided by Pakistani Prime Minister Nawaz Sharif.

"India has what's called the triad, the ability to launch nuclear weapons form air, land, and now soon by sea. Pakistan is looking for the same," Arif Rafiq, a researcher at the Middle East Institute, told Business Insider. He believes nuclear parity between the countries has achieved deterrence. "Since India and Pakistan tested nuclear weapons in 1998, there has been a greater level of restraint in terms of the behavior of both countries when it comes to war," Rafiq said. "They've advanced their nuclear arsenal but they've also taken significant steps towards normalizing relations." While nuclear weapons can be beneficial, Rafiq doesn't exactly applaud them: "Having one nuclear warhead is something that's terrible enough for this world," he said.

Transparent nanoscintillators for radiation detection

Source: http://www.homelandsecuritynewswire.com/dr20141003-transparent-nanoscintillators-for-radiation-detection-in-homeland-security-medical-safety

A University of Texas at Arlington research team says recently identified radiation detection properties of a light-emitting nanostructure built in their lab could open doors for homeland security and medical advances.

In a paper to be published in the 1 October issue of *Optics Letters*, UT Arlington Physics Professor Wei Chen and his co-authors describe a new method to fabricate transparent nanoscintillators by heating nanoparticles composed of lanthanum, yttrium and oxygen until a transparent ceramic is formed. A scintillator refers to a material that glows in response to radiation.

A UT Arlington release reports that the new structure is known as $La_{0.2}Y_{1.8}O_3$.

The researchers say the resulting “nanostructured polycrystalline scintillators” have better energy resolution than currently used materials sodium iodide and caesium iodide and the new scintillator is more stable than sodium iodide. It also has a fast luminescence decay time that is essential for radiation detection because it affects how quickly a detector can work, Chen said.

“Many people use this compound as a host material for lasers or other optical operations, but no one had ever tried this for radiation detection as far as we know,” Chen said. “We used a new way to make these materials and found that they hold a lot of promise as a new direction for luminescent scintillator research.”

Chen is head of UT Arlington’s Security Advances Via Applied Nanotechnology Center, or SAVANT Center. In 2010, he became principal investigator on a $1.3 million grant from the National Science Foundation and the U.S. Department of Homeland Security, with the goal of looking for a new type of radiation detector that could help reduce the threat of nuclear materials being brought into the U.S. for terrorism.

Andrew Brandt, a physics professor and co-director of the SAVANT Center, is co-principal investigator on the grant funding and a co-author of the new paper. He said the team is still working to evaluate the new nanomaterials for practical applications and to understand their physics, “but we’re very excited about the possibilities this discovery brings with it.”

Brandt noted grant funding and the subsequent research stemmed from an interdisciplinary partnership that teamed his expertise in detector and scintillator technology with Chen’s knowledge of nanoparticle behavior. “This trans-disciplinary type of research spawned the SAVANT Center, and is in concert with the vision UT Arlington administrators have for the future,” he said.

Scientists know that nanoparticles hold promise as a new type of scintillator, but the current method of embedding them into a clear polymer or glass faces the challenge of losing transparency because of a process called aggregation. The UT Arlington work, which involves the synthesis of nanoparticles using wet chemistry and heating them at temperatures much lower than their melting point, avoids the problem of aggregation to maintain their transparency.

Kenarangui said the team tried several samples at the Radiation Measurement and Application Laboratory and the $La_{0.2}Y_{1.8}O_3$ had the best potential of any they examined.

Weiss said the team’s work is a breakthrough. “They’ve developed a way to take these nanoparticles and process them in such away that you can make a practical device,” he said.

The new material is made from two of the least expensive rare earth elements, so it is cost-effective, Chen said. He estimates producing a $La_{0.2}Y_{1.8}O_3$ scintillator would cost a little over $7 per cm^3.

In lab tests, the $La_{0.2}Y_{1.8}O_3$ also proved to have better energy resolution than currently used materials sodium iodide and caesium iodide. **That resolution is what allows the scintillator to pinpoint the energy of a radiation source, which can be like a signature for investigators.**

“If we see a radiation material, we want to know where it came from and those energies can tell us that,” Chen said.

▶ **Read the full paper at:** http://www.opticsinfobase.org/ol/fulltext.cfm?uri=ol-39-19-5705&id=301749

— Read more in Wei Chen et al., “Luminescence of $La_{0.2}Y_{1.8}O_3$ nanostructured scintillators,” Optics Letters *39, no. 19 (1 October 2014): 5705-8*

Islamic State is hatching plan to gain Iranian nuclear secrets

Source: http://www.jpost.com/Middle-East/Report-Islamic-State-is-hatching-plan-to-gain-Iranian-nuclear-secrets-378050

The jihadist organization IS plans to pay off Russia, seized document states, exchanging its control of Anbar province's vast gas fields for information on Iran's nuclear program.

The British newspaper *The Sunday Times* reported on Sunday morning that Islamic State is calling on its members to brace for war with Iran in order to take over its nuclear secrets. The newspaper cited a document believed to have been written by top Islamic State member Abdullah Ahmed al-Meshedani, a member of the group's highly secretive six-man war cabinet.

According to the *Times*' report, the so-called manifesto was uncovered when Iraqi forces raided a home of a senior official of the jihadist group.

The document is allegedly being looked into by western security personnel, who have so far deemed it authentic, according to the newspaper.

The jihadist organization plans to pay off Russia, the document states, exchanging its control of Anbar province's vast gas fields for information on Iran's nuclear program.

The commander behind the manifesto also wants Russia to denounce its support for Iran and Syrian President Bashar Assad.

The *Times* story is not the first report of the Islamic State's desire to obtain non-conventional weapons

In August, *Foreign Policy* reported that Islamic State was also trying to develop **biological weapons**. The report cited information found on a **laptop** computer seized from an IS operative.

Foreign Policy obtained the computer from a moderate Syrian rebel group who seized the laptop in the Idlib province from an Islamic State hideout whose fighters had fled.

The laptop, belonging to a Tunisian operative of the Islamic State, named Muhammed S., with a background in chemistry and physics, included a 19-page document on developing biological weapons and weaponizing the bubonic plague.

"The advantage of biological weapons is that they do not cost a lot of money, while the human casualties can be huge," the document says in Arabic, according to Foreign Policy.

Among the files on the seized computer is also a ruling from a Saudi cleric justifying the use of weapons of mass destruction. **"If Muslims cannot defeat the unbelievers in a different way, it is permissible to use weapons of mass destruction...Even if it kills all of them and wipes them and their descendants off the face of the Earth."**

Belgium – Jihad fighter previously worked at Doel nuclear plant

Source: http://www.flanderstoday.eu/current-affairs/jihad-fighter-previously-worked-doel-nuclear-plant

Ilyaas Boughalab, currently in Syria but on trial in his absence in Antwerp, worked in the part of the **Doel nuclear power plant** (photo) where sabotage occurred last summer

Ilyass Boughalab, 26, worked as a technician with the subcontractor Vincotte. The company carries out inspections of repairs at the plant and delivers safety certificates. **Boughalab's task, until he left the company in November of 2012, was to inspect the quality and safety of welding work, which gave him access to the most secure part of the installation.**

That is where an incident took place last August that forced the closure of the plant until the end of the year. The incident is being investigated as possible sabotage.

Boughalab is part of the trial against Sharia4Belgium in Antwerp in his absence; he is still in Syria. He is one of more than 40 people charged with being a member of a terrorist organisation.

Electrabel, which owns the nuclear power plant, carries out security screenings of personnel allowed access to sensitive areas of nuclear plants, VTM reported. Boughalab was screened once during the three years he worked at Doel.

"If we had known the man had become radicalised, we would have reacted immediately," said an Electrabel spokesperson. According to nuclear inspection agency Fanc, Boughalab would have been subject to checks each time he entered and left the technical zone, regardless of his clearance.

There is at present no evidence to link Boughalab to the incident in August, when he was not working at the plant or even in the country. However, the security services will now be looking **more closely** at possible connections he had during his time at Doel.

EDITOR'S COMMENT: No comment! – apart from my favorite Einstein's quota on stupidity…

Electrabel confirms Doel 4 nuclear power plant sabotage

15/08/2014

Source: http://www.powerengineeringint.com/articles/2014/08/electrabel-confirms-doel-4-nuclear-power-plant-sabotage.html

Belgium has been left without half of its nuclear capacity, as GDF Suez subsidiary Electrabel confirmed that its Doel 4 nuclear reactor has been shut down due to sabotage.

Reuters reports that a GDF Suez spokesman confirmed Belgian press reports about suspicion of sabotage. "There was an intentional manipulation," he said, adding that somebody had tampered with the system used for emptying oil from the Alstom-made turbine at the nuclear power plant.

He said no outsiders had penetrated into the plant but declined to say whether an employee could have purposely caused the leak, as has been reported in some Belgian media. He said Electrabel had filed a complaint and that the Belgian police had started an investigation.

Repairs being carried out on the major damage inflicted on a steam turbine, which caused an oil leak at the site, means it most likely won't be reactivated until the end of the year; a situation that could lead to Electrabel losing 40 million euros a month on net recurring income.

The firm says the main damage is to the turbine's high pressure section.

The closure of Doel 4 takes place after two other reactors – Doel 3 and Tihange 2 – were forced offline because of fractures in steel casings housing their respective reactors. The closure of all three takes 3 GW off the Belgian grid, more than half its total nuclear capacity.

The implications of all that is that the Belgian government may have to consider boosting its interconnection capacity with neighbouring countries over the winter in order to prevent a potential blackout.

The problems found at Doel 3 have dogged the company in recent years.

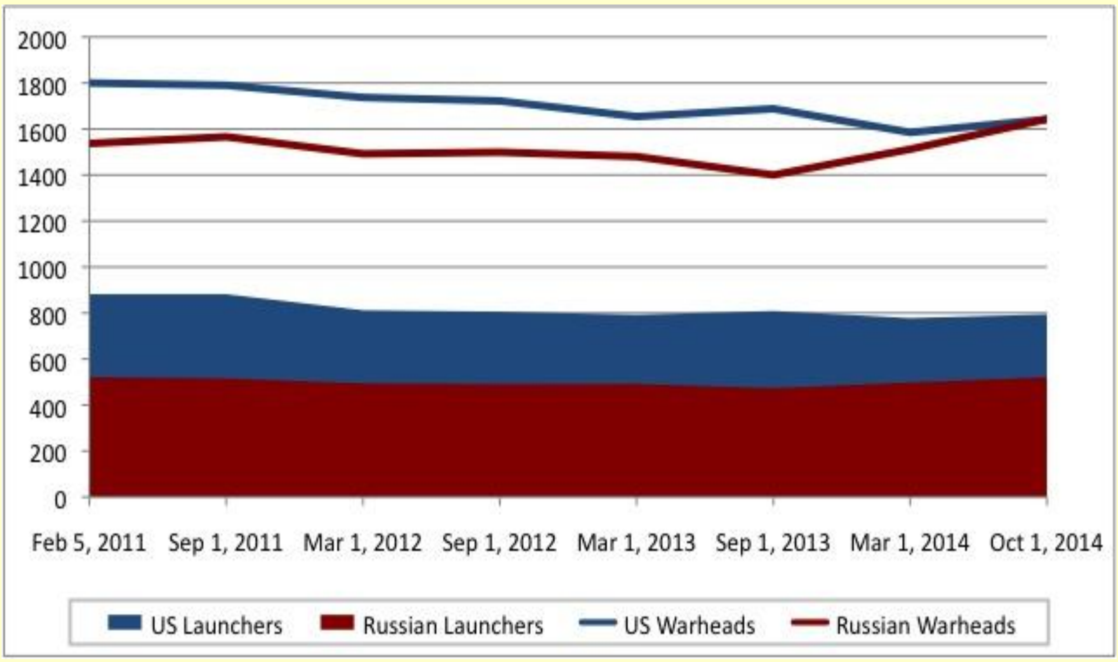
The Federal Agency for Nuclear Control (FANC) told Power Engineering International that Doel 3 is in the process of being assessed, particularly with regard to the vessel structure housing the reactor. The results will be of interest to other nuclear managements whose plants were developed by the same construction outfit.

FANC spokesperson Sebastien Berger told PEi, "Electrabel is still carrying out the test program at the Belgian Nuclear Research Center (SCK•CEN) in Mol. This program of

mechanical tests and metallurgical assessments will run until autumn. At the end of the program, a justification file should be submitted to the FANC which will decide on the restart of both reactors."
"About the possible implication for other reactors around Europe, the FANC regularly takes contact with its counterparts to inform them about the situation in Belgium. It's up to them to communicate on their own situation and the tests they are carrying out," he added.

New START: Russia and the United States Increase Deployed Nuclear Arsenals

By Hans M. Kristensen
Source: http://fas.org/blogs/security/2014/10/newstart2014/



Three and a half years after the New START Treaty entered into force in February 2011, many would probably expect that the United States and Russia had decisively reduced their deployed strategic nuclear weapons.

On the contrary, the latest aggregate treaty data shows that the two nuclear superpowers both *increased* their deployed nuclear forces compared with March 2014 when the previous count was made. Russia has increased its deployed weapons the most: by 131 warheads on 23 additional launchers. Russia, who went *below* the treaty limit of 1,550 deployed strategic warheads in 2013, is now back *above* the limit by 93 warheads. And Russia is now counted – get this – as *having more strategic warheads deployed than when the treaty first went into force in February 2011!*

Before arms control opponents in Congress get their banners out, however, it is important to remind that these changes do not reflect a build-up the Russian nuclear arsenal. The increase results from the deployment of new missiles and fluctuations caused by existing launchers moving in and out of overhaul. Hundreds of Russian missiles will be retired over the next decade. The size of the Russian arsenals will most likely continue to decrease over the next decade.

Nonetheless, the data is disappointing for both nuclear superpowers – almost embarrassing – because it shows that neither has made substantial reductions in its deployed nuclear arsenal since the New START Treaty entered into force in 2011.

The meager performance is risky in the run-up to the nuclear Non-Proliferation Treaty review conference in April 2015 where the United States and Russia – together with China, Britain, and France – must demonstrate their progress toward nuclear disarmament to ensure the support of the other countries that have signed the NPT in strengthening the non-proliferation treaty regime.

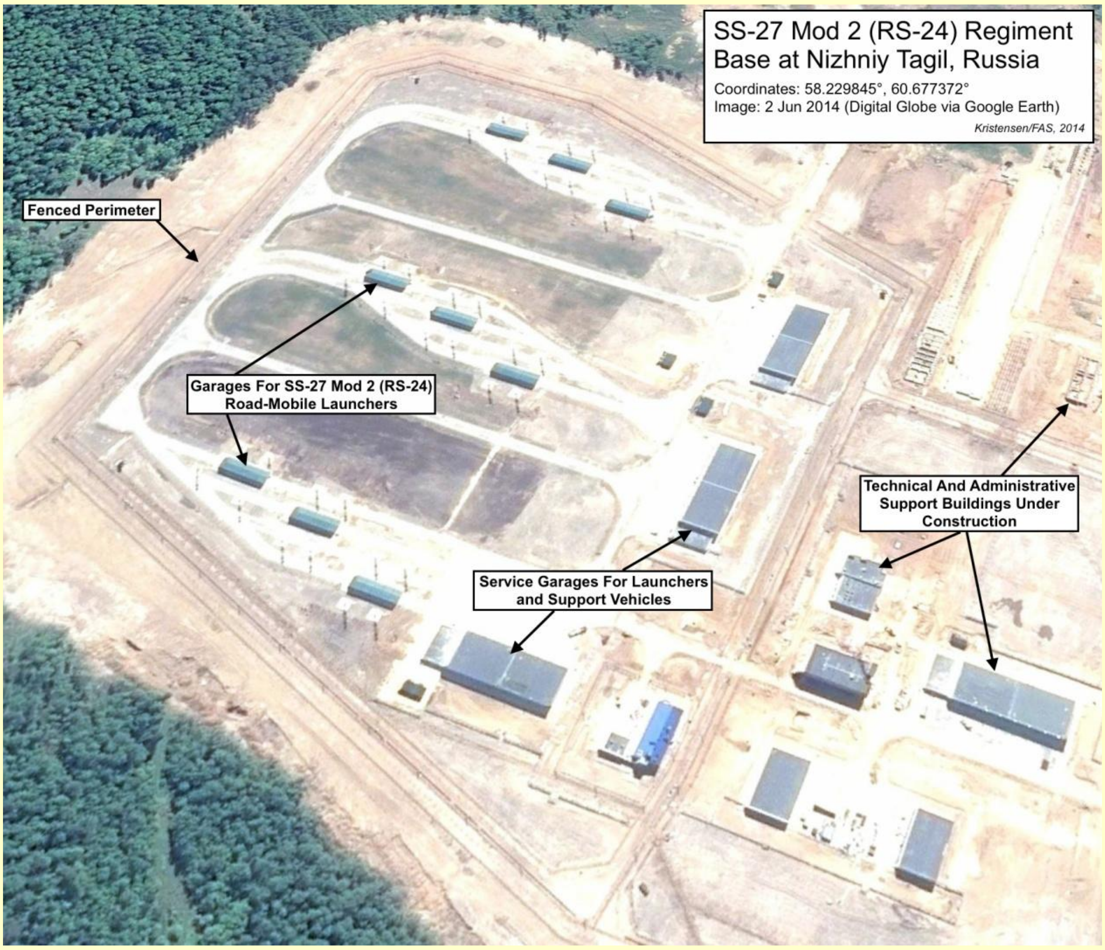
Russian Deployments

The data for Russia is particularly interesting because it now has 106 warheads *more* deployed than when the New START Treaty went into force in February 2011. The number of deployed launchers is exactly the same: 106.

This does not mean that Russia is in the middle of a nuclear arms *build-up*; over the next decade more than 240 old Soviet-era land- and sea-based missiles are scheduled to be withdrawn from service. But the rate at which the older missiles are withdrawn has been slowing down recently from about 50 missiles per year before the New START treaty to about 22 missiles per year after New START. The Russian military wants to retire all the old missiles by the early 2020s, so the current rate will need to pick up a little.

At the same time, the rate of introduction of new land-based missiles to replace the old ones has increased from approximately 9 missiles per year to about 18. The net effect is that the total missile force and warheads deployed on it have increased slightly since 2013.

