December 2014

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders

10 years

Nuclear war, the black swan we can never see

By Seth Baum

Source: http://thebulletin.org/nuclear-war-black-swan-we-can-never-see7821

Several centuries ago in England, the black swan was a popular symbol for the impossible because no such creature had ever been seen. Then came the surprise: Black swans were discovered in Australia. Since then, the bird has symbolized that which seems impossible but can in fact occur. The black swan reminds us that believing something cannot happen is often just a failure of imagination.

Parts of society today hold the same view of nuclear war that society in England did of black swans centuries ago: No nuclear war has ever been observed, so it may seem impossible that one would occur. Though nations possess some 16,000 nuclear warheads, deterrence just seems to work. And so, especially with the Cold War a fading memory, attention has shifted elsewhere. But it is just as much of a mistake to think that nuclear war couldn't happen now as it was to think that black swans couldn't exist back then.

It is true that, in any given year, nuclear war is unlikely, but the chance of it happening is not zero. Stanford professor emeritus Martin Hellman has a great way of explaining the risk. He compares it to a coin of unknown bias, flipped once a year for every year since the first Soviet nuclear weapon test in 1949. For 65 years, the coin has always landed on heads. If the coin had always landed flat on heads, we might think the probability of tails was close to zero. But in some years, the coin has teetered on its edge before falling on heads. Given this, should we still think the probability is near zero?

We have, after all, witnessed many teetering-on-the-edge moments. On October 27, 1962, during the Cuban missile crisis, the United States targeted the Soviet submarine *B-59* with depth charges. Two out of three Soviet officers wanted to launch the submarine's nuclear weapons in response, but launch procedures required agreement between all three. On January 25, 1995—after the Cold War—Russian radar detected the launch of a scientific weather rocket over the northern coast of Norway, and radar operators suspected it was a nuclear missile. Yeltsin and his associates decided not to launch a nuclear weapon in retaliation, correctly guessing that the rocket was not actually an attack. And from May to July of 1999, India and Pakistan fought a war over the Kargil district of Kashmir. Both countries already had nuclear weapons, which might have been used had the war escalated.

Calculating the odds

How does one go about estimating the annual probability of nuclear war—that is, the likelihood that it will occur during any one-year period? It is important to think in terms of probabilities per unit of time. The probability of nuclear war occurring next year is smaller than that of it occurring in the next decade. But the longer we wait, the more likely it is to occur. If the probability of nuclear war occurring in one year is, say, one in a thousand, then there will probably be a nuclear war within the next thousand years.

For certain kinds of events, one could figure out annual probabilities by looking back at history to see what portion of previous years had witnessed the events in question. But this doesn't work for nuclear war. To take this backward-looking approach would be as though people in England hundreds of years ago had looked at their own historical experience to calculate what portion of swans were black.

To start calculating the odds, my colleagues and I studied one specific type of scenario: inadvertent nuclear war between Russia and the United States, in which one side mistakenly believes it is under attack and launches what it believes to be a counterattack but is actually a first strike. We found that the chance of such a war occurring during any given year is anywhere from about one-in-a-hundred to about one-in-a-hundred-thousand, depending on various assumptions. The total

annual probability for all types of nuclear war will be larger than this, possibly much larger.
My colleagues and I estimated the probability of an inadvertent Russia-United States nuclear war by modeling the steps involved in going from a false alarm to a launch in response. When alarms are received, they are passed up the chain of command, receiving greater scrutiny at each step as officials decide whether the event in question poses a true threat. Only if the news reaches the top—in the United States that means the president—will weapons be launched in retaliation.
There is some publicly available historical data for how often false alarms have occurred and how far up the chain of command they've gone (other data is classified). We used as much historical data as we could find, but this still leaves a lot of uncertainty. We considered a variety of assumptions about how the uncertainty might be resolved, which is what gave us such a wide range of possible annual probability estimates. For example, it is unknown how often there are false alarms that could be perceived as nuclear attacks, so we considered a range of 43 per year to 255 per year based on data from 1977 to 1983. While there is no guarantee that the false alarm rate is still in that range (this information is classified), the range at least gives a sensible starting point.