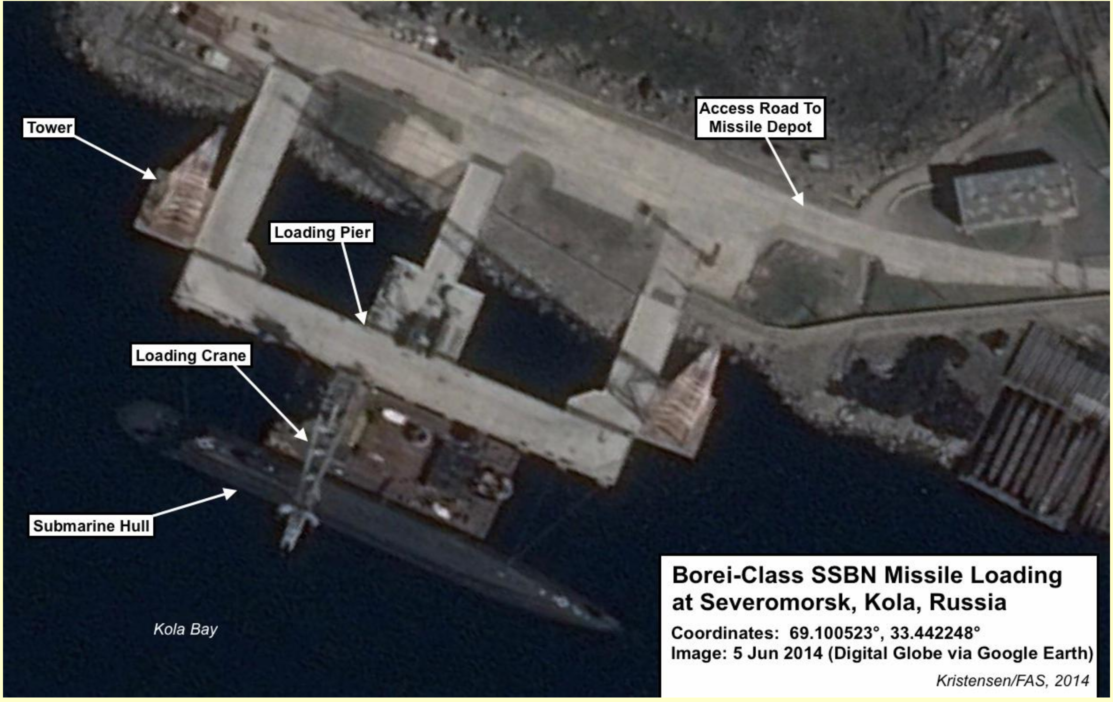
The new deployments include the SS-27 Mod 2 (RS-24) ICBM, of which the first two regiments with 18 mobile missiles were put in service with the Teykovo division in 2010-2012, replacing SS-25s (Topol) previously there. Deployment followed in late-2013 at the Novosibirsk and Nizhniy Tagil divisions, each of which now has one regiment for a total of 36 RS-24s. This number will grow to 54 missiles by the end of this year because the two divisions are scheduled to receive a second regiment. And because each RS-24 carries an estimated 4 warheads (compared with a single warhead on the SS-25), the number of deployed warheads has increased.


SS-27 Mod 2 (RS-24) Regiment Base at Nizhniy Tagil, Russia
Coordinates: 58.229845°, 60.677372°
Image: 2 Jun 2014 (Digital Globe via Google Earth)
Kristensen/FAS, 2014
Fenced Perimeter
Garages For SS-27 Mod 2 (RS-24) Road-Mobile Launchers
Technical And Administrative Support Buildings Under Construction
Service Garages For Launchers and Support Vehicles

Introduction of the SS-27 Mod (RS-24) road-mobile ICBM is underway at the 42nd Missile Division at Nizhniy Tagil in central Russia.

Also underway is the deployment of SS-27 Mod 2 (RS-24) in silos at the Kozelsk division, where they are replacing old SS-19s. The first regiment of 10 RS-24s was scheduled to become operational by the end of this year but appears to have fallen behind schedule with only 4 missiles expected. It has not been announced how many missiles are planned for Kozelsk but it might involve 6 regiments with a total of 60 missiles (a similar number of SS-27 Mod 1s (Topol-M) were installed at Tatishchevo between 1997 and 2013). Since each RS-24 carries 4 warheads compared with the 6 on the SS-19, the number of silo-based warheads will decrease over the next decade.

Another reason for the increase in the latest New START data is probably the long-awaited introduction of the new Borei-class of ballistic missile submarines. The precise loadout status of the first submarines is uncertain, but the first might have been partially or fully loaded by now. The first two boats (Yuri Dolgoruy and Alexander Nevsky) entered service in late-2013 but have been without missiles because of the troubled test-launch performance of their missile (SS-N-32, Bulava), which has failed about half of its test launched since 2005. After fixes were made, a successful launch took place on September 10 from the third Borei SSBN, the Vladimir Monomakh. The Yuri Dolgoruy is scheduled to conduct an operational launch later this month. A total of 8 Borei SSBNs are planned, each with 16 Bulavas, each with 6 warheads, for a total of nearly 100 warheads per boat.


Tower
Access Road To Missile Depot
Loading Pier
Loading Crane
Submarine Hull
Kola Bay
Borei-Class SSBN Missile Loading at Severomorsk, Kola, Russia
Coordinates: 69.100523°, 33.442248°
Image: 5 Jun 2014 (Digital Globe via Google Earth)
Kristensen/FAS, 2014

A new Borei-class SSBN at missile loading pier by the Okolnaya SLBM Deport at Severomorsk on the Kola Peninsula.

United States

For the United States, the data shows that the number of warheads deployed on strategic missiles increased slightly since March, by 57 warheads from 1,585 to 1,642. The number of deployed launchers also increased, by 16 from 778 to 794.

The reason for the U.S. increase is not an actual increase of the nuclear arsenal but reflects fluctuations caused by the number of launchers in overhaul at any given time. The biggest effect is caused by SSBNs loading or offloading missiles, most importantly the return to service of the USS West Virginia (SSBN-736) after a refueling overhaul with a load of 24 missiles and approximately 100 warheads.

More details will be come available in December when the State Department is expected to release the detailed unclassified breakdown of the U.S. aggregate data for October.

Overall, however, the U.S. performance under the treaty is better than that of Russia because the data shows that the United States has actually *reduced* its deployed force structure since 2011: by 158 warheads and 88 launchers. In addition, the U.S. military has also destroyed 124 non-deployed launchers including empty silos and retired bombers.

The better U.S. performance does not indicate that the Pentagon has embarked upon a program of unilateral disarmament. Rather, it reflects that the U.S. nuclear forces structure is much larger than that of Russia and that the U.S. therefore has more work to do before the treaty enters into effect in February 2018.

Conclusions and Recommendations

The increase in Russian and U.S. deployed strategic nuclear weapons shown by New START aggregate data is disappointing because it illustrates the degree to which the two nuclear superpowers are holding on to excessively large nuclear arsenals. While there is no doubt that the two countries will eventually implement the treaty by 2018, they have been exceedingly slow in doing so.

The fact that Russia now has *more* warheads deployed than when the treaty first entered into force in 2011 is particularly disappointing. And it illustrates just how modest the New START Treaty is.

The increase in U.S. deployed warheads and launchers is also disappointing especially when considering that the Nuclear Employment Strategy issued by the White House in June 2013 concluded that the United States has one-third more strategic nuclear weapons deployed than it needs to fulfill its national and international security commitments.

The United States currently has 273 deployed strategic launchers *more* than Russia, as well as a reserve of several thousand non-deployed warheads that are not counted by the treaty but intended to increase the loadout on the launchers if necessary.

Faced with the planned retirement of Soviet-era missiles within the next decade, Russia appears to be compensating for the disparity by accelerating deployment of new land-based missiles with multiple warheads to maintain parity with the larger U.S. missile force structure.

Russia and the United States each has over four times more nuclear weapons than all the seven other nuclear-armed states in the world – combined! Clearly, the large Russian and U.S. arsenals exist in a bubble justified predominantly by the large size of the other's arsenal.

Russia and the United States need to do more to reduce their nuclear arsenals faster. The lackluster performance in implementing and following up on the New START Treaty, as well as the extensive nuclear weapons modernization underway in both countries, mean that the two nuclear superpowers will have very little to show at next year's nuclear Non-Proliferation Treaty review conference in New York to demonstrate how they are meeting their obligations and promises made under the treaty to reduce and eventually eliminate nuclear weapons.

Neither Russia nor the United States can afford the expensive nuclear weapon modernization programs currently underway to sustain their large arsenals. And they certainly cannot afford to weaken the support of the non-proliferation treaty regime in strengthening efforts to halt and curtail the proliferation of nuclear weapons.

***Hans M. Kristensen** is the director of the Nuclear Information Project at the Federation of American Scientists where he provides the public with analysis and background information about the status of nuclear forces and the role of nuclear weapons.*

Iranian Sources Deny Explosion at Parchin

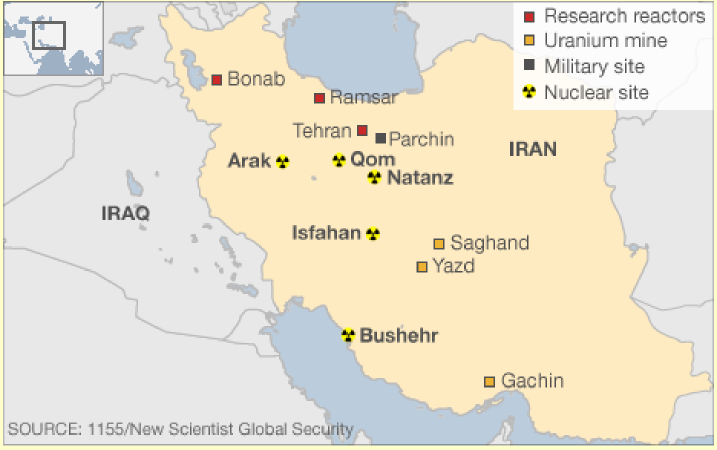
Source: http://www.israelnationalnews.com/News/News.aspx/185882#.VDON-haPwxA

October 06 – **An explosion at Iran's Parchin nuclear plant has killed at least two people, among them an unnamed "nuclear expert", according to Iranian media reports.**

Reports on the explosion that took place in or near the Parchin nuclear plant outside Tehran may have been due to a technical issue, a report said. The report said that two people had died, although that could not be confirmed. The Iranian government has made no statement on the matter, and nearly all reports in the incident are based on reports from sites outside of Iran, most of them run by anti-government groups outside the country.

In the first official comment on the incident, official Iranian sources said that there had been an "incident," but not an explosion, at the Parchin plant. Two people are classified as "missing." The sources added that there was no nuclear work being done at Parchin.

The semi-official *Isna* news agency claimed the explosion took place at around 10:00 a.m. after a fire erupted in an "explosive materials production unit".



SOURCE: 1155/New Scientist Global Security

"Unfortunately, due to the incident, two workers of this production unit lost their lives," the site reported. Other Iranian outlets cited witnesses who said a "loud explosion" could be heard several kilometers away.

The opposition *Sahamnews* outlet claimed the blast was so powerful it shattered windows some 15 kilometers away from the site, raising the possibility that a far more destructive explosion had taken place than official outlets are letting on.

Aerial view of Parchin site (Reuters)

Iran has refused to allow International Atomic Energy Agency (IAEA) inspectors to access Parchin since 2005, and both opposition figures and others have accused the regime of using the site to house an illegal nuclear weapons program.

Last month, Israel's Internal Security Minister Yuval Steinitz said he had "reliable information" that Parchin was being used for secret tests of technology that could be used only for detonating a nuclear weapon.

The latest development comes as talks between Iran and world powers remain deadlocked over Iran's illegal nuclear program, as a November 24 deadline for a permanent deal.

Retired senior German defense ministry official: "Turkey is on its way to have its own nuclear bomb"

Source: http://i-hls.com/2014/10/senior-german-defense-ministry-official-turkey-way-nuclear-bomb/

The German intelligence services have credible information according to which "Turkey is headed towards its own nuclear bomb". This is revealed in an interview former senior German defense ministry official Hans Rühle gave to the important German-speaking weekly *Die Welt*. Rühle, who served in the ministry between 1982 and 1988 in a high-ranking position, claims "we have reliable information that Erdogan's nuclear ambitions are real, and that while the world is endlessly talking about Iran's and North Korea's nuclear programs, we might be witnessing the nuclear experiment in the Middle East which will be carried out by Turkey rather than by Iran."

Rühle further reveals, that German intelligence passed the information on “to our friends in the West, who, surprisingly, had a great deal of intelligence material on this issue.” According to Rühle, the

Turks are definitely busy secretly developing nuclear arms under the guise of a civilian nuclear program. In 2011, Turkey concluded a deal with Russia to build a nuclear power plant 300 kilometers from Anatolia, at a cost of 15 billion Euro. The technological information required to produce nuclear arms came from Pakistan, and the planned Turkish bomb is identical to the Pakistani one.

In the course of his interview, Rühle explained that for the time being, work on the plant had ceased due to Turkey’s demand to take an active part in the building works and to have control over the materials used in the plant. Turkey refuses to part with plutonium, which, after being enriched to a level of 90%, can be sued as a fissile material. According to the information German intelligence has, Erdogan ordered, as early as 2010, to establish secret installations, some of which are subterranean, on Turkish soil. Also in 2010, Pakistan sent Turkey numerous centrifuges.

In tandem with its nuclear program, Turkey is also busy developing long-range missiles. During the interview, Rühle explained that in 2012, Turkey conducted an experiment on a 1500 km range missile. Another experiment is planned for 2015, to test a 2500 km range missile. According to Rühle, the Turkish missiles are quite inaccurate, and their payload is low compared with similar missiles as well as with nuclear warheads. Nevertheless, “the missiles’ payload is enough to carry a compact nuclear warhead.”

Following the publication in *Die Welt*, intelligence experts in the West claim that should Turkey ultimately acquire nuclear arms, then this could mark the start of a nuclear arms race, and eventually, all or most Middle Eastern countries will have either developed nuclear arms or acquired them, rendering the region riddled with nuclear countries.

HAZMAT threat in Kazakhstan

Source: http://hisz.rsoe.hu/alertmap/site/index.php?pageid=event_desc&edis_id=HZ-20140902-45119-KA

Kazakh authorities are searching for a canister of radioactive cesium 137 that has gone missing in the western part of the Central Asian nation. Local authorities in the western Manghystau region (red in map) said on September 2 that a metal cylinder containing the substance had been lost in the region on August 27 **while being transported by car**. They have warned residents not to open the container if it is found because it could be deadly. Cesium 137 is a radioactive isotope used in the nuclear industry and in medicine. It can sharply raise the level of radioactivity in an area it contaminates. Kazakhstan's National Security Committee (KNB) has joined the investigation and search for the container.

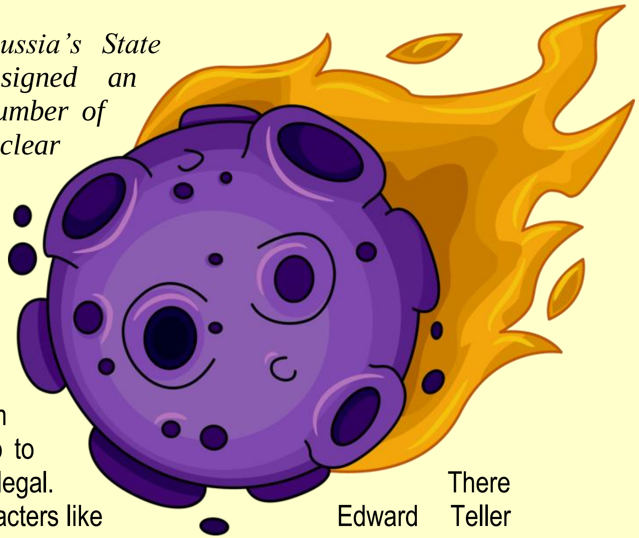
Astroid Defense Isn't A Good Enough Reason To Keep Nuclear Weapons Around

Source: http://www.businessinsider.com/should-we-nuke-asteroids-2014-10

Though designated as in excess of national defense needs by the National Nuclear Security Administration, parts of certain nuclear warheads containing uranium have been granted a reprieve from disassembly "pending a senior-level government evaluation of their use in planetary defense against earthbound asteroids."

In *Foreign Policy*, Jeffrey Lewis elaborates.

The US Department of Energy (DOE) and Russia's State Atomic Energy Organization (ROSATOM) signed an agreement that provides for cooperation in a number of areas, including safeguards against nuclear proliferation, nuclear reactors, and defense from asteroids … It's not entirely clear to me what there is to talk about with ROSATOM beyond how we absolutely, positively cannot do any of the things they are discussing.



If, Lewis writes "some labbie wants to simulate a megaton-sized nuclear explosion against an asteroid, I suppose that's fine with me. But a cooperative program of work with ROSATOM seems like a permission slip to start planning things that are neither a good idea nor legal. There is a long and disreputable history of Strangelovian characters like Edward Teller and Lowell Wood using 'planetary defense' as a justification for one nuclear weapons scheme or another, long after the demise of what little Cold War rationale might have existed. … In other words, a mess of legal obligations stand between us and detonating a nuclear weapon in outer space."

Such as:

- ✓ The Outer Space Treaty [which] prohibits placing "any objects carrying nuclear weapons or any other kinds of weapons of mass destruction" in orbit, on celestial bodies, or "in outer space in any other manner" — to say nothing of blowing them up.
- ✓ The Limited Test Ban Treaty [which] prohibits nuclear explosions anywhere except underground. That means no explosions in the atmosphere or "beyond its limits, including outer space."
- ✓ The Threshold Test Ban Treaty [which] limits the size of underground nuclear explosions but also has a companion agreement on "peaceful" nuclear explosions that makes clear any such explosions must be underground.

"Waste not, want not" is a useful adage — for everything but nuclear weapons (lest they waste us all).

But if nukes must remain in existence, at least for the time being, would that defense against asteroids be their only intended use. Oh, and defense against an extraterrestrial attack. As Ronald Reagan said: "I occasionally think how quickly our differences worldwide would vanish if we were facing an alien threat from outside this world."

And on another occasion: "in our obsession with antagonisms of the moment, we often forget how much unites all the members of humanity. Perhaps we need some outside, universal threat to make us recognize this common bond."

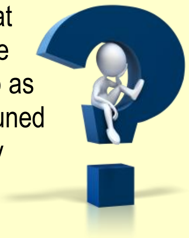
In fact, that universal threat which could unite us already exists: nuclear weapons.

Tactical nuclear weapons – used in Syria?

Source: http://i-hls.com/2014/10/tactical-nuclear-weapons-used-syria/

October 17 – **Two explosions rising into the skies just like 'nuclear mushrooms', about a year ago above Homs and Qasyoon, raised a wave of rumors these were the product of a strike using tactical nuclear weapons launched from the air.** In order to get to the bottom of this and see if there is any truth to it, and whether the 'nuclear genie' did get out of the bottle in the Middle East, *Veterans Today* sent Jon Snow to interview nuclear arms specialists and hear what they had to say.

The most meaningful and surprising statement came from Greg Thielmann, an expert on nuclear arms control, who said **"what we see in both cases, in the real-time videos, are tactical nuclear blasts carried out using aircraft-launched cruise missiles. The aircraft came from either close to the border with Syria or from the direction of the Mediterranean. It is very likely the perpetrator in both cases is Israel – the only nation capable of using such weapons without fear of retaliation."**



Thielmann further explained that "tactical nuclear weapons lower the threshold on use of a nuclear bomb as their modern incarnation can be tuned in yield in order to target military sites using stand-off weapons without escalating by destroy surrounding civilian infrastructure." He went on to say**, "Keep in mind a nuclear bomb sounds like a huge device, but its can be carried by F-15s."**

Another strategist who was interviewed and asked to remain anonymous, made another argument: "we are not on the verge of an age when the world is beginning to play with 'nuclear fire' or with other means of mass destruction. One example is the chemical weapon Syria still holds. All this poses a real danger, so the application of tactical nuclear weapons could be much more useful than big bombs that could bring about a nuclear holocaust."

The expert went on to say that despite this, it cannot be completely ruled out that the explosions were indeed the result of an airstrike whose origin was out of Syria, "but in this case, it would have been an explosion of some major depot for fuel storage or a major arms depository."

Veterans Today was unable to come with an unequivocal solution to the mystery they set out to crack wide open, so they ran the story with a question mark in the headline. **Nevertheless, one question remains unanswered: why was the story pulled shortly after it aired?**

Emergency Agencies Practice Response To Nuclear Explosion In Times Square

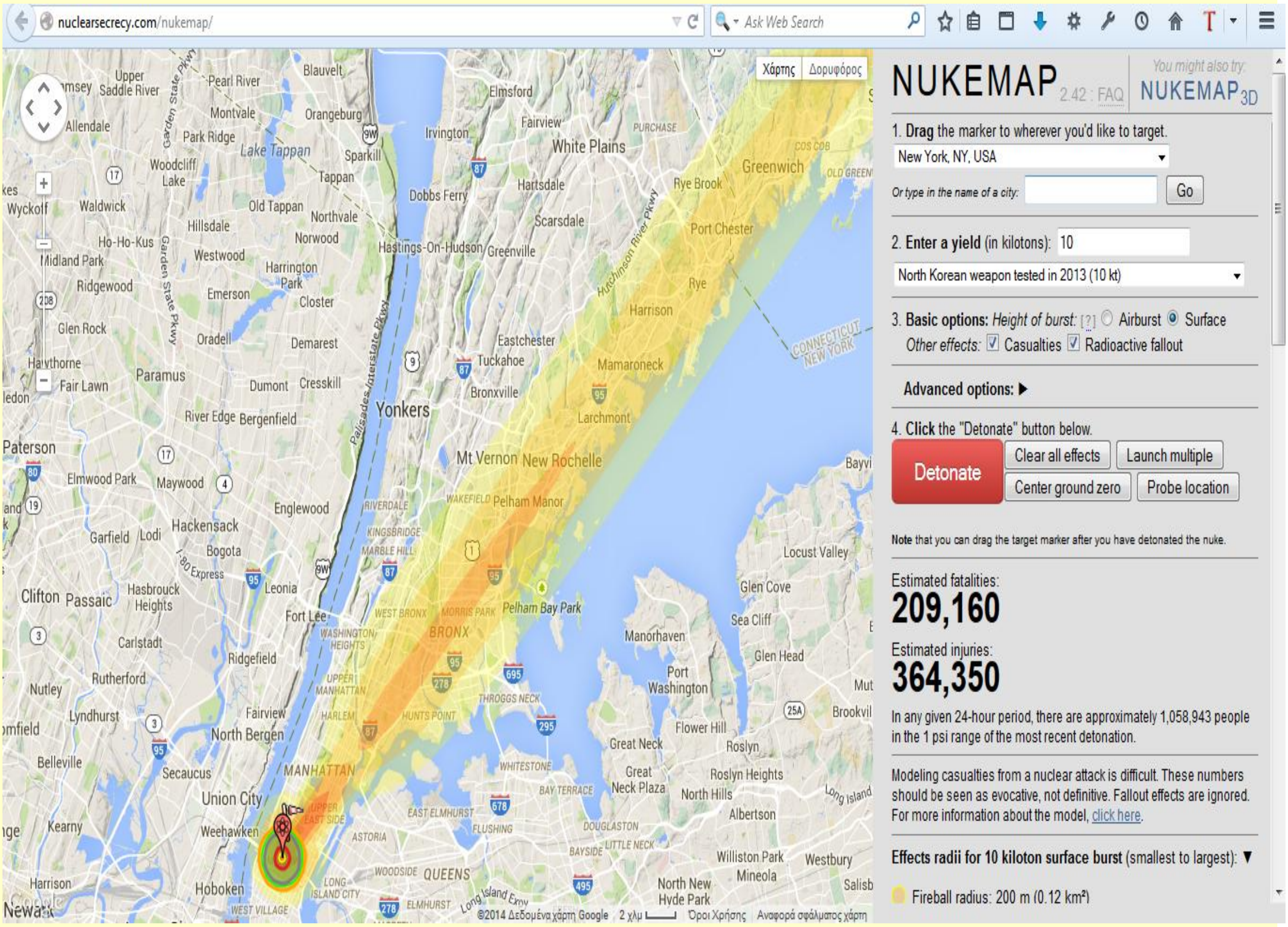
Source: http://newyork.cbslocal.com/2014/10/22/emergency-agencies-practice-response-to-nuclear-explosion-in-times-square/

October 22 – The New York City region's emergency agencies are practicing for a disaster.

The city's Office of Emergency Management ran a training exercise Wednesday that simulated a response to **a 10-kiloton nuclear device** exploding at 42nd Street and Seventh Avenue in Times Square, WCBS 880's Rich Lamb reported.

According to the exercise, 100,000 people were instantly killed; a wave of overpressure took down buildings for a half-mile radius and did damage for up to two miles; and a radiation cloud swept over the region.

The drill's scenario also included a shutdown of subway service and interruptions to cellphone service.



1. Drag the marker to wherever you'd like to target.

New York, NY, USA ▾

Or type in the name of a city:

2. Enter a yield (in kilotons): 10

North Korean weapon tested in 2013 (10 kt) ▾

3. Basic options: Height of burst: [?] ○ Airburst ● Surface

Other effects: ☑ Casualties ☑ Radioactive fallout

Advanced options: ▶

4. Click the "Detonate" button below.

Note that you can drag the target marker after you have detonated the nuke.

Estimated fatalities:
209,160

Estimated injuries:
364,350

In any given 24-hour period, there are approximately 1,058,943 people in the 1 psi range of the most recent detonation.

Modeling casualties from a nuclear attack is difficult. These numbers should be seen as evocative, not definitive. Fallout effects are ignored. For more information about the model, click here.

Effects radii for 10 kiloton surface burst (smallest to largest): ▼

Fireball radius: 200 m (0.12 km²)

The city agency practiced rehearsing communications with the federal government and local law enforcement agencies in the Tri-State area.

"We would have to get that message to speak with one voice, with our partners in Connecticut, in Jersey, in the state of New York," OEM Commissioner Joe Esposito said.

The agency also rehearsed how it would get word to the public during the crisis.

Esposito said the blast would produce an electromagnetic pulse, disrupting much of communications, Lamb reported.

"What's the message? **Shelter in place, evacuate, and seek medical aid.** How would we do that? Social media, if it's up and running. We know a lot of this is going to be down for a time period, so we know that a big part of it would be radios," Esposito said. "The best thing would be portable radios."

Officials stressed that while not everything can be predicted in a disaster, the training exercises are vital practice.

▶ **Simulate more at:** http://nuclearsecrecy.com/nukemap/

Homemade bomb blast kills man in Chile

Source: http://www.cbsnews.com/news/homemade-bomb-blast-kills-man-in-chile/

Police forensics inspect an area where a bomb exploded in a residential neighborhood in downtown Santiago, Chile, Thursday, Sept. 25, 2014. The homemade bomb killed a man, officials said, adding to a string of blasts in Chile's capital. (AP Photo/Luis Hidalgo) AP

September 25 – The fiery explosion of a homemade bomb killed a man in downtown Santiago on Thursday, officials said, adding to a string of blasts in Chile's capital.

Prosecutor Claudio Orellana initially said **the man was handling the bomb when it exploded about 1 a.m., but he later opened the possibility that the man was a bystander.** Witnesses posted online photos of the man in flames before he was taken to an emergency clinic where he died.

Doctors at the clinic said the man, identified as Sergio Guillermo Landskron Silva, had grave injuries as well as burns. The coroner's office said he was 29.

The dead man's brother, Bastian Landskron, expressed doubts that his sibling was involved in planting a bomb, saying he was a drug addict who didn't live with the family and had no friends. Prison records show Sergio Landskron had completed a five-year sentence for theft and been free since June.

Officials say anarchist cells have planted some 200 bombs around Santiago over the past decade, including 30 so far this year.

The only other fatality was also a man believed to be planting an explosive.

President Michelle Bachelet on Thursday described the bombings as "terrorist acts, but isolated."

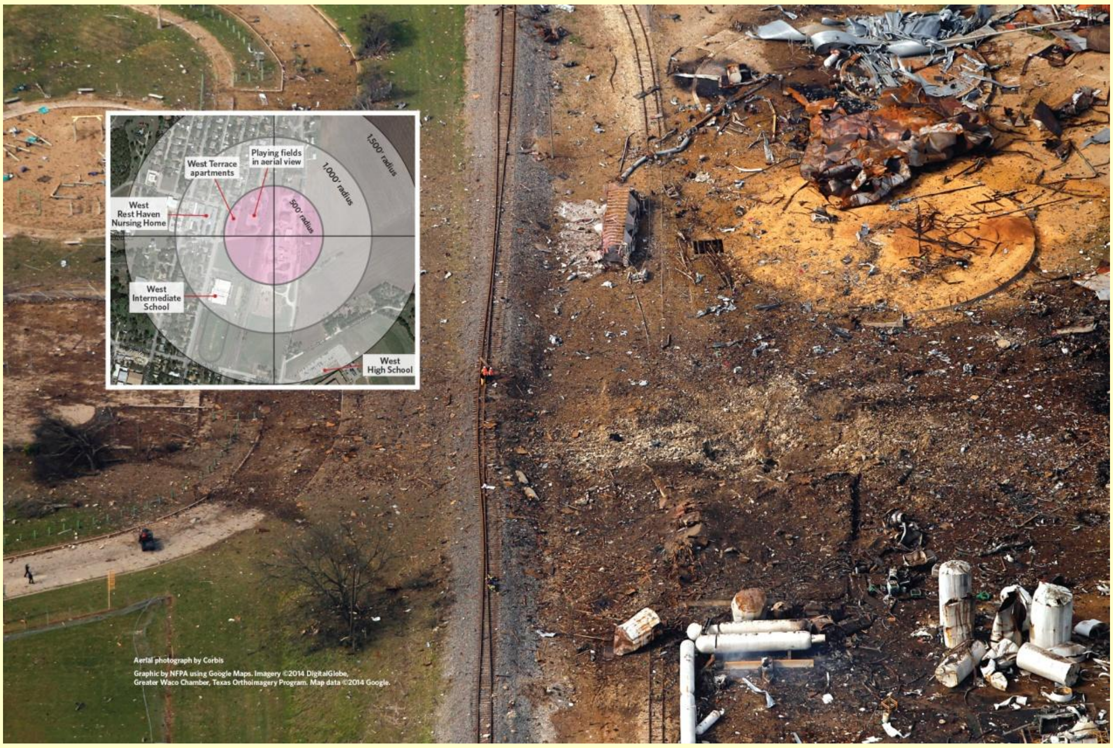
The explosion came two days after three alleged anarchists appeared in court and were ordered held on suspicion of planting at least four bombs, including one that injured 14 people at a shopping plaza near a subway station this month.

Interior Minister Rodrigo Penailillo said the design of latest bomb appeared to differ with that used in the subway blast.

Enhanced Technical Brief on Blast Effects of Ammonium Nitrate

By Anthony Kimery (Editor-in-Chief HSToday.US)

Source: http://www.hstoday.us/single-article/enhanced-technical-brief-on-blast-effects-of-ammonium-nitrate/83a88092643efd0500fa0225fa57d335.html



Aerial photograph by Corbis

Graphic by NFPA using Google Maps. Imagery ©2014 DigitalGlobe, Greater Waco Chamber, Texas Orthoimagery Program. Map data ©2014 Google.

Following the massive explosion on April 18, 2013 at the West Fertilizer Company in West, Texas -- where ammonium nitrate was stored and distributed -- that killed 15 and injured 160, considerable attention has been focused on ammonium nitrate.

Fears about the use of ammonium nitrate being used in highly destructive bombs have been etched into the national psyche since Al Qaeda's first attack on New York City's North Tower of the World Trade Center on February 26, 1993. A truck carrying a 1,336 pound gas enhanced urea nitrate bomb was detonated below the building, killing 6 and injuring more than 1,000.

Two years later, on April 19, 1995, an ammonium nitrate truck bomb killed 168 people and injured more than 680 when it was detonated in front of the federal building in downtown Oklahoma City.

In direct response to the West Fertilizer Company event, President Obama signed Executive Order 13650 – Improving Chemical Facility Safety and Security -- in August 2013. The subsequent working group substantively focused on updating and improving safety standards for facilities storing ammonium nitrate. As a result, many public safety officials have a greater awareness and understanding of ammonium nitrates dangers.

This week, Aristatek, Inc, a leading provider of hazardous materials response solutions, will release an enhanced version of its widely distributed technical paper that details the blast and explosive effects of ammonium nitrate.

The original brief, which was presented and distributed to lawmakers during a hearing by the Texas House Homeland Security and Public Safety Committee in August 2013 has been enhanced with shipped quantity blast effects and widely accepted handling and storage tips for ammonium nitrate.

The enhanced brief is complimentary for fire departments, fire marshals, fire inspectors, LEPC/EMA officials or any other public safety and health professionals that visit the company's web site at www.aristatek.com .

"These enhancements to our ammonium nitrate tech brief have helped transform it into a one-stop resource for public safety officials," said AristaTek CEO

Bruce King. "Now anyone trying to do a full analysis of ammonium nitrate blast effects in their community, whether it be shipped or stored, can do so from this one document along with gaining an understanding of how this substance should be safely stored, handled, etc."

"After a year, there is still a lot of concern over this substance," King said in a statement. "We hope this enhanced brief aids those folks still trying to deal with these hazards in their community, especially those that missed the brief the first time around."

The enhanced technical brief, *Ammonium Nitrate Estimated Blast Effects and Best Handling Practices*, includes a blast effects table for ammonium nitrate quantities from one ton to 300 tons, as well as expert commentary on how to interpret the blast effects table. According to the company, the table was prepared using a combination of the firm's industry-leading hazardous materials response software, PEAC-WMD, and its in-house chemists and engineers.

The newest updates to the technical brief include enhancements to the blast effects table to highlight common shipping quantities for the substance via rail or truck. It also includes "best practices" for safe handling and storage of ammonium nitrate compiled from many articles and guidelines that have been issued by federal and state agencies over the past year.

The primary damage generated from an explosion is the blast or shock wave, also referred as over-pressurization, that's generated by the rapid temperature rise and subsequent expansion from the chemical reaction within the components of the explosive substance upon detonation, the technical brief states, noting that, "Additional damage can result from fragments or shrapnel thrown from the blast by the shock wave."

With sufficient energy within a defined area, these fragments "would cause serious injury," the briefing states.

"The risk of fire or explosion is greatly increased if ammonium nitrate is mixed with combustible or incompatible materials, such as powdered metals, alkali metals, urea, chromium or copper salts, organic and carbonaceous materials, sulfur, nitrites, alkalis, acids, chlorates and reducing agents," the brief said.

Bulgaria explosives factory blast kills 15

Source: http://www.bbc.com/news/world-europe-29455550

October 02 – **A blast at an explosives factory north of the Bulgarian capital Sofia has killed 15 people, prompting the government to declare Friday a day of national mourning.**

SERBIA
Gorni Lom
Sofia
BULGARIA

Thirteen men and two women were killed, and three other women employees hurt, at the factory near Gorni Lom.

"The blast was so powerful that it left craters," civil defence force director Nikolay Nikolov said.

He said the cause of the explosion was probably "human error".

With the country holding a general election on Sunday, one leading politician said his party was muting its campaign as a sign of respect.

Former Prime Minister Boiko Borisov, whose Gerb party is tipped to win against the outgoing Socialists, told Bulgarian TV station 24 Hours that concerts and other events would be called off.

The explosion occurred at around 17:00 (14:00 GMT) on Wednesday with a big secondary blast reported at 21:45.

The factory, some 120km (75 miles) north of Sofia, destroys stockpiles of obsolete munitions for the Bulgarian army and Dnes daily newspaper quoted an expert as saying it had been handling explosives from Greece.

Some 10 tonnes of highly explosive chemicals were being stored at the plant.

"The factory has been reduced to ashes," an interior ministry spokesman said.

There were explosions at the factory in 2007 and 2010, in which several people were hurt.

Two units of the plant were flattened in the 2010 blast.

Sensor network will track down illegal bomb-making

Source: http://www.homelandsecuritynewswire.com/dr20141002-sensor-network-will-track-down-illegal-bombmaking

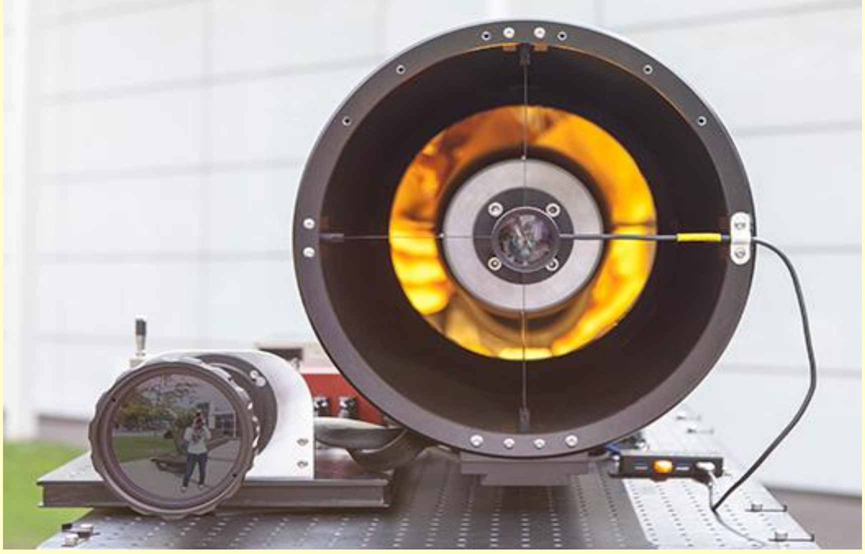
A network of different sensors will detect illicit production of explosives and improvised explosive devices (IEDs). Traces on doorknobs, in sewage, or in the air will be detected by the sensors and the data will be fused in a command center. The Fraunhofer Institute for Applied Solid State Physics IAF is developing an imaging laser technology which will allow a precise localization of the dangerous substances.