Close calls

The fact that no nuclear war has ever happened does not prove that deterrence works, but rather that we have been lucky. What if the third officer on *B-59* had felt differently about launching the submarine's nuclear weapons? What if the Norwegian rocket incident had happened during a US-Russia crisis? What if India and Pakistan could not resolve the Kargil conflict so readily? Accidents happen. In 2013, during the brief period when the United States was threatening military intervention in Syria, Israel launched missiles from the Mediterranean towards its own coast to test its missile defense systems. Russian radar detected the launch. Israel cleared up the confusion before any damage was done, and no nuclear weapons are believed to have played any role in the incident. But it demonstrates the sorts of quirky perils we must still live with.
Likewise, looking around at current geopolitics, it should be clear that nuclear war is no less likely than it ever has been since the invention of the atomic bomb. Consider some of the states known to possess nuclear weapons: US-Russia relations may be worse now than they were in 1995, thanks to disagreements regarding Ukraine. India and Pakistan certainly have not resolved all their differences. China has its individual differences with India, Russia, and the United States. And Israel and North Korea are not exactly at peace with their neighbors.
While nuclear war is like a black swan, though, there is a critical difference between the two: Black swans don't kill massive numbers of people. We can observe black swans and live to tell about it, but the same cannot necessarily be said of nuclear wars. Our continued existence may depend on the fact that one has never yet occurred. Nuclear war is the black swan we can never see, except in that brief moment when it is killing us. We delay eliminating the risk at our own peril. Now is the time to address the threat, because now we are still alive.

Seth Baum *is executive director of the Global Catastrophic Risk Institute, a nonprofit think tank that Baum co-founded in 2011. Baum's research focuses on risk, ethics, and policy questions about major threats to human civilization, including nuclear war, global warming, and emerging technologies.*

How does religion really influence Iranian nuclear policy?

By Ariane Tabatabai

Source: http://thebulletin.org/how-does-religion-really-influence-iranian-nuclear-policy7820

One of the most enduring myths about post-revolutionary Iran is that the country's policies, including those on nuclear matters, are shaped by its leadership's obsession with martyrdom and Messianic ideals.

Many observers, especially in the arms control community, base their analyses on this notion, and it leads to some harrowing conclusions. If, after all, a country's stance is basically suicidal, there's no telling what it would do with a nuclear weapon. A careful and more nuanced look at the role of religion in Iranian decision-making, though, debunks the idea that martyrdom rules in Tehran, and gives a much more realistic basis for understanding the regime's behavior.

To be sure, there are reasons why some analysts see the Iranian government as driven by martyrdom. The idea originated with the 1980-1988 Iran-Iraq War, which helped shape the Iranian psyche and the image of the Islamic Republic in the world. During the war, Iran famously launched a series of "human wave attacks," sending untrained and unprepared men (and occasionally boys) to the front, sometimes through minefields, to clear the way for the trained forces. This tactic went hand-in-hand with the notion of martyrdom, with members of this ill-equipped vanguard promised a place in paradise if they gave their lives for God and country. Mental images of young boys wearing plastic "keys to paradise" around their necks and running across minefields have haunted the war's observers, and though whether such keys actually existed remains controversial, the picture lingers and contributes to perceptions of Iran.

Much later, former President Mahmoud Ahmadinejad probably encouraged the notion of martyrdom's importance in politics with rhetoric deemed bizarre. For instance, in 2005 he said that some delegates at the United Nations General Assembly had seen a "halo" around his head. During his 2005-2013 presidency, Iranians joked that Ahmadinejad would always put out an extra plate at his table for the "Mahdi."

Shia Muslims believe that the Mahdi, born in the ninth century and also known as the Hidden Imam or the Twelfth Imam, is the Prophet Mohammed's last legitimate successor. They believe that he has gone into occultation—the state of being blocked from view—but will eventually return, much as Christians believe that Jesus Christ will return some day. According to Shia belief, the Hidden Imam will reappear along with Christ and together they will restore peace and justice, saving the world from the chaos into which it would otherwise descend.

The notions of martyrdom and "Mahdism" have led many to extrapolate that the Iranian leadership's actions are governed by an inherent suicidal tendency and a willingness to cause chaos, even if it's self-destructive, in order to facilitate the Mahdi's return. But if one goes beyond the revolutionary rhetoric and examines the Islamic Republic's actions, one realizes that more often than not, Tehran is driven by national or regime interests, rather than pure ideology and belief. In fact, Iran's rulers often use ideology as a means, and do not see it as an end. It's true that the regime sometimes makes decisions that seem irrational to outside observers. But this is not generally due to religious belief but rather to the fact that the regime's interests and the national interest do not align—for example, Iran and Israel have many common strategic interests, yet Tehran has adopted anti-Israeli rhetoric and policies since the 1979 revolution. This stance may not serve national interests, but it certainly advances the Islamic Republic's interest in a strong, external-enemy narrative.