Terrorists can manufacture bombs with relative ease, few aids, and easily accessible materials such as synthetic fertilizer. Security forces do not always succeed in preventing the attacks and tracking down illegal workshops in time. Bomb manufacturing, however, leaves its traces: **Remains of the synthetic fertilizer stick to stairs and doorknobs, waste from the manufacturing process gets into the sewerage and is deposited in air ducts.** Until now, no technology for systematically discovering illegal bomb production in an early stage has been commercially available. Researchers have now developed a sensor network as part of the EU project EMPHASIS which can detect such activity early on and locate it precisely. A Farunhofer IAF release reports that last week, they showed how a simple kitchen used to manufacture explosives can be tracked down at the test site of the Swedish Defense Research Agency (FOI) near Grindsjön in southern Sweden.

Different sensors send data to command center

To keep the rate of false alarms as low as possible, different sensor technologies for early and precise localization of illegal bomb manufacturing are implemented. **The sensors are placed at different locations such as on apartment buildings or in sewers. Thus waste produced during the manufacturing of explosives and bombs can be detected early on. In the command center, the data from all sensors is collected and automatically analyzed.**

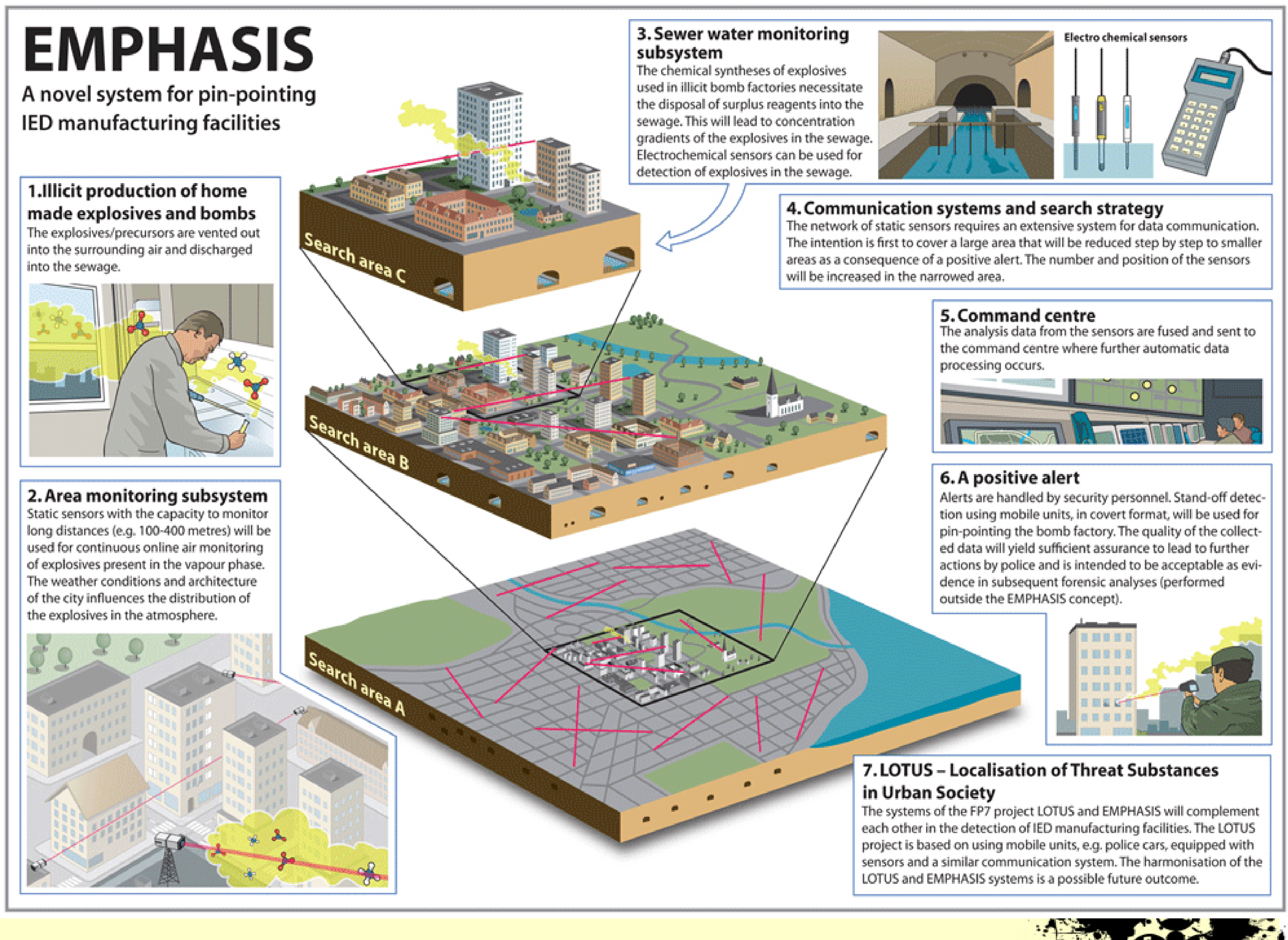
Suspicious results trigger the alarm. With the help of laser-based measurement techniques, security forces can then localize the bomb workshop from a distance. The infrared laser system of Fraunhofer IAF in Freiburg evaluates the data from the spectroscopic measurements directly and shows the results on a monitor. "Our laser technology can reliably detect even faint traces of dangerous substances from a distance of about twenty meters," says Dr. Frank Fuchs, who leads the project at Fraunhofer IAF. This reduces the safety risk for the operational forces. The implemented quantum cascade lasers emit in the infrared area and so do not endanger the human eye. The wavelength area between 7.5 and 11 micrometers is well-suited for sensorics anyway: The molecules of organic compounds absorb very strongly in these wavelengths. Chemical compounds show specific absorption lines in this area. They can thus be exactly determined using these characteristic "fingerprints."



Quantum cascade lasers (photo) can solve many of sensorics' problems

Laser-based spectroscopy combined with a real-time visualization of the measurement results will solve many of sensorics' problems in the future.

At airports or train stations, laser technology can be implemented to check suspicious luggage for explosives. It also promises quick and precise spectroscopic measurements



EMPHASIS

A novel system for pin-pointing IED manufacturing facilities

1. Illicit production of home made explosives and bombs
The explosives/precursors are vented out into the surrounding air and discharged into the sewage.

2. Area monitoring subsystem
Static sensors with the capacity to monitor long distances (e.g. 100-400 metres) will be used for continuous online air monitoring of explosives present in the vapour phase. The weather conditions and architecture of the city influences the distribution of the explosives in the atmosphere.

3. Sewer water monitoring subsystem
The chemical syntheses of explosives used in illicit bomb factories necessitate the disposal of surplus reagents into the sewage. This will lead to concentration gradients of the explosives in the sewage. Electrochemical sensors can be used for detection of explosives in the sewage.

4. Communication systems and search strategy
The network of static sensors requires an extensive system for data communication. The intention is first to cover a large area that will be reduced step by step to smaller areas as a consequence of a positive alert. The number and position of the sensors will be increased in the narrowed area.

5. Command centre
The analysis data from the sensors are fused and sent to the command centre where further automatic data processing occurs.

6. A positive alert
Alerts are handled by security personnel. Stand-off detection using mobile units, in covert format, will be used for pin-pointing the bomb factory. The quality of the collected data will yield sufficient assurance to lead to further actions by police and is intended to be acceptable as evidence in subsequent forensic analyses (performed outside the EMPHASIS concept).

7. LOTUS – Localisation of Threat Substances in Urban Society
The systems of the FP7 project LOTUS and EMPHASIS will complement each other in the detection of IED manufacturing facilities. The LOTUS project is based on using mobile units, e.g. police cars, equipped with sensors and a similar communication system. The harmonisation of the LOTUS and EMPHASIS systems is a possible future outcome.

without costly laboratory examinations when controlling food, medicine or drinking water. The source of pollution could be found more quickly in factories and production halls. “Quantum cascade lasers can principally be used wherever the chemical nature of a surface or its change through pollution is of interest,” says Fuchs. “As our lasers are widely tunable, they can be adapted specifically for different issues and be the basis for highly sensitive sensors in different applications.”

About the project
The goal of the EU project EMPHASIS (Explosive Material Production Hidden Agile Search and Intelligence System) aims to develop and test a system concept for detecting ongoing illicit production of explosives and improvised explosive devices (IEDs) in urban areas. The project is funded by the EU as part of the Seventh Framework Program (FP7). Under the coordination of the Swedish Defense Research Agency FOI, the following partners are working on the project: the Fraunhofer Institutes for Applied Solid State Physics IAF and for Chemical Technology ICT, the Netherlands Organization for Applied Scientific Research TNO, the Institut National de Police Scientifique from France, and the companies Cascade Technologies from Scotland, Morpho S.A. from France, as well as VIGO System S.A. from Poland.

Rapiscan launches new explosives trace detector

Source: http://www.counteriedreport.com/news/rapiscan-launches-new-explosives-trace-detector

Rapiscan Systems Inc. has launched a new handheld explosive trace detection system called DETECTRA HX.

The device features high-throughput and high-detection capabilities for detecting trace explosives in both particulate and vapor form on surfaces that may have directly or indirectly absorbed explosive residues.
It also features a swipe sampling system and a "touch-free inhalation sampling method for threat scenarios that involve highly unpredictable explosives compositions."

"The RAPISCAN DETECTRA HX was completely designed with the end-user in mind," said Brad Buswell, president of Rapiscan Systems North America. "Not only does the solution detect threats with tremendous accuracy, it also features an intuitive user interface with just three-buttons and detects threats in seconds.
"Operator training can take as little as an hour, which means that the DETECTRA HX is easy to deploy."
Rapiscan said there are no end-user radiation licensing requirements for use in the United States. The system uses an ionization source which has U.S. Nuclear Regulatory Commission Exempt Distribution status.
DETECTRA HX was launched at the 60th Annual ASIS International Seminar and Exhibit in Atlanta, Ga.

Counter IED and Mine System unveiled

Source: http://i-hls.com/2014/10/hebrew-counter-ied-mine-system-unveiled/

Israel Aerospace Industries (IAI) unveiled its new CIMS (Counter IED and Mine Suite) – an integrated suite of sensors for protection of tactical maneuvering vehicles.

Although mines and IEDs (Improvised Explosive Devices) are hardly new, the use of these devices has become a matter of concern for modern armies both in conventional and assymetric warfare. The CIMS suite was designed under the premise that no one sensor can provide the adequate probability of detection and low false-alarm rate required by today's operational needs.

The CIMS suite detects surface and underground IEDs, mines, and roadside bombs, and consists of an ADS – Above-surface Detection System, and MIDS – underground Mine and IED Detection System.

The ADS includes a groundbreaking side-looking SAR radar, high-resolution optical detection system and an infrared multispectral investigation system. MIDS comprises a Ground Penetrating Radar (GPR) and a magnetic detector.

Integration of the sensor suite through a central processing and management system delivers accurate synergetic real-time mapping of IED threats to the warfighter, requiring minimal training and decision-making. The CIMS suite and its subsystems can be adapted to any combat tactical vehicle.

"CIMS was designed first and foremost to save lives," said Nissim Hadas, IAI VP & ELTA President. "Our combination of unique sensors allows a simple and highly effective mine and IED detection system to be provided to forward forces. We see huge potential for this system and consider it to be a groundbreaking solution."

New Cargo Inspection and Explosives Trace Detection Systems from Smiths Detection

Source: http://www.hstoday.us/single-article/new-cargo-inspection-and-explosives-trace-detection-systems-from-smiths-detection/984e84ba8c3dfb6995de543b5e45786d.html

HI-SCAN 180180-2is pro is an advanced dual-view X-ray system for screening large-scale freight, air cargo and mail. It is an advanced version of the HI-SCAN 180180-2is.

The new 'pro' version meets the current global legal requirements for 100% inspection of air cargo on passenger flights. It also reflects the increasing need for X-ray units capable of screening LD3 containers as well as the largest package size accepted by the Transportation Security Administration: 48 x 48 x 65 ins / 122 x 122 x 165 cm (W x L x H).

HI-SCAN 180180-2is pro is capable of screening large containers without the need to disassemble consolidated freight into individual packages. This measure is designed to cut re-inspection times considerably and ensure both high throughput and a fast, efficient inspection process.

Security standards are increased by the use of dual-view, with top and side views of the screened objects to allow precise image interpretation.

Although the system features a large tunnel opening of 180 x 180 cm, capable of screening LD3 containers, the HI-SCAN 180180-2is pro offers a compact footprint which minimizes the required floor space and the associated lifecycle costs. The small pitch roller conveyors provide a smooth passage for the scanned goods and supports a total load of up to 5000 kg/m (evenly distributed).

“In the course of redesigning the HS 180180-2is we have revisited nearly every important feature and are proud to present our customers with a unique product, both in performance and reliability," said Hans Zirwes, vice president international sales for Smiths Detection. "We are confident that HI-SCAN 180180-2is pro will support our customers whenever the requirement is for the efficient inspection of air freight, as well as applications in other sectors such as customs or critical infrastructure security.”

The launch follows Smiths Detection’s introduction of a new explosives trace detector to its IONSCAN series in late September. Building on the IONSCAN 500DT, the new IONSCAN 600’s breakthrough feature is a proprietary non-radioactive Ion Mobility Spectrometry source which eliminates the need for special licensing, handling or disposal requirements.

The IONSCAN 600 weighs 23 pounds (10.4 kg) and is equipped with a built-in handle making it portable. Its hot-swappable battery provides continued sampling and analysis capability, allowing it to be moved while still in use.

Shodan: The scariest search engine on the Internet

Source: http://money.cnn.com/2013/04/08/technology/security/shodan/

**When people don't see stuff on Google,
they think no one can find it.
That's not true!**

That's according to John Matherly, creator of Shodan, **the scariest search engine on the Internet.**

Unlike Google which crawls the Web looking for websites, Shodan navigates the Internet's back channels. It's a kind of "dark" Google, looking for the servers, webcams, printers, routers and all the other stuff that is connected to and makes up the Internet.

Shodan runs 24/7 and collects information on about 500 million connected devices and services each month.

It's stunning what can be found with a simple search on Shodan. Countless traffic lights, security cameras, home automation devices and heating systems are connected to the Internet and easy to spot.

Shodan searchers have found control systems for a water park, a gas station, a hotel wine cooler and a crematorium. Cybersecurity researchers have even located command and control systems for nuclear power plants and a particle-accelerating cyclotron by using Shodan.

What's really noteworthy about Shodan's ability to find all of this -- and what makes Shodan so scary -- is that very few of those devices have any kind of security built into them.

"It's a massive security failure," said HD Moore, chief security officer of Rapid 7, who operates a private version of a Shodan-like database for his own research purposes.

A quick search for "default password" reveals countless printers, servers and system control devices that use "admin" as their user name and "1234" as their password. Many more connected systems require no credentials at all -- all you need is a Web browser to connect to them.

In a talk given at last year's Defcon cybersecurity conference, independent security penetration tester Dan Tentler demonstrated how he used Shodan to find control systems for evaporative coolers, pressurized water heaters, and garage doors.

He found a car wash that could be turned on and off and a hockey rink in Denmark that could be defrosted with a click of a button. A city's entire traffic control system was connected to the Internet and could be put into "test mode" with a single command entry. And he also found a control system for a hydroelectric plant in France with two turbines generating 3 megawatts each.

Scary stuff, if it got into the wrong hands.

"You could really do some serious damage with this," Tentler said, in an understatement.

So why are all these devices connected with few safeguards? Some things that are designed to be connected to the Internet, such as door locks that can be controlled with your iPhone, are generally believed to be hard to find. Security is an afterthought.

A bigger issue is that many of these devices shouldn't even be online at all. Companies will often buy systems that can enable them to control, say, a heating system with a computer. How do they connect the computer to the heating system? Rather than connect them directly, many IT departments just plug them both into a Web server, inadvertently sharing them with the rest of the world.

"Of course there's no security on these things," said Matherly, "They don't belong on the Internet in the first place."

The good news is that Shodan is almost exclusively used for good.

Matherly, who completed Shodan more than three years ago as a pet project, has limited searches to just 10 results without an account, and 50 with an account. If you want to see everything Shodan has to offer, Matherly requires more information about what you're hoping to achieve -- and a payment.

Penetration testers, security professionals, academic researchers and law enforcement agencies are the primary users of Shodan. Bad actors may use it as a starting point, Matherly admits. But he added that cybercriminals typically have access to botnets -- large collections of infected computers -- that are able to achieve the same task without detection.

To date, most cyberattacks have focused on stealing money and intellectual property. Bad guys haven't yet tried to do harm by blowing up a building or killing the traffic lights in a city.

Security professionals are hoping to avoid that scenario by spotting these unsecured, connected devices and services using Shodan, and alerting those operating them that they're vulnerable. In the meantime, there are too many terrifying things connected to the Internet with no security to speak of just waiting to be attacked.

IBM Security Services 2014 - Cyber Security Intelligence Index

Source: http://www.slideshare.net/ibmsecurity/2014-cyber-security-intelligence-index

IBM Security Services 2014
Cyber Security Intelligence Index

Analysis of cyber attack and incident data from IBM's worldwide security operations

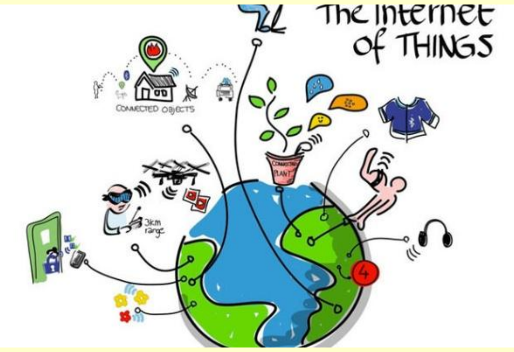
IBM

▶ **Read online at source's URL**

Bot-herders can launch DDoS attacks from dryers, refrigerators, other Internet of Things devices

By Tim Greene

Source: http://www.networkworld.com/article/2687169/security0/bot-herders-can-launch-ddos-attacks-from-dryers-refrigerators-other-internet-of-things-devices.html



A new malware kit called Spike can infect not only traditional desktops but also routers, smart thermostats, smart dryers and a host of other Internet of Things devices to herd them into massive botnets.

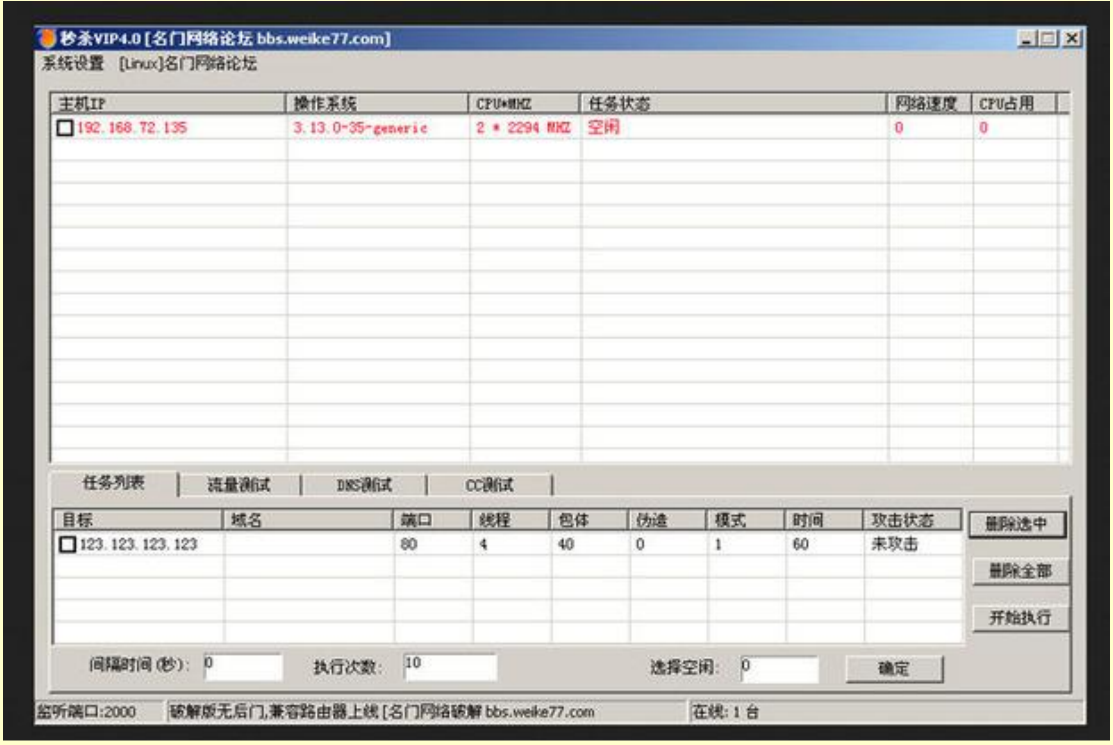
Spike botnets have carried out various forms of DDoS attacks including SYN, UDP, DNS query and GET floods, according to Akamai's Prolexic Security Engineering & Response Team

(PLXsert).

The Akamai team has seen Spike DDoS attacks in action in Asia and the U.S. and reports that one such attack peaked at 215Gbps and 150 million packets per second. Akamai has validated that 12,000 to 15,000 devices made up one botnet created with the kit, says David Fernandez, who heads up Akamai's PLXsert team.

Corporate security pros need to harden devices they might not have thought were at risk as well as get traditional DDoS protection in place, Akamai says.

PLXsert and Russian anti-virus company Dr. Web say that between them they have seen the malicious Spike payload ported to Linux and Windows desktops and servers as well as ARM-based Linux devices, specifically customer routers installed by ISPs. But the ARM malware could be used to infect other devices such as smart appliances, Fernandez says.



主机IP	操作系统	CPU*MHZ	任务状态	网络速度	CPU占用
□ 192.168.72.135	3.13.0-35-generic	2 * 2294 MHZ	空闲	0	0

目标	域名	端口	线程	包体	伪造	模式	时间	攻击状态
□ 123.123.123.123		80	4	40	0	1	60	未攻击

间隔时间(秒): 0 执行次数: 10 选择空闲: 0

监听端口:2000 破解版无后门,兼容路由器上线 [名门网络破解 bbs.weike77.com 在线: 1 台

Screen shot of the command and control interface for the Spike DDoS toolkit.

Data integration is often underestimated and poorly implemented, taking time and resources. Yet it
Telltale binary code on these devices is the sign that they have been infected, the company says. The Spike code consists of a single binary while the infections found by Dr. Web include several binaries and scripts. The kit interface is written in Mandarin Chinese. So far, it has not yet been seen in underground marketplaces, Fernandez says.

Timestamps on the binaries indicate they were written about six months ago. The toolkit gets its name from the word "spike" found in the code, he says.

Fernandez says his group is working on a proof of concept attack to infect IoT devices, but hasn't done so successfully yet. "The ability of the Spike toolkit to generate an ARM-based payload suggests that the authors of such tools are targeting devices such as routers and IoT devices to expand their botnets for a post-PC era of botnet propagation," says the Akamai advisory.

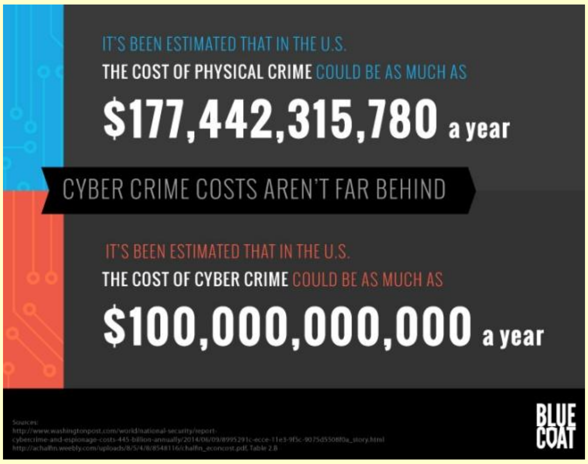
Akamai says the DDoS attacks can be mitigated using access control lists. It has written a SNORT signature that can mitigate application-layer GET flood attacks generated through the toolkit. The Akamai advisory lists sites where users can find methods for hardening the various operating systems Spike attacks.

***Tim Greene** covers Microsoft for Network World and writes the Mostly Microsoft blog.*

Cyber Crime Growing – Common Attack Techniques

By Sean Huggett

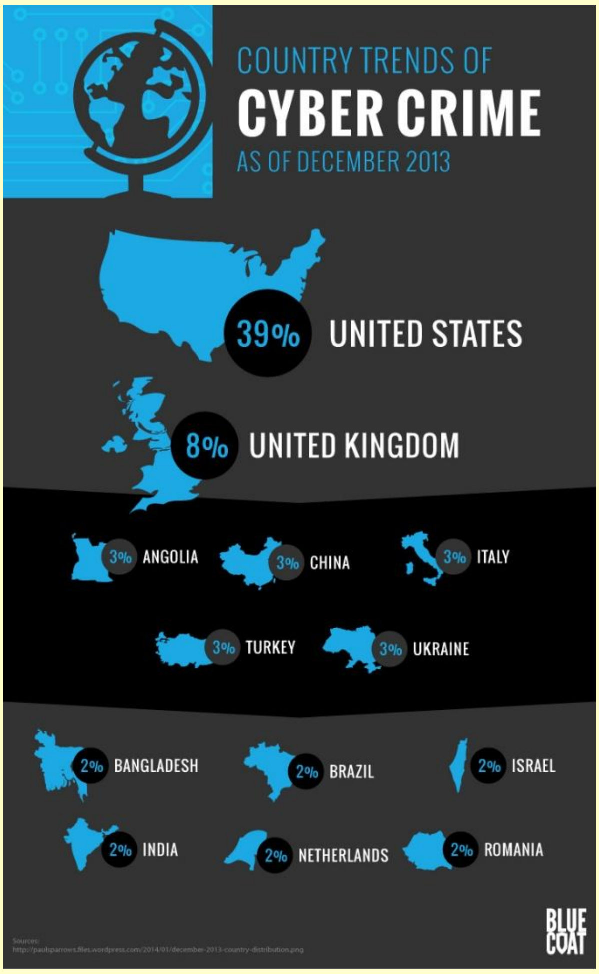
Source: http://www.voyager.net.uk/blog/cyber-crime-growing-common-attack-techniques/#sthash.UEaMaF5b.dpuf



Sources:
http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/09/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html
http://achalfin.weebly.com/uploads/8/5/4/8/8548116/chalfin_econcost.pdf, Table 2.8

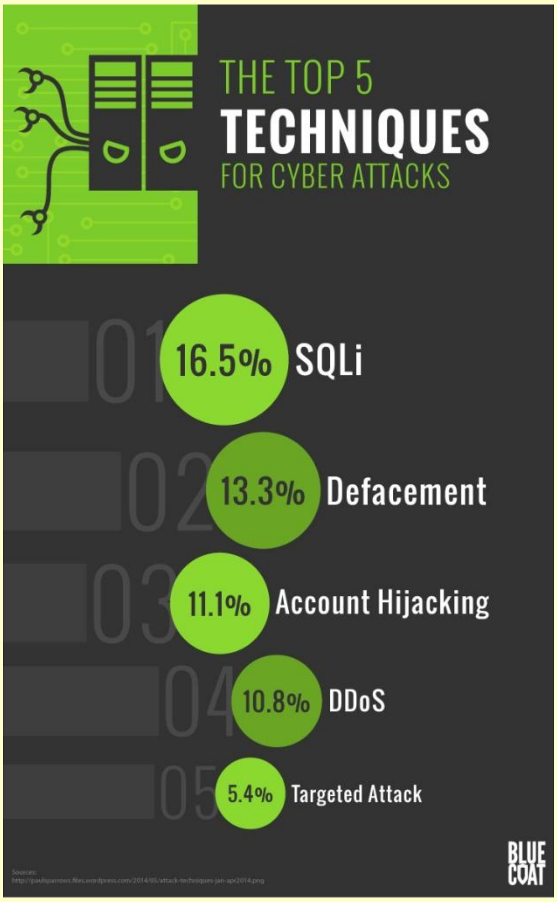
Our partner Blue Coat Systems recently published a blog post accompanied with powerful statistics that compared real-world crime and cyber crime and showed that cyber crime is at an all time high.
Cyber crime is estimated to cost the US $100bn a year. By contrast real world crime is estimated to cost the country $177bn each year. So whilst not yet at the same level it is catching up quickly.

Digging into the statistics some more, the Blue Coat post reports that the number of internet crime complaints in 2000 was 16,838. This rose to 262,813 complaints to the Internet Crime Center in 2013.



Sources:
http://paulsparrows.files.wordpress.com/2014/01/december-2013-country-distribution.png

Some of the main techniques for cyber attacks include:



Sources:
http://paulsparrows.files.wordpress.com/2014/05/attack-techniques-jan-apr2014.png

SQL Injection (SQLi)

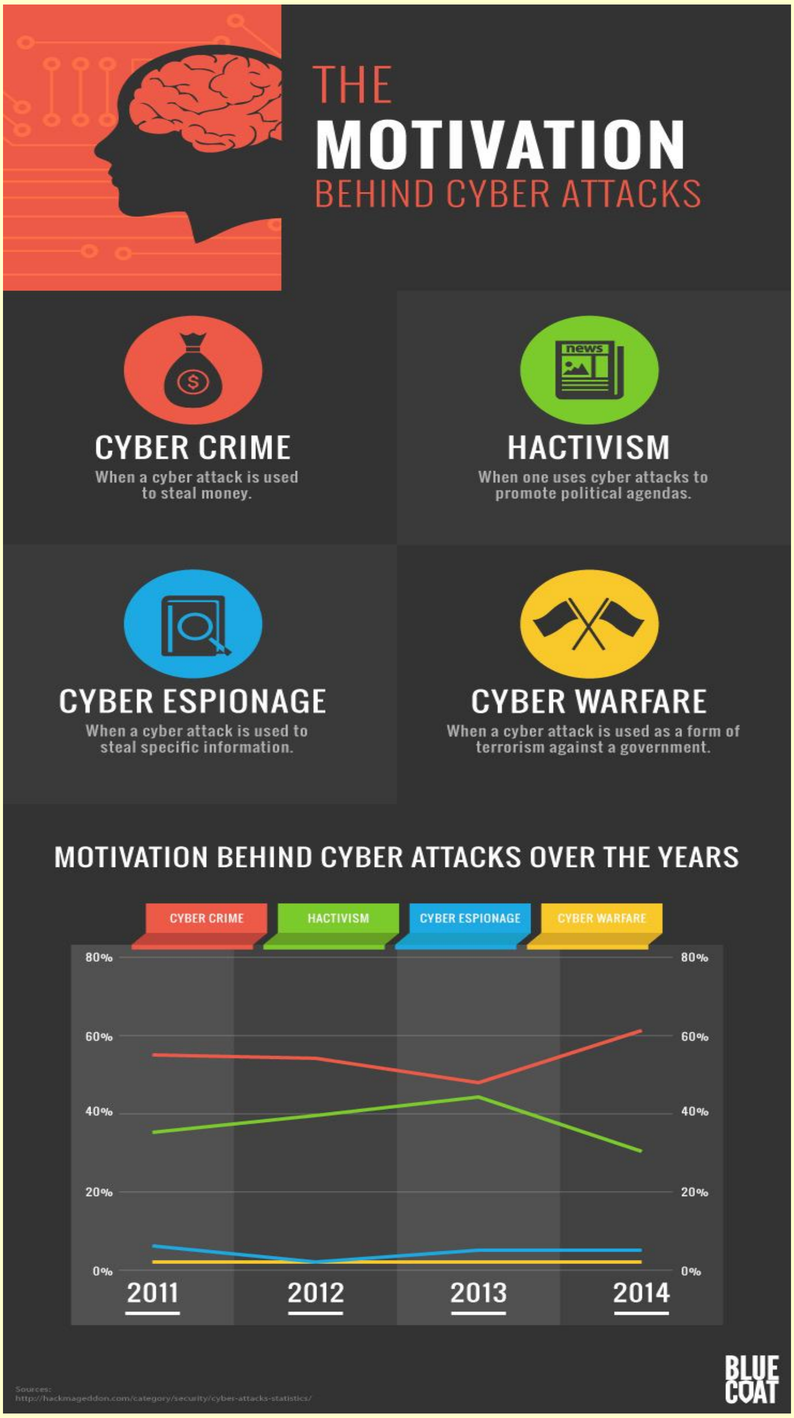
An SQLi attack targets code and vulnerabilities in software. It is a common technique by so-called "hacktivists," and was the main technique used for cyber attacks last year.

Defacement

Hacktivists also favour website defacement according to Blue Coat. This involves changing the appearance of a site or a web page. It is akin to graffiti but with a far wider reaching audience.

Account Hijacking

This technique is becoming increasingly common. It started with hijacked emails but is becoming a bigger problem on social media. Hackers aim to get access to accounts and personal information. This article shares a powerful story of how one man's digital life was turned upside down when his digital accounts were hijacked.



Sources:
http://hackmageddon.com/category/security/cyber-attacks-statistics/

DDoS

Distributed denial-of-service or DDoS attacks make a machine or network resource unavailable to its users. This is a common threat for big organisations and can be incredibly inconvenient and especially costly. I use Feedly as my RSS reader of choice and **they were subject to DDoS attacks** in June which rendered the service unusable for a while – the attackers were demanding money to stop the attacks. **Evernote also suffered DDoS attacks** around the same time.

Targeted Attack

A targeted attack seeks to breach the security of a specific person or organisation. – it's exactly as it sounds and, sadly, could be the result of someone paying for 'cyber crime as a service',

As Blue Coat say in their in their blog post, it is important to take steps to protect yourself and your organisation from cyber crime – their point being that we don't invite criminals into our house or office from the street so we shouldn't let them into our house or office online either.

At Voyager, we work with a number of Gartner Magic Quadrant leading cyber security partners and specialise in network and internet security solutions. We can arrange a free of charge security audit of your network or free product trial if you;re considering improving your security. Please contact us using the button below for more details.

***Sean Huggett** is Managing Director at Voyager Networks, specialists in Cloud, Mobility, Communication & Security Solutions and Managed Services.*

Tracks of tears on eye's corneal surface could hold key to cyber security

Source:http://www.disclose.tv/news/Tracks_of_tears_on_eyes_corneal_surface_could_hold_key_to_cyber_security/109103

Tears can expose our most private emotions but could they also secure our most private information online?

Stephen Mason, an Australian optometrist, has discovered a new way to use scans of people's tears as passwords which he calls "the world's first one-time biometric pin".

He has focused on the cornea, rather than the iris, which is the norm in most optical scanners, because cyber criminals cannot copy the unique way tears change our eyes.

The scanner can recognise a person because each cornea has a unique map. But if a criminal was to steal and try to use the data from the last time someone logged in, the machine would find it invalid because it expects the data to change slightly each time.

"The corneal surface is wet with tears so our own data changes from moment to moment," he said.

"Each data set I capture from any eye has these really tiny variations."

The hope is that the technology could be included on smartphones, from where it could be used to verify payments and access services such as email or sensitive corporate documents online. It could also be embedded in ATMs or doors to access confidential areas.

From intimate photos snatched and released online from celebrities' Apple iCloud accounts to an attack on Home Depot, the largest known security breach of a retailer, the rise in cyber crime has experts searching for better ways to verify people's identities.

Simple passwords remain the most common way that individuals protect their data but many experts and technology companies believe this is an outdated form of protection and are turning to biometric alternatives.

Identity X, a US-based security company, uses voice identification as one factor for identifying people trying to access banking services remotely. Barclays Bank is set to launch scanners in the UK to identify some corporate customers using the unique vein patterns in their fingers.

Companies using more conventional fingerprint readers include Apple, which has one on its iPhone 5s and iPhone 6 devices, Samsung, which includes one on the most recent Galaxy handset, and Lenovo, the Chinese PC maker which has used them on its Thinkpad laptops.

Vinny Sakore, cloud security manager at the International Computer Security Association Labs, a security testing company, said passwords are probably the main reason why systems are breached.

One concern about existing biometric security systems is the risk of having the data stolen. Mr Mason said that people did not know what an exact copy of a fingerprint could be used for in the future.

But biometric technology is not the only potential solution. Many start-ups are trying to solve the same security problem, from password managers which store encrypted passwords and enter them on each site, to hardware key fobs which contain codes that are difficult to crack.

Mr Sakore cautioned that biometric technology "isn't quite there yet", with glitches such as not working with swollen fingers.

North Korea cyber warfare capabilities exposed

Source: http://i-hls.com/2014/09/north-korea-cyber-warfare-capabilities-exposed/

A new HP report suggests the reclusive country’s cyber warfare capabilities are rapidly making North Korea a credible threat to Western systems.

Warfare capabilities are on the rise despite being entrenched in ageing infrastructure and dampened by a lack of foreign technology.

According to a report released by Hewlett-Packard researchers and published by *ZD NET*, the so-called ‘Hermit Kingdom’ may keep Internet access from the masses and maintain an iron grip on information exchange, but this hasn’t stopped the country from training up the next generation of cybersecurity and cyber warfare experts.

A number of countries, including the United States, have imposed restrictions on North Korea which prevents the open trade of technologies which would enhance cyber tools and capabilities due to the regime’s treatment of citizens and closed-border policy. However, according to HP, the country is “remarkably committed” to improving its cyber warfare capabilities.