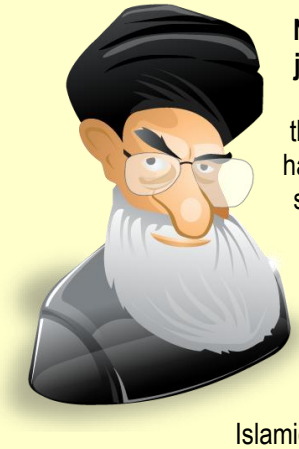
The phantom fatwa

None of this is to say that Islam does not play any role in security decision-making in Iran. Most followers of the country's nuclear affairs are aware of the famous fatwa reportedly issued by Iran's Supreme Leader Ayatollah Khamenei prohibiting nuclear weapons. But this fatwa, or religious edict, has become a puzzle.

In order to issue a fatwa, a religious figure must be deemed an authority in Islamic jurisprudence. (This is why to most Islamic scholars; fatwas issued by Al Qaeda leadership in support of the use of nuclear weapons are void of any legitimacy.) But a fatwa does not have to be written. It can be spoken if it meets certain requirements, such as having been witnessed. In this particular case, Khamenei does not appear to have written the fatwa, but it has been communicated to the International Atomic Energy Agency (IAEA) and repeated a number of times by Khamenei himself, as well as by other government officials. It is unclear whether the fatwa covers only the "use" of these weapons, or their "production and stockpiling" too, as Khamenei has been quoted saying both.

Some scholars and policy makers believe the Khamenei nuclear-weapons fatwa to be bogus because it is not written, and therefore irrelevant. Others believe it to be all-important. Neither side has seen a fatwa, and it has not been published on Khamenei's otherwise extremely comprehensive website.

Adding further ambiguity to the fatwa's status is the fact that such rulings can be overturned, allowing the faith to change and adapt to the times. The founder of the Islamic Republic, the Ayatollah Khomeini, famously overturned a number of fatwas. Even this possibility of reversal, though, does not necessarily make pursuit of an Iranian Bomb more likely, because while there is no religious constraint on canceling a fatwa, the geopolitical cost of overriding this one would be high. Iran has promoted the fatwa in various forums for more than a decade and it is finally being recognized and referred to by world leaders. In a way, by leading a public relations campaign promoting the edict, Tehran has constrained its ability to overturn it.



Nuclear weapons in Shia jurisprudence

Virtually absent from the debate is the fact that Shia scholars who have spoken on nuclear weapons show consensus. Few Grand Ayatollahs have discussed the issue, but those who have present arguments similar to Khamenei's, regardless of personal political stance. Hence, whether they support the Islamic Republic or oppose it, and whether or not they believe that politics and religion should be intertwined (many Iranian Shia clerics say they should not), they believe weapons of mass destruction to be against the faith. What is unclear, however, is the scope of this prohibition. Clerics tend to be generalists, trained to cover all possible matters from which foot to enter the bathroom with (left!) to the use of technology in warfare. This means that the legal debate is neither elaborate nor nuanced.

But the basic principles underlying the Supreme Leader and the other clerics' rulings are very close to those in international law. In Shia jurisprudence, like in international humanitarian law, there must be a distinction between combatants and non-combatants. **Non-combatants, typically defined as women, children, the elderly, and those mentally unfit to fight, are not to be targeted. Hence, using poison in bodies of water and burning trees is not allowed. The environment too must be protected.** These are among the key notions shaping Shia thinking on indiscriminate warfare.

Does it matter what the faith says?

A dissident Iranian Shia cleric, Mohsen Kadivar, points out that when Saddam Hussein's missiles targeted Iranian cities during the Iran-Iraq war, officials asked Khomeini for permission to retaliate in kind. At first he refused, hewing to the Shia ban on indiscriminate warfare. Eventually, though, he allowed similar attacks to be carried out. There are similar examples in which Iran has acted rationally with little or no regard to religious doctrine or sectarianism. Consider Tehran's relations with two neighbors to its northwest, Azerbaijan and Armenia. Armenia is a Christian country, with good ties to Tehran, while Azerbaijan, a Shia-majority state, has had complicated relations with Iran. In Iranians' view, Azerbaijan tries to arouse their own Azeri population's separatism and enables some Israeli actions that target Iran. Tehran's policies are not driven by sectarianism and ideology here, but rather by national interests.