South Korea views the regime’s cyber capabilities as a terrorist threat, and has prepared for a multifaceted attack in the future – although it is important to note no such attack has yet occurred. According to a report written by Captain Duk-Ki Kim, a Republic of Korea Navy officer, "the North Korean regime will first conduct a simultaneous and multifarious cyber offensive on the Republic of Korea's society and basic infrastructure, government agencies, and major military command centers while at the same time suppressing the ROK government and its domestic allies and supporters with nuclear weapons." South Korea also claims that North Korea's "premier" hacking unit, Unit 121, is behind the US and Russia as the "world's third largest cyber unit."

In 2012, South Korea estimated that North Korea's hacking team comprises of roughly 3000 staff, while a report released by South Korean publication Yonhap upgraded this figure to 5900.

According to the PC maker, it is difficult to gather intelligence on the isolated North Korea's hacking teams. Reports not only often come from the US and South Korea, but reports coming from the latter may be biased due to the political tension between the two regions. Another problem is North Korea's heavy restriction on Internet use, which is censored by the state and only used by the social elite. However, this means that any attacks originating from the country are highly likely to be state-sponsored, and rogue actors are unlikely to exist. Cyberattacks will therefore be attributed to the country's governing body. HP says that many attacks sponsored by the regime originate from other countries, including China, the US, Europe and even South Korea.

North Korea's Reconnaissance General Bureau (RGB) is in charge of both traditional and cyber operations, and is known for sending agents abroad for training in cyber warfare. The RGB reportedly oversees six bureaus that specialize in operations, reconnaissance, technology and cyber matters, two of which have been identified as the No. 91 Office and Unit 121. The two bureaus in question comprise of intelligence operations and are based in China.

The RGB also reportedly oversees state-run espionage businesses located in 30 to 40 countries, often hosted in unsuspecting places such as cafes. Members of this espionage network reportedly "send more than $100 million in cash per year to the regime and provide cover for spies," the report says.

In addition, the country's Worker's Party oversees a faction of ethnic North Koreans living in Japan. Established in 1955, the group – dubbed the Chosen Soren – refuse to assimilate in to Japanese culture and live in the country in order to covertly raise funds via weapons trafficking, drug trafficking and other black market activities. The group also gathers intelligence for the country and attempts to procure advanced technologies.

Despite ageing infrastructure and power supply problems, North Korea reportedly was able to gain access to 33 of 80 South Korean military wireless communication networks in 2004, and an attack on the US State Department believed to be approved by North Korean officials coincided with US-North Korea talks over nuclear missile testing in the same time period. In addition, a month later, South Korea claimed that Unit 121 was responsible for hacking into South Korean and US defense department networks.

North Korea also tested a logic bomb in 2007 – malicious code programmed to execute based on a pre-defined triggering event – which led to a UN sanction banning the sale of particular hardware to the country.

According to the report, the regime regularly exploits computer games in order to gain financially and orchestrate cyberattacks. In 2011, South Korean law enforcement arrested five men for allegedly collaborating with North Korea to steal money via online games, specifically the massive multiplayer online role-playing game (MMORPG) “Lineage.” The games were believed to act as conduits for North Korea to infect PCs and launch distributed denial of service (DDoS) attacks against its southern neighbor.

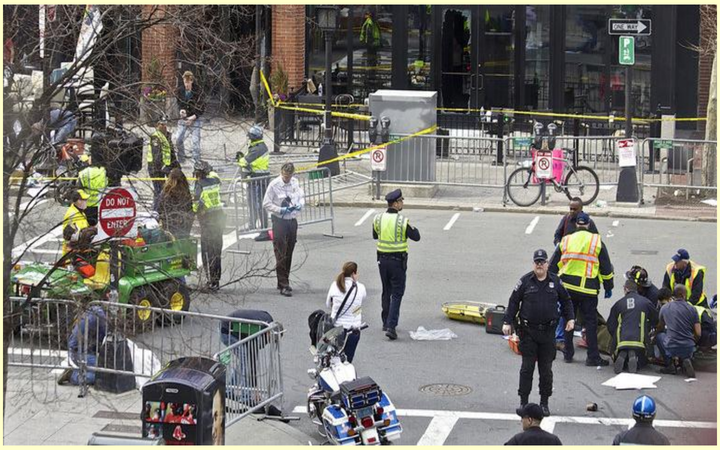
However, it is worth noting that North Korea’s DDoS capabilities are lacking as there are few outgoing connections due to heavy censorship and Internet restriction. This is why researchers believe the country uses the networks of other nations and botnets instead.

► **See also this video:** http://www.youtube.com/watch?v=eVd-tve7MFM

Social Media: Big Lessons from the Boston Marathon Bombing

Source: http://www.emergencymgmt.com/training/Social-Media-Lessons-Boston-Marathon-Bombing.html

At 2:49 p.m. on April 15, 2013, at the height of Boston’s annual Marathon, two bombs exploded near the finish line, killing three people and injuring more than 260 others. What followed was an extraordinary manhunt, which included a shelter-in-place request from the governor that virtually shut down the city, along with the use of social media by law enforcement as a key communications tool to keep the media and frightened citizens accurately informed about what was going on.



Within 10 minutes of the bombing, Boston Police Department (BPD) Commissioner Edward Davis told his department to start using social media and to let people know what had occurred. The importance of social media as a policing tool, in particular Twitter and Facebook, soon became apparent. Misinformation, spread by professional media outlets and social media itself, was quickly corrected by the BPD. It didn’t take long for the media to realize that the most accurate information about the bombing was coming from the official BPD Twitter account.

“The Boston Police Department was outstanding and it was so simple and effective,” said Lt. Zachary Perron, public information officer for the Palo Alto, Calif., Police Department. “They became the news source during the crisis. It was a watershed moment for law enforcement and social media."

Perron should know. He is in charge of the department’s social media program in a Silicon Valley city where just about everybody uses social media and news is covered by four daily newspapers. What began as part-time work is now a full-time position for Perron. His job, as well as for other police officers in charge of social media, is to direct public relations through the various channels — Twitter, Facebook, YouTube — but to do it in a real-time manner and with a much broader constituency. No longer do press releases just go out to the established media; they are available to anyone in the community who follows the Palo Alto police via social media.

Social media has three sets of characteristics with key implications for law enforcement, according to a Harvard Kennedy School research report, Social Media and Police Leadership.

The **first** is the scope of social media, which continues to grow. Perron said his department’s social media outlets have thousands of followers compared to the handful of traditional media outlets that were interested in press releases issued by the Palo Alto PD.

The **second** characteristic is structure. Social media lets police have two-way conversations with the community. Palo Alto routinely receives messages from citizens via social media, including anonymous tips. Perron also conducts “virtual ride-alongs,” live-tweeting during an entire shift from an officer's patrol car. "It gives the public a great view of what we do and a better understanding of what's going on." Ultimately social media provides law enforcement a level of transparency it couldn't attain otherwise. When done correctly, the benefits are immeasurable, said Perron.

The **third** characteristic is tone. When the police use social media, they are having a conversation with their community; it's informal and quite distinct from traditional press releases. "We try to use a voice and tone that is cultivated and professional, but also human and sometimes humorous," Perron said. Corporate marketing campaigns have struggled to adopt that kind of human and humorous tone. But beat cops have a lot of practice talking directly to the community in an informal manner. For that reason, they have probably been more successful than other government agencies at engaging the public via social media.

Besides using social media as a two-way communications tool with the public and media, police also use Twitter and Facebook in investigations. Four out of five law enforcement agencies say they use social media for investigations, according to a 2012 survey by LexisNexis Risk Solutions.

The most common uses include: evidence collection — people are more than willing to brag about their actions on social media sites; location of suspects — one investigator "friended" a suspect and was able to track his location; criminal network investigation — again, people are prone to talking about their actions on social media sites, giving the police a window into their activities. The New York City Police Department found that 72 percent of its social networking use was by its detective bureau, investigating crime patterns and suspects, according to a 2013 report by the Police Executive Research Forum and the U.S. Department of Justice's COPS program.

But using social media has its challenges too. There's the cultural shift from a one-way form of communication with the public and media to one that is clearly two way now. Social media also can amplify, even distort information as it gets passed along. In addition, police departments must set policies as to who controls the information. In Palo Alto, Boston and elsewhere, social media content is centralized. But other agencies let individual police officers communicate through their own Twitter accounts.

For someone like Perron, who knows how hard it can be to manage social media, the problem is one of who monitors social media accounts when an officer is off duty? "Twitter is going 24 by 7. What happens if there's an emergency and no one responds?" he asked.

With more than 20 years of experience covering state and local government, ***Tod Newcombe*** *previously was the editor of* Public CIO*, e.Republic's award-winning publication for information technology executives in the public sector. He is now a senior editor for* Government Technology *and a columnist at* Governing *magazine.*

#EbolaFacts and #EbolaFiction on Social Media

Source: http://www.homelandsecurity.org/node/1425

Between Sept. 16th and Oct. 6th 10.5 million tweets mentioning the word "Ebola" were sent from 170 countries around the world.

Users of social media are spreading facts and misinformation, advocating for victims and squelching rumors about the Ebola outbreak.

Information about Ebola, both accurate and not, spreads faster thanks to social media. Trying to staunch the spread of bad information online shares many similarities with containing a real-world virus as users, "infected with bad information," then infect others.

Why do people post and rebroadcast jokes, rumors and dread of a distant disease that public health officials say is extremely unlikely to pose serious risk to the U.S.? The science behind how and why ideas spread on social media reveals that people tend to share stories that stir their deepest feelings, whether positive or negative.

But, social media can also can also be used to dispel rumors and disseminate accurate information. Two months ago the Centers for Disease Control and Prevention (CDC) took to Twitter to explain Ebola. Two months later the CDC hosted its second online chat about the virus, after it had claimed many more lives. In a sampling of questions under #CDCChat many users asked about an Ebola epidemic in the U.S., experimental drugs, and pets infected by Ebola.

In West Africa fighting the disease often means fighting misconceptions, refuting rumors, and working together with locals to disseminate accurate information through social media. Although Western experts have been reaching out to refute the rumors as well as change the information environment with new, accurate scientific information, locals who share, retweet, or host conversations with health experts are key to the process.

On Twitter, @EbolaFacts retweets information from the CDC and WHO and @EbolaAlert holds Twitter chats to debunk Ebola myths. Liberians have posted videos on YouTube on proper hygiene. In Sierra Leone social media is overtaking the radio as a source for news about Ebola. Residents have formed support groups online, advocated for experimental drugs for victims, and highlighted the importance of good hygiene. And in Nigeria #FactsOnEbola has been trending, with many users educating each other on the symptoms and prevention methods.

Why the terrorists shouldn't be stopped from tweeting

By Daniel Byman and Jeremy Shapiro

Source: http://www.dawn.com/news/1137175/why-the-terrorists-shouldnt-be-stopped-from-tweeting

The Islamic State mixes primitive savagery and high-tech sophistication. Its fighters behead and crucify while they post photos of a child holding a severed head and tweet about cats. Although the content is abhorrent and helps the Islamic State radicalise and recruit in the West, the group's massive social media presence is also useful to those fighting terrorism.

The Islamic State's public relations campaigns are slick, even hijacking seemingly benign hashtags such as #WorldCup2014 to propagate the militants' message. And the propaganda is issued in multiple languages — including English, French, Russian and Turkish — to appeal to potential followers. Some of this content is spread from the top ranks of the Islamic State, but the jihadists also have thousands of online followers who retweet messages and create their own content, enabling them to effectively crowdsource jihad.

Although such death videos nauseate most of the world, they make the Islamic State look cool to a key demographic: angry young Muslim men susceptible to indoctrination. Throw in a bit of sectarian hatred and a touch of promise about Islamic government, and the mix helps keep the Islamic State well supplied with impressionable foreign fighters.

On the other hand, the Islamic State's broadcasting of its brutality over social media makes it easier for people to support the United States and its allies' war with the militants, and it has sparked calls to block the jihadists from the internet. In the United States, sites such as Facebook, Twitter and YouTube remove some offensive comments linked to terrorism, with support from government agencies. British Prime Minister David Cameron has gone one step further, saying the time has come to be "intolerant of intolerance" and boasting of government efforts to take down thousands of internet pages.

How can democratic governments, with great concern for civil liberties and free speech, ever hope to impose their will on social media? In some cases, banning particular sites or individuals may make sense if the risk of recruitment and radicalisation is high. But those risks have to be weighed against the intelligence value of having groups such as the Islamic State active on social media.

Social media is a counter-intelligence nightmare for Islamic State militants. Although tweets and Facebook postings inspired them to fight and helped them get to Syria and Iraq, these technologies are easily monitored. As former FBI official Clint Watts points out, social media offers "a window into what's going on in Iraq and Syria right now". The same bragging the group did in Syria to inspire others can be turned against it: intelligence services can determine the identities of supporters and potential recruits, flagging individuals not previously on the government's radar.

With data analysis, governments can use social media to trace entire networks of contacts. A constant problem for intelligence services is detecting a terrorist before he acts. Now we have one good marker: the would-be terrorist is a "friend" or a "follower" of militants in Syria. The Carter Center, among many other organisations, has used online data to map the complex Syrian civil war with a level of fidelity that was never possible in previous conflicts. Intelligence agencies are putting it to similar good use.

At the very least, intelligence officers can learn the most prominent ways jihadists recruit others and try to counter them. At best, they can communicate with actual and potential terrorists, feeding information — and misinformation — to their networks.

Like political movements everywhere, terrorists have a message they want to communicate. But because every fighter can broadcast anything to the world, leaders cannot control the narrative. For example, the Islamic State is in a flame war with Jabhat al-Nusra, the official Al Qaeda affiliate in Syria: the contest makes both groups less appealing as it reveals divisions within the jihadist camp for all to see. According to European security officials we interviewed, this dissension turns off potential recruits.

If foreign fighters return home, they might find that they have incriminated themselves on social media. In most western countries it is illegal to join a designated terrorist group such as the Islamic State, but in the past it was often hard to prove that someone was a member of such a group. Tweets and Facebook pictures of fighters standing over dead bodies and declaring their allegiance to Islamic State leader Abu Bakr al-Baghdadi don't look good in a court of law.

Because the volunteers think they are heroes joining an army, they are not operating in a clandestine way. Despite Edward Snowden's leaks and other revelations about the power of the National Security Agency, terrorists seem to think that no one is listening — or that they don't care. As John Mueller, a senior fellow at the Cato Institute, told us, "We've had 13 years in which officials talk about how they listen to 'chatter' by jihadists, and yet the jihadists continue to chatter."

Beyond the debate about the wisdom of barring terrorists from social media, it may simply be impossible. Websites and Twitter accounts move and reappear as quickly as they can be taken down. Technological tools and methods quickly arise to circumvent controls — and those who most want to avoid scrutiny are the first to go underground. Even the Chinese government, with all of its vast apparatus and effort devoted to the Great Firewall of China, has not succeeded in completely cutting off protesters from using social media.

In most cases, social media promotes openness, collaboration, creativity and the spread of information. But when it comes to terrorism, social media is both disease and cure. It has helped the Islamic State recruit and grow, but it also strengthens the counterterrorism response and ultimately will weaken the group's message. Even though terrorists can exploit social media, these networks are an important source of our strength and our advantage over repressive groups such as the Islamic State.

***Daniel Byman** is a professor in Georgetown University's School of Foreign Service and the research director of the Center for Middle East Policy at the Brookings Institution.*

***Jeremy Shapiro** is a fellow in the Brookings foreign policy programme.*

The owners of Ebola.com want $150,000 for the domain

Source: http://factually.gizmodo.com/the-owners-of-ebola-com-want-150-000-for-the-domain-1645895875

There are a lot of different ways to make money in times of fear. A company in Nevada has apparently found their own way, now that more than 4,000 people have died from Ebola and the world is in a state of panic. **Blue String Ventures owns the domain name Ebola.com and they're offering to sell it for $150,000.**

"Ebola.com would be a great domain for a pharmaceutical company working on a vaccine or cure, a company selling pandemic or disaster-preparedness supplies, or a medical company wishing to provide information and advertise services," the president of Blue String Ventures, Jon Schultz, told CNBC via email.

www.ebola.com

Apparently Schultz bought the domain in 2008 with his business partner Chris Hood**. They're also the proud owners of BirdFlu.com, Fukushima.com, and PotassiumIodide.com,** among a host of others. Potassium iodide is a compound that would be used to fight radiation-induced cancer in the case of a bioterrorism or nuclear attack.

It could not be confirmed at press time whether Schultz and Hood's respective mothers were embarrassed that their sons were opportunistic pieces of human garbage who profit from the fears of others and contribute nothing of value to society.

Blackout? Robots can help

Source: http://www.homelandsecuritynewswire.com/dr20140926-blackout-robots-can-help

Big disasters almost always result in big power failures. Not only do they take down the TV and fridge, they also wreak havoc with key infrastructure like cell towers. That can delay search and rescue operations at a time when minutes count.

Now, **a team led by Nina Mahmoudian of Michigan Technological University has developed a tabletop model of a robot team that can bring power to places that need it the most.**

"If we can regain power in communication towers, then we can find the people we need to rescue," says Mahmoudian, an assistant professor of mechanical engineering–engineering mechanics. "And the human rescuers can communicate with each other."

Unfortunately, cell towers are often located in hard-to-reach places, she says. "If we could deploy robots there, that would be the first step toward recovery."

The team has programmed robots to restore power in small electrical networks, linking up power cords and batteries to light a little lamp or set a flag to waving with a small electrical motor. The robots operate independently, choosing the shortest path and avoiding obstacles, just as you would want them to if they were hooking up an emergency power source to a cell tower. To view the robots in action, see the video posted on Mahmoudian's Web site.

"Our robots can carry batteries, or possibly a photovoltaic system or a generator," Mahmoudian said. The team is also working with Wayne Weaver, the Dave House Associate Professor of Electrical Engineering, to incorporate a power converter, since different systems and countries have different electrical requirements (as anyone who has ever blown out a hair dryer in Spain can attest).

In addition to disaster recovery, their autonomous power distribution system could have military uses, particularly for Special Forces on covert missions. "We could set up power systems before the soldiers arrive on site, so they wouldn't have to carry all this heavy stuff," said Mahmoudian.

The team's next project is in the works: a full-size, working model of their robot network. **Their first robot is a tank-like vehicle donated by Michigan Tech's Keweenaw Research Center.** "This will let us develop path-planning algorithms that will work in the real world," said Mahmoudian.

The robots could also recharge one another, an application that would be as attractive under the ocean as on land.

During search missions like the one conducted for Malaysia Airlines Flight 370, the underwater vehicles scanning for wreckage must come to the surface for refueling. **Mahmoudian envisions a fleet of fuel mules that could dive underwater, charge up the searching robot and return to the mother ship.** That way, these expensive search vehicles could spend more time looking for evidence and less time traveling back and forth from the surface.