The role of religion in post-revolutionary Iranian politics is complex and often misunderstood in the West. It seems clear, though, that the regime follows its practical interests. When ideology serves these interests, it is put forward as a rationale; otherwise, it takes a backseat. Observers who continue to argue that the regime wishes to hasten the return of the Mahdi, and that Iran will therefore withdraw from the Nuclear Non-Proliferation Treaty and develop nuclear weapons, are contradicted by the facts. In actuality, Tehran highlights that it is party to a number of international treaties, and that its program has been in strict compliance with its international obligations. Whether or not this is the case is a different story, but a suicidal regime wouldn't bother preserving appearances. The regime has not reversed the fatwa or withdrawn from the NPT—precisely because those would be suicidal moves. It is to the government's advantage to be seen as unlikely to pursue a nuclear weapon, so it cites Khamenei's fatwa. But the

regime puts forward no religious rationale for the fact that 35 years after the US embassy hostage crisis, with the backing of the Supreme Leader, it is negotiating with what the revolutionaries then called the "Great Satan." It would not be doing so if it did not believe it was acting in its own real-world interest.

Ariane Tabatabai is an associate (and former Stanton nuclear security fellow) at Harvard Kennedy School's Belfer Center for Science and International Affairs.

New light shed on reactor fuel behavior during severe nuclear reactor accidents

Source: http://www.homelandsecuritynewswire.com/dr20141124-new-light-shed-on-reactor-fuel-behavior-during-severe-nuclear-reactor-accidents

A new discovery about the atomic structure of uranium dioxide will help scientists select the best computational model to simulate severe nuclear reactor accidents.

Using the Advanced Photon Source (APS), a Department of Energy (DOE) Office of Science User Facility, researchers from DOE's Argonne National Laboratory and Brookhaven National

Laboratory, along with Materials Development, Inc., Stony Brook University, and Carnegie Institution of Washington, found that the atomic structure of uranium dioxide (UO2) changes significantly when it melts.

UO2 is the primary fuel component in the majority of existing nuclear reactors, but little is known about the molten state because of its extremely high melting point. Until now, the extremely high temperature and chemical reactivity of the melt have hindered studies of molten UO2. This lack of fundamental information has made it **difficult to evaluate issues associated with the interaction of molten UO2 with a reactor's zirconium cladding and steel containment vessel.**

An ANL release reports that the research team found that **when uranium dioxide melts, the number of oxygen atoms around uranium changes from eight-fold to a mixture of six- and seven-fold, which changes the way it interacts with other materials.** Many existing models, however, do not account for this change in structure or the rapid oxygen dynamics that occur at high temperatures.

An Argonne-led research team found that when uranium dioxide melts, the number of oxygen atoms around uranium changes from eight-fold to a mixture of six- and sevenfold, which alters how it interacts with other materials. The discovery about will help scientists select the best computational model to use when simulating severe nuclear reactor accidents.

"Determining the behavior of UO2 under extreme conditions is essential to enhancing our understanding of reactor safety during severe accidents," said Mark Williamson of Argonne's Chemical Sciences and Engineering Division.

"Very few places in the world have the capability to safely measure the structure of molten UO2 at 3,000 degrees Celsius without introducing contamination from the container that holds the melt," added Chris Benmore of Argonne's X-ray Science Division.

Researchers studied the UO2 in the hot crystalline and molten states. In this experiment, researchers relied on the APS's high-energy synchrotron X-ray beam to study a bead of UO2 that was

aerodynamically levitated on a stream of argon and heated with a laser beam.
X-ray experiments were performed at sector 11-ID-C at the APS.
The work was funded by the DOE Office of Science (Office of Basic Energy Sciences), the DOE Small Business Innovation Research program and the Argonne Laboratory Directed Research and Development program.
The paper, "Molten uranium dioxide structure and dynamics," is published in *Science* magazine.
"Our group plans to continue to use innovative synchrotron techniques to study molten materials like this," said John Parise, who holds a joint appointment with Brookhaven National Laboratory and Stony Brook University. "The next steps include putting molten materials under different atmospheres, and that requires modifications to the existing set-up used at APS."
Parise said this group of researchers, which includes colleagues from Materials Development, Inc., who built the apparatus used to study UO2, is discussing designs for next-generation levitation devices that could be installed at the X-Ray Powder Diffraction beamline at Brookhaven's National Synchrotron Light Source II, for example.
"There's a lot more work to be done," Parise said. **"It's important to understand how many other materials behave in a molten state.** Theory is a good way to do that, but theorists need data on how atoms interact with each other in the molten state, under conditions that are as realistic as possible."