The team presented a paper describing their work, "Autonomous Power Distribution System," at the 19th World Congress of the International Federation of Automatic Control, held 24-29 August in Cape Town, South Africa.

— Read more in Nina Mahmoudian et al., "Autonomous Power Distribution System" (paper presented at the 19th World Congress of the International Federation of Automatic Control, 24-29 August 2014, Cape Town, South Africa)

Houston's Top Chefs Make Gourmet Emergency Rations

Source: http://www.emergencymgmt.com/disaster/Houstons-Top-Chefs-Make-Gourmet-Emergency-Rations.html

With canned peaches and tuna, marshmallows and Spam, professional chefs competed Saturday to show Houstonians that they can eat more than just peanut butter and jelly during a natural disaster.

Chef Kate McLean of Tony's won the 2nd annual Ready Houston Preparedness Kit Chef's Challenge at Market Square with a dish judge Albert Nurick said he "could see on the menu exactly as it is."

"The creativity is off the hook on this one," said Nurick, writer for the H-Town Chow Down blog.

On a fold-out table with a camp stove and average household cookware, McLean created a play on fish and chips. She and her competitors — David Grossman of Fusion Taco, Jonathan Jones of El Big Bad, Travis Lenig of Liberty Kitchen & Oysterette and Kevin Naderi of Roost — had 25 minutes to cook after lifting a tablecloth off a surprise stack of non-perishable items.

McLean seared canned tuna coated in crispy potato flakes. The fish cake sat in a Nutella gastrique made from the chocolate hazelnut spread, vinegar and powdered ramen seasoning. Atop that was a white marshmallow chip with blackened edges.

While Eric Sandler of CultureMap appreciated McLean's decision not to use Spam, unlike the rest of her competitors, he said it was certainly great hurricane cuisine, but not quite menu-worthy.

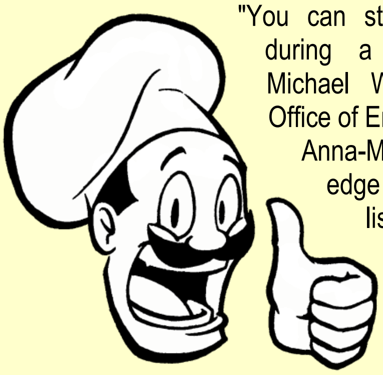
"It is quite good for the circumstances," he said.

Preparedness Event

About 50 people attended the event hosted by the City of Houston Mayor's Office of Public Safety and Homeland Security and the Houston Community Preparedness Collaborative. In patio chairs, they smelled marshmallows melting and saw the chefs arrange bias-cut slices of brown sugar-seared Spam over ramen noodles and broth.

Many earlier had peeked inside the Houston Fire Department's evacuation ambulance or stopped by a booth to pick up a bag filled with emergency phone numbers, a disaster preparedness list and "the Houston

Emergency Preparedness Cookbook."



"You can still have a good dessert during a natural disaster," said Michael Walter from the Mayor's Office of Emergency Management.

Anna-Megan Raley sat on the edge of a water fountain and listened to the judges describe how the chefs were preparing the dishes.

"I might use the cookbook just for regular cooking," she laughed. "I'm like a college boy. Just the basics."

Preparing in Advance

Raley, who lives nearby and said she frequents many Market Square events, said she appreciated the creative tack taken by the city to inform Houston about the need to prepare in advance for emergencies.

Her family home in Kemah "that had never had a drop of water in it" was torn away by Tropical Storm Allison in 2001, whose extreme flooding also killed 23 people.

"We didn't know whether to evacuate or what to do with the food we had," she said. "I am pretty sure all my high school trinkets and prom dresses are floating out there in the ocean somewhere."

How to Recruit, Retain and Organize Volunteers

By Margaret Steen

Source: http://www.emergencymgmt.com/training/How-to-Recruit-Retain-Organize-Volunteers.html

There are times during disasters when first responders will be overwhelmed and unable to do all that needs to be done without help from volunteers, who will do much of the work either in an organized fashion or spontaneously.

Volunteers are an important cog in disaster response, and developing a volunteer program before disaster strikes can be invaluable. It allows emergency responders to focus on some of the more major tasks as volunteers handle easier work like traffic control and light search and rescue.

Developing a volunteer program "saves lives and money," said Karen Baker, California's chief service officer and head of CaliforniaVolunteers, part of the governor's office.

A good volunteer program needs up-front planning and recruitment, and it needs to keep volunteers engaged in between emergencies. A first step for local emergency management professionals who think they need a volunteer program is to decide what they want volunteers to do.

"Some people just want to train the local community to be sure people know what to do in an earthquake [or other disaster]," said Suu-Va Tai, a disaster program specialist with CaliforniaVolunteers. "They're just training them — they don't see them again. They don't have the infrastructure for volunteers." Other departments need help regularly, not just during emergencies, he said. Especially when they have been hit hard by budget cuts, agencies may want volunteers to answer phones and do other routine tasks.

Whether just training locals or developing a program, it's important that it be defined as such. "You need a job description," said Dave Nichols, medical reserve and workforce deployment manager for Public Health of Seattle and King County, Wash. A big part of Nichols' job is managing volunteers, and he is also a volunteer with ShelterBox, a British nonprofit that responds to disasters around the world. "If you just recruit people and don't do anything with them, they'll disappear."

Nichols offered suggestions for where to find volunteers:

- Colleges and universities are good sources, especially if they have training programs for doctors, nurses, pharmacists and veterinarians — all people with skills that are valuable in emergencies.

- Churches and fraternal organizations like the Rotary or Lions clubs are also good places to ask: They have members who know the community and are often seeking opportunities to help others.
- Ask other emergency response groups such as the American Red Cross. “What might be a disaster for us, might not be a disaster for those groups,” Nichols said.
- Approach the private sector, since many companies match dollars for volunteer hours to encourage community service.
- Retirees are another good source — with the baby boomers leaving the workforce, there are a lot of skilled people who may be interested in volunteer opportunities.

After developing a roster of volunteers, it’s important to train them to the job description, perform background checks on those who may end up working in situations where that’s necessary like a hospital, and create a database to keep track of them.

Ideally every participant is an affiliated volunteer — signed up, given a background check and trained in certain areas, said Barbara Nelson, a community educator with Pierce County Emergency Management in Washington. Nelson’s office also tries to associate volunteers with agencies or organizations that can use their help. “For example, when we have donations in our county, the Salvation Army is in charge of that,” she said. “We can support them with people trained to support them.”

Shelter volunteers work with a variety of groups, including churches that open emergency housing when necessary. “All of these people are background checked, and they’ve had specific training for how to open a shelter,” Nelson said. “We know where they’re from and what their capabilities are, and we can put them to work right away.”

Once the list of volunteers is developed, it’s also important to keep participants engaged. If volunteers are recruited for just a one-time event, they may not respond the next time unless they’re continually engaged, Tai said. “You need to find different activities to engage with them and keep them training.”

Nichols’ program includes a reserve corps of 700 active volunteers who are used frequently in the community. About half are medically licensed, and the rest are support volunteers who can handle logistics. To become a volunteer, a person must attend an orientation and take two FEMA courses. Then, after a background check, they receive a badge and vest that identify them as volunteers.

Nichols’ department uses volunteers to test its ability to handle mass vaccinations by giving flu shots to the uninsured. He also calls on volunteers to support the American Red Cross when it opens a shelter.

“I spend a lot of time trying to find things for my people to do, not make-work but real stuff,” Nichols said. “That keeps them engaged, plus it adds people to our pool.”

It’s helpful to have volunteers working regularly, and it’s crucial to know both how to activate the volunteers and what they will do when disaster strikes.

California is developing a statewide Disaster Volunteer Network, an online tool to help local programs manage their volunteers. “If you’re an emergency manager at a county level who wants to understand the footprint of Spanish-speaking CERT volunteers that have had training in traffic control, you can find out,” Baker said.

Debbie Goetz, community planning coordinator with the Seattle Office of Emergency Management, said her office coordinates volunteer ham radio operators. In case of disaster, a few of them are designated to report to the EOC, where they will receive information from others in neighborhoods around the city. “They would start doing field reporting,” Goetz said. Looking for problems with bridges and the transportation system, for example, or places where large-scale rescues are needed.

Nichols’ office uses the WAserv (Washington State Emergency Registry of Volunteers) Web-based system to reach volunteers, though they must have Internet access to see it. The organization also is creating a plan to use ham radio operators to contact volunteers if necessary.

It’s important to plan realistically, as well. “In a catastrophic event, we expect not to have 700 volunteers — some will be affected by the event and some will be out of the area,” Nichols said.

In addition to the volunteers who were scheduled but can’t make it to help, there will be spontaneous volunteers who show up. Their motives are good, and in the right situation they can be helpful. But they can also create complications and be a distraction during the middle of an emergency, which is not the time to figure out who people are. However, since these volunteers are inevitable, it's important to think through what they will be able to do and have a plan for that. For example, spontaneous volunteers are perfect for certain jobs, such as filling sandbags and clearing rubble, where a background check isn't necessary.

The effort invested before an emergency is invaluable. "We spend a lot of time and effort trying to get people signed up ahead of time," Nichols said. His office is working with local hospitals to develop a system so that emergency workers could recognize hospital employees' badges and know which badges mean the person has had the proper background checks.

One way to handle volunteers is to set up a reception center. Ideally the center should be away from the area impacted by the disaster, so volunteers can be organized and assigned to appropriate jobs before being bused to the site, according to Nelson. "When you have a situation where you have a lot of people coming in and offering to help and you don't have any idea who they are or what their capabilities are, that's when we open a volunteer reception center."

Plan for Success

Beyond initial planning and recruiting, experts offer these tips for creating a successful volunteer program:

Affiliate with statewide or other organizations. The first responders to a disaster are local, with the state providing resources when local resources can't meet the needs. CaliforniaVolunteers has a seat in the state operations center, said Karen Baker, chief service officer for California. She leads CaliforniaVolunteers, and it can help mobilize extra resources for a community in need. "The state has your back, because it can tap volunteers in the community or in a neighboring community to immediately come to the aid of fellow Californians," Baker said.

Make local connections. Barbara Nelson, a community educator with Pierce County, Wash., Emergency Management coordinates efforts not only of official volunteers but also of local organizations, including the Red Cross, the American Legion and churches that respond to disasters. "We started at that point of trying to identify who is available with what sort of resources," said Nelson. "We wanted to make sure we did this in an organized way."

Don't overpromise. "If the bottom line is that you need help with data entry and traffic control, and you recruit someone to become part of the fire team, you're going to attract someone who's going to want a high activity level when you want administrative support," Baker said. "Don't do false advertising — be accurate with what kind of volunteer experience you can promise, deliver and support."

Learn about liability. Volunteer coordinators should learn what the laws are in their state regarding liability coverage for volunteers who are injured while helping in a disaster, said Suu-Va Tai, a disaster program specialist with CaliforniaVolunteers. With proper training, they can assess the need for waivers or additional insurance.

Track volunteers' hours. Knowing how much time volunteers put in helping after a disaster can be helpful later on, because they can be translated into local hours and count toward federal matching funds, Nelson said. It helps to have detailed sign-in and sign-out sheets, and also to document what the volunteers are doing so an hourly rate can be assigned.

Use volunteers for a variety of activities. "It's important that you don't create a response junkie; you are going to need them in all phases," Baker said. "Ensure your volunteers understand out of the chute that they are going to be needed for a variety of tasks."

Show volunteers they're appreciated. "If you have a great volunteer coordinator, you will be amazed at the lengths volunteers will go to for that person," said Tai.

Margaret Steen is a contributing writer for Emergency Management magazine.

Confronting the Challenges of Evacuating People with Disabilities

By Deborah Hayes

Source: http://www.emergencymgmt.com/training/Challenges-Evacuating-People-with-Disabilities.html

In 2013, the United Nations Secretary-General's Special Representative for Disaster Risk Reduction, Margareta Wahlström, noted that people with disabilities experience a disproportionately high level of disaster-related injury and death because their needs are neglected by the official planning process in most situations.

The UN conducted a survey of people with disabilities who had survived disasters around the world. Few respondents were aware of any disaster management plans in their communities, and fewer had participated in any planning processes, although half of the respondents expressed a desire to do so.

According to survey respondents, just 20 percent said they could evacuate "immediately without difficulty" in the event of a sudden disaster. If "sufficient" time were available, the percentage of those who could evacuate without difficulty nearly doubled (to 38 percent), underscoring the need for effective and inclusive early warning systems. There is no reason to believe that the situation in the U.S. is substantially different than the one highlighted in the UN report.

According to a report issued by the U.S. Census Bureau in 2012, about 56.7 million people, or approximately 19 percent of the population, had a disability in 2010. Of those individuals who reported having a disability:

- **About 7.6 million people experienced difficulty hearing, including 1.1 million whose difficulty was severe. About 5.6 million used a hearing aid.**
- **Roughly 30.6 million had difficulty walking or climbing stairs, or used a wheelchair, cane, crutches or walker.**
- **About 19.9 million people had difficulty lifting and grasping. This includes, for instance, trouble lifting an object like a bag of groceries or grasping a glass or pencil.**

This means that in any disaster planned for by emergency management personnel, one in five people encountered will have a disability of some type. Studies after Hurricane Katrina found that approximately one-third of those who did not leave their homes during the disaster had a disability. In fact, when survivors were interviewed after the storm, the two primary reasons given for not evacuating were either the person had a disability or was a family member of someone with a disability and stayed behind to act as a caretaker. One of the lessons learned from Hurricane Katrina and other recent disasters is that the special needs of people with disabilities must be integrated into all aspects of emergency management.

So how does an emergency manager plan for the evacuation needs of disabled persons in the community?

Become familiar with planning tools that have already been developed by reputable organizations, such as the National Organization on Disability

The organization's guide, titled *Functional Needs of People with Disabilities: A Guide for Emergency Managers, Planners and Responders*, is a step-by-step how-to document on all aspects of planning for emergency managers and the people in their communities who have disabilities.

Include representation by the disabled community throughout the planning process

Evacuation planning should include representation by community members who are disabled. This process will help establish a strong working relationship with the community before a disaster occurs. This involvement can also assist the emergency manager in identifying organizations or resources within the community that are already used by individuals with disabilities. These organizations can in turn disseminate information that will aid people with disabilities to assume a role in determining their own needs and therefore take on some of the planning responsibility for their needs.

Identify the needs of the community
Working with the disabled community in the planning process also allows the emergency manager to identify areas of need, particularly in the two most challenging aspects of evacuation: communication and transportation. Community organizations or agencies that represent the varied needs of the disabled population can assist in getting access to information about people with disabilities and where they live. This information can aid the emergency manager in getting a clearer picture of this segment of the community.

Self-identification and preparation
People with disabilities should have a means by which they can self-identify. Some methods have been shown to be successful, including: registration with the local emergency management department; pre-made emergency go bags or the provision of information about specific emergency information readily available for the community; and an emergency notification system for people who might need assistance to be informed promptly in the event of a disaster.

Develop a list of resources to assist people with disabilities
This list must be maintained and updated to reflect information and resources as they exist. Additionally, this list must be made available to organizations and individual members of the community who have disabilities.

Train first responders in the needs of persons with disabilities
Many first responders aren't familiar with the specific needs of disabled people. Providing training to first responders using community members will heighten awareness and allow the responders to find out firsthand what needs might arise in the event of a disaster.

Build strong relationships with government agencies that work with disabled people
Emergency managers should develop relationships with government entities that regularly work with people who have disabilities. This will allow learning in both directions and help pinpoint potential problems before they occur. Such organizations should also be involved in the planning and information dissemination process as they are usually aware of community resources that might be unknown to the emergency manager.
With careful planning incorporating input from a broad spectrum of the community, emergency managers can make better decisions. These decisions will lead to a smoother evacuation, as well as fewer injuries and deaths.

***Deborah Hayes** has worked in emergency management and disaster response for more than 10 years for various organizations, including the American Red Cross, FEMA and the International Federation of Red Cross and Red Crescent Societies. She completed her Ph.D. in architecture from Georgia Tech examining building safety issues.*

Risk Perception Analysis Can Help Authorities Understand How People Interpret, Respond to Crises

By Kylie Bull (Managing Editor HSToday.US)

Source: http://www.hstoday.us/single-article/risk-perception-analysis-can-help-authorities-understand-how-people-interpret-respond-to-crises/1303916e7d69cb9725a9e0e6822d5e0f.html

Is it possible that people who have survived a disaster, be it natural or man-made, are able to perceive the risk of the same or another disaster occurring more than a person who has not experienced disaster? A German/UK study involving more than 1,000 disaster survivors finds that they are.

Those who have experienced events such as an earthquake, flood or terrorist attack have a heightened perception of the risks posed by these, and, in some cases, unrelated risks. The study, which included participants from seven European countries, points to the importance of risk perception analysis in helping governments and others understand how people interpret and respond to crises.

Risk perception researcher Daniela Knuth, along with two colleagues from the University of Greifswald, Germany, and Lynn Hulse from the University of Greenwich, United Kingdom, outlined how experience and "objective risk" affect risk perception. They define "objective risk" as the likelihood of the average person experiencing emergency events and their negative consequences.

In their paper, *Risk Perception, Experience and Objective Risk: A Cross-national Study with European Emergency Survivors*, published in the journal, *Risk Analysis*, the authors focused on "involuntary, memorable events," and administered a questionnaire to gather data on whether experience with a particular hazard will lead to elevated risk perceptions for this hazard. Based on their findings, they concluded that "experience with a particular hazard was one of the most important predictors of perceived risk of the same hazard." This effect was most clearly seen for people who had experienced floods, mainly in the Czech Republic, where 91.7 percent of respondents recalled floods, Germany (85.7 percent) and Poland (61.5 percent). It was also strongly seen for earthquake survivors, mainly from Turkey and Italy, where almost half of these earthquakes occurred in the last 30 years.

Knuth told *Homeland Security Today* she believes there are different explanations for elevated risk perceptions. "In the context of assessing risks, the availability heuristic [a mental shortcut that relies on immediate examples that come to mind] gives one explanation," she said. "It suggests that risk judgments depend on the possibility and the ease with which events can be recalled when making judgments about risks. Direct experience in that case makes the recall of such an event easier and leads to higher ratings."

In exploring whether experience with one hazard will elevate the perceived risk from at least some other hazards, the researchers found evidence of such "cross-over effects" in risk perception. For example, experience with a public fire not only increased perceived risk of a public fire but also perceived risk of a terrorist attack. Furthermore, experience with a public fire and a terrorist attack increased perceived risk of a traffic accident, possibly because all three events share a common context of occurring in public settings.

"We hypothesized that the context of disaster experiences might play a crucial role," Knuth said. "Thus, if a person had experienced an emergency before in a building (or outdoor space) that was not so familiar, surrounded by lots of people who also might not have been so familiar, with a place of safety and comfort some distance away, they might have been able to easily picture themselves in those circumstances again when imagining the context of the non-experienced events."

The researchers also focused on how "objective risk" influences risk perception. They found that the objective risk of earthquakes and terrorist attacks most strongly influenced perceived risk. For example, in Turkey and Spain, where such risks were the highest, people's perceptions reflected the statistical likelihood of experiencing these emergencies.

This led the researchers to examine whether different countries would exhibit differences in perceived risk -- and that's what they found. Perceived earthquake risks differed most markedly, followed by perceived risks of terrorist attacks and floods. The researchers concluded that perceived risk for all events was significantly influenced by country of residence, although the extent of the influence differed across events. For example, respondents to the risk perception questionnaire scored high across perceived risks in Turkey, where earthquakes and terrorist attacks are experienced more frequently, as are traffic accidents. However, in all seven countries, the risk of domestic and public fires was perceived similarly, even though objective risks differed, possibly because such events receive little nationwide media attention and therefore governments and other agencies have less need "to publicize objective information as a counteraction."

Knuth believes the media plays a very important role in risk perception, and said this role is also important for the factor of fear.

"First of all," she said, "the media makes indirect experience possible. We can see or read about the impact of different disasters in the media. The effect of media can be tricky since very rare events are sometimes over-represented, whereas very common events are under-represented. This can lead to differences in perceived risk. Therefore I would hypothesize that someone without any access to media would have a different level of risk perception concerning some events than someone with media access, even if they both experienced a disaster event. Fear might be an important factor in perceived risk since the factor of dread is especially important concerning the judgments of people. The higher the dread associated with an event, the higher the perceived risk for this event."

Homeland Security Today also asked Knuth whether the survivors' disaster perception would be expected to increase, decrease or stay the same over time.

"We are not sure about that, but this is a very interesting point," Knuth said. "Further analyses of a different sample revealed that especially concerning flood risk perception; time might be a crucial factor (i.e.: a negative relation between the time elapsed since the event and perceived risk). It is possible that the effect of heightened risk perception concerning an experienced event will decrease in time. Especially if preventive measures were taken in order to avoid further events, it might be the case that risk perception will decrease after a period of time without direct experiences (e.g.: suggesting that preventive measures are working)."

Another recent study published in *Risk Analysis* also tackled key aspects of risk perception. In the paper, *An Assessment of Change in Risk Perception and Optimistic Bias for Hurricanes Among Gulf Coast Residents*, Craig Trumbo of Colorado State University and four other colleagues evaluated the level of concern about hurricanes following the two year quiescent period after Hurricane Katrina. The researchers used data from 201 questionnaires that were returned at the beginning and end of the two year period by residents living in 41 counties immediately adjacent to the Gulf Coast.

The data were mixed regarding the effects of income, education and other demographic variables on risk perception. But overall, there was a significant drop in the level of hurricane risk seen by the residents. The researchers concluded that risk communicators and emergency managers should work to counter the public's tendency to become complacent about coastal hurricane risks after a quiet period following highly destructive events.

The findings from these studies come at a time when emergency management officials are seeking to communicate with the public about the need for greater awareness of risks ranging from hurricane flooding and increased forest fires to terrorist attacks and climate change.

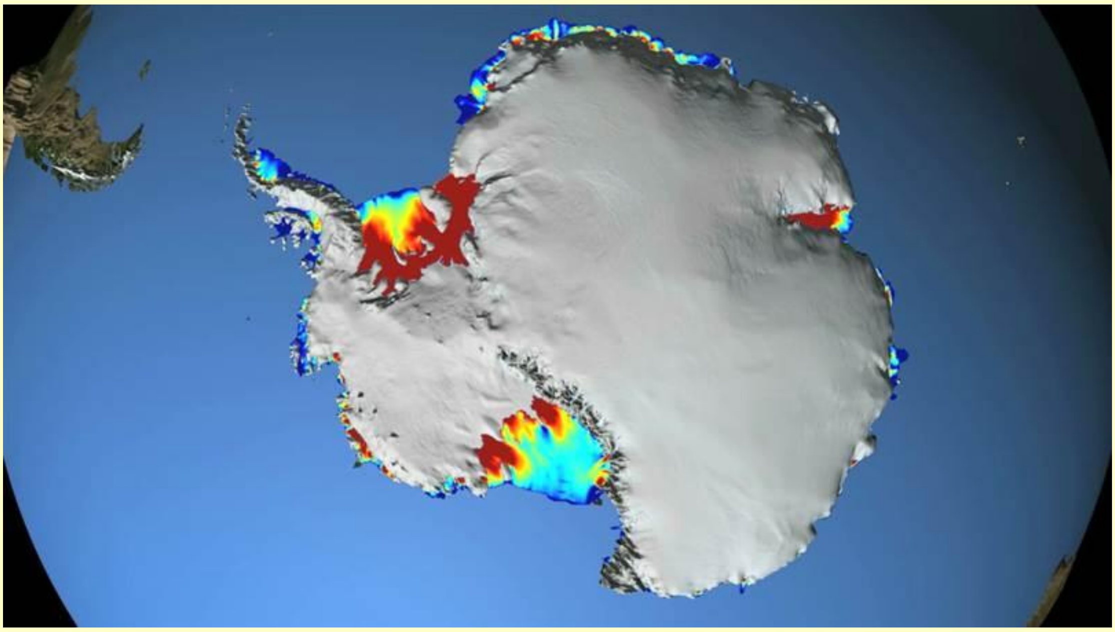
It would be beneficial for such research studies to continue, and perhaps to run alongside public awareness campaigns in order to glean more understanding into this phenomena and how it may develop over time with varying environmental factors.

Warnings from a warming ocean

Source: http://www.homelandsecuritynewswire.com/dr20141001-warnings-from-a-warming-ocean

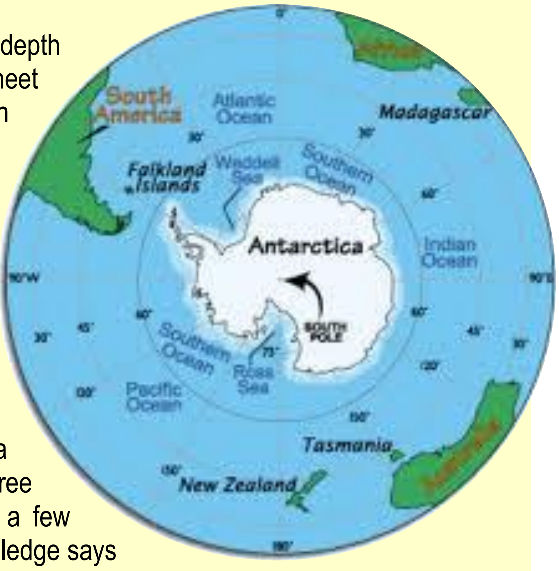
Using geological data to verify their model results, scientists found that when the ocean around Antarctica became more stratified, or layered, warm water at depth melted the ice sheet faster than when the ocean was less stratified. A dramatic example of this process occurred around 14,000 years ago, and led to an abrupt rise in global sea level of nearly three meters over just a few centuries.

Dr. Nick Golledge, a senior research fellow at Victoria's Antarctic Research Center, alongside a team of scientists from Victoria University, GNS Science, and the University of New South Wales in Sydney, is trying to understand the way that the Antarctic ice sheet responds to ocean warming.



A Victoria University of Wellington release reports that together they used sophisticated ice sheet and climate models to recreate the Antarctic ice sheet as it came out of the last ice age, when both the ocean and the atmosphere warmed quickly.

The results, published in *Nature Communications*, suggest that oceanic changes might trigger a significant shift in the stability of the Antarctic ice sheet, which Dr. Golledge says could lead to an increase in global sea level.



Using geological data to verify their model results, they found that when the ocean around Antarctica became more stratified, or layered, warm water at depth melted the ice sheet faster than when the ocean was less stratified.

A dramatic example of this process occurred around 14,000 years ago, and led to an abrupt rise in global sea level of nearly three meters over just a few centuries. Dr. Golledge says current oceanographic observations around Antarctica show the ocean is once again becoming more stratified.

"At the surface the water is getting colder and less salty, with more extensive sea ice occurring in some areas. But the deeper ocean is warming, and is already accelerating the decline of glaciers such as Pine Island and Totten," he says.

"Whether the ice sheet will react to these changing ocean conditions as rapidly as it did 14,000 years ago is unclear, but with 10 percent of the world's population living less than ten meters above present sea-level, this study highlights the need to better define the complex relationship between Antarctica and the Southern Ocean.”

— Read more in N. R. Golledge et al., “Antarctic contribution to meltwater pulse 1A from reduced Southern Ocean overturning,” Nature Communications *5, Article number: 5107 (29 September 2014)*

Asymmetric Warfare Goes Both Ways

By Eric Jorgensen

Source: http://ciceromagazine.com/opinion/asymmetric-warfare-goes-both-ways/

During the last decade and a half of militant extremism with global ambitions, asymmetric warfare has been a much-ballyhooed concept sometimes alleged to give the weaker belligerent an inherent, automatic advantage. But this is a gross oversimplification, and when it takes root in the minds of those threatened by and opposing terrorism, it can become a self-defeating distortion of the truth. Asymmetric warfare goes both ways in conflicts between peers, near-peers, and non-peers alike; and the U.S. and our global partners should constantly be using innovative asymmetry to our own advantage, in every contest of wills we face.

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines *asymmetric* like this: “In military operations the application of dissimilar strategies, tactics, capabilities, and methods to circumvent or negate an opponent’s strengths while exploiting his weaknesses.” Asymmetric warfare is nothing magical. The application of dissimilar strategies, tactics, capabilities, and methods is commonsense common practice in every kind of competition, including armed conflict, and it always has been.

Since that is true, it is striking that JP 1-02 had no definition of asymmetric at all until the definition was first introduced in 2012’s brand new JP 3-15.1, *Counter-Improvised Explosive Device Operations*. JP 3-15.1 is a doctrine document produced only after terrorists and insurgents in Iraq and Afghanistan had demonstrated both the ingenuity and the capability to develop and employ improvised weapon systems whose strategic effects sometimes far surpass their tactical impact, despite relatively small investments. But the fact that it took that painful experience to add the word asymmetric to our military lexicon should tell us that we are selling ourselves short, even if it is only because we have gotten too comfortable thinking of ourselves as the biggest kid on the block and the odds-on favorite.

How then should the U.S. use asymmetry to our advantage regardless of the type of adversary we face? Going bigger and better with our military forces, even at high cost, is clearly part of the answer. It is also clearly not the entire answer, and it comes with stringent fiscal limits of late.

Iraq and Afghanistan were the proving grounds for a new generation of IED tactics, including the way in which IED attacks have been staged, recorded, and then broadcast for all the world to see. Those tactics allowed Al Qaeda and the Afghan Taliban to deliver their own version of “shock and awe,” with devastating direct results for far too many of our American warriors and troubling indirect results for all Americans watching. The barbarous recordings of the beheadings of one civilian at a time are intended to have the same asymmetric strategic impact. How should we respond? By fighting our enemies just as asymmetrically as they fight us.

Asymmetry and The American Way Of War

In his groundbreaking 1973 book by the same name, Russell Weigley described *The American Way of War* as one of attrition and annihilation. During the Revolutionary War, Americans fought from a relative absolute position of weakness, and had to apply lots of asymmetric creativity to do that. Increasingly, however, Americans have been able to fight from a relative absolute position of strength, in a way that has overwhelmed the ability of our enemies to fight back. But even this is asymmetric, whether we call it that or not. In that transition from weakness to strength and beyond, Americans first relied on the sheer asymmetric weight of *numbers* pushed out by a logistics machine with no equal. Think World Wars I and II. Later – and outside the scope of Weigley's treatise – Americans relied on the sheer asymmetric superiority of *capabilities* pushed out by that same machine. Think Gulf War I, and especially the early stages of Gulf War II.

When writing about what he called "*The New American Way of War*" in the summer of 2003, after watching the successful coalition invasion of Iraq, Max Boot said the true genius of U.S. forces that spring had been their creative ability to leverage the benefits of superior American technology, often by improvising on the spot, but all the while as part of a combined arms network. Boot explained how that kind of transformational military cost more than legacy forces, but argued that the improved effectiveness of an increasingly better integrated Joint military team makes it worth the investment.

Part of the beauty Boot saw in this new way of war was its ability to win quickly, with minimal casualties on both sides. "Total war" was no longer necessary. Attrition and annihilation were reserved for the opposing military forces American and coalition forces couldn't quickly negate or avoid altogether. But the invasion's initial success was more a result of the specific new kinds of asymmetric advantages we had over the opposition we faced at that specific time than it was a result of choosing a new way of war. In fact, the insurgency that followed the invasion drove American forces back to the bloody slogging which Boot said our military had eschewed; and even after a great deal of effort to squash that insurgency, we are facing the same thing again, in the same place, and worse.

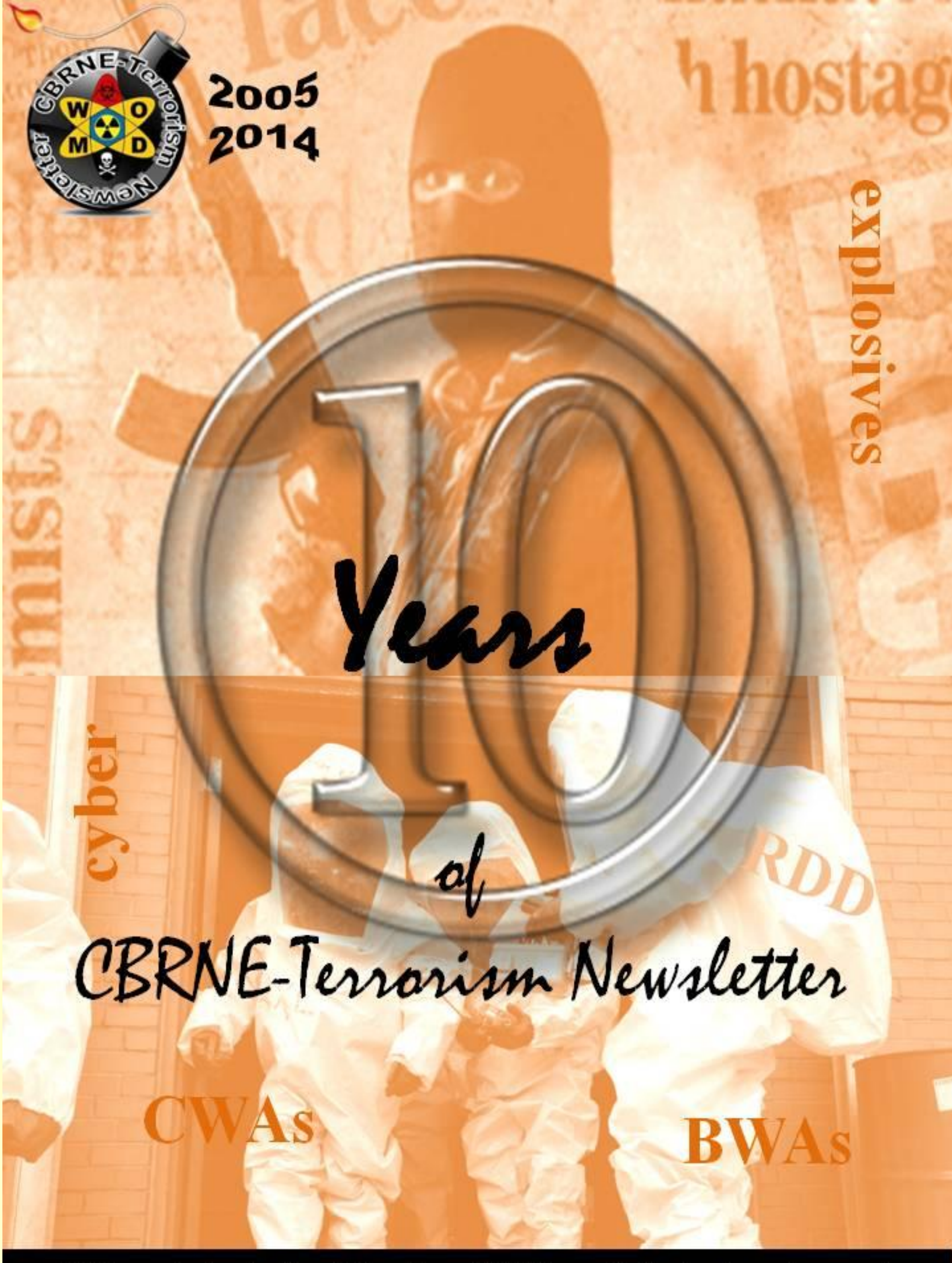
Using Asymmetry to our Advantage

How then should the U.S. use asymmetry to our advantage regardless of the type of adversary we face? Going bigger and better with our military forces, even at high cost, is clearly part of the answer. It is also clearly not the entire answer, and it comes with stringent fiscal limits of late. Even General Mike Hostage, commander of the Air Force's Air Combat Command and perhaps the world's most impassioned proponent of the extremely capable but high-priced F-35, has said we need to flip the cost imposition formula, so that our adversaries are spending a million dollars to defend against our five dollar weapons, and not the other way around. As a point of reference, see this informative article on "*Asymmetric Power in Advanced Weapons*" for a taste of what is possible in military capabilities that won't break the bank.

As we strive to fight our enemies just as asymmetrically as they fight us, we will keep an eye toward reducing the military costs while simultaneously improving the results. But, more importantly, we will work to extend the network praised by Boot far beyond the military – before, during, and after each occasion when we decide we must unfortunately engage in military combat. We need to build that network to take asymmetric advantage of the full range of U.S and partner nation instruments of national power, in a way that overwhelms our adversaries – and, whenever possible, we should strive to do that without any resort to military action at all. This means applying the best minds not only to careful cultivation of high-tech military capabilities, but to the fully engaged, cross-functional and proactive management of our national security challenges at every level.

Asymmetric warfare that plays to the full range of American strengths will be about much more than warfare. Having a silver bullet is awesome. Having a silver bullet made out of copper is even better. Having a silver bullet made out of copper that's not a bullet at all is better again.

*After retiring as an Air Force colonel in 2013, **Eric Jorgensen** served the National Commission on the Structure of the Air Force as a Senior Research Analyst. In his final military assignment, he was Chief of the Total Force Enterprise Management division in the Air Force Directorate of Strategic Planning in the Pentagon. He is a pilot with more than 4,000 military flying hours in aircraft including the F-111F, the F-15E, and the KC-135R.*



2005
2014

10 Years of CBRNE-Terrorism Newsletter

WE have to be lucky all the time. THEY have to be lucky only once!