— Read more in L. B. Skinner et al., "Molten uranium dioxide structure and dynamics," Science *346, no. 6212 (21 November 2014): 984-87*

Scientist develops uncrackable security code for nuclear weapons

Source: http://www.homelandsecuritynewswire.com/dr20141125-scientist-develops-uncrackable-security-code-for-nuclear-weapons#.VHPZppoxk5I.linkedin

Nuclear weapons exist, so control of nuclear weapons is essential. Intrinsic Use Control (IUC) is a concept which is capable of providing improved quantifiable safety and use control within a nuclear weapon. As a basic concept, use control is best accomplished in the weapon itself rather than depending on administrative controls, fences, and guards. Using established technology, IUC uses passive use control to resist any attacks or unauthorized use of a weapon at either the component or the fully assembled levels.
Mark Hart, a scientist and engineer in Lawrence Livermore National Laboratory's (LLNL) Defense Technologies Division, has been awarded the 2015 Surety Transformation Initiative (STI) Award from the National Nuclear Security Administration's (NNSA) Enhanced Surety Program.
A LLNL release notes that the STI award aims to stimulate and encourage the development of potentially transformational nuclear weapon surety technologies and explore innovative, preferably monumental shift solutions, to unmet surety needs.
"STI's task is to reach beyond the traditional stockpile stewardship function of maintaining existing nuclear weapon capability in the absence of supercritical testing," said Robert Sherman, enhanced surety federal program manager in NNSA's Technology

Maturation Division. "STI is intended not to maintain or polish 'your grandfather's Oldsmobile,' but to go beyond it: to invent devices and technologies that serve the 21st century nuclear security needs of the American people better than they are served by existing Cold War legacy technologies."

Hart's winning proposal is for Intrinsic Use Control (IUC), a concept which is capable of providing improved quantifiable safety and use control within a nuclear weapon. Nuclear weapons exist, therefore control is essential. Use control of a weapon is focused on providing unencumbered authorized use while restricting unauthorized use. Safety, use control and physical security work in concert for the weapon's surety.

As a basic concept, use control is best accomplished in the weapon itself rather than depending on administrative controls, fences, and guards. Using established technology, IUC uses passive use control to resist any attacks or unauthorized use of a weapon at either the component or the fully assembled levels.

"An IUC-class weapon would function reliably as intended, when intended, exclusively under authorization by the National Command Authority," Hart said. "The component use control that IUC provides is sufficiently robust to defeat any unauthorized attempt to make these components function, even by the people who designed and built the arming, firing and initiation components."

This is accomplished by designing the components to function in a way that cannot be replicated by any individual. Using the IUC concept, weapon components would be initialized and made secure during assembly by using the weapon's fluctuating radiation field to generate unique component IDs and use-control numbers, only known to the weapon. Any anomaly in their verification, caused by removal or replacement of any protected component, will cause all protected components to be unusable.

IUC provides a less than 10-18 chance of controlling or operating an individual protected component, and a less than 10-72 chance of controlling or operating the entire protected system.

"Using the random process of nuclear radioactive decay is the gold standard of random number generators," Hart said. "You'd have a better chance of winning both Mega Millions and Powerball on the same day than getting control of IUC-protected components."

STI projects are competitively selected from proposals submitted by the nuclear weapon design laboratories (Los Alamos National Laboratory, Lawrence Livermore National Laboratory, and Sandia National Laboratories). Hart's proposal was selected from seven applicants and will receive $2 million in funding over three years.

Electromagnetic Pulses - Six Common Misconceptions

By George H. Baker

Source:http://www.domesticpreparedness.com/Commentary/Viewpoint/Electromagnetic_Pulses_-_Six_Common_Misconceptions/

Many misconceptions about electromagnetic pulse (EMP) effects have circulated for years among technical and policy experts, in press reports, on preparedness websites, and even in technical journals. Because many aspects of EMP-generation physics and its effects are obscure, misconceptions from those who do not perceive the seriousness of the effects to those who predict a doomsday chain of events are inevitable. However, not all EMPs are the same, with the most significant effects being caused by E1 and E3 fields.

Nuclear bursts detonated at altitudes above 40 km generate two principal types of EMPs that can debilitate critical infrastructure systems over large regions:

- The first, a "fast-pulse" EMP field, also referred to as E1, is created by gamma ray interaction with stratospheric air molecules. The resulting electric field peaks at tens of kilovolts per meter in a few nanoseconds, and lasts a few hundred nanoseconds. E1's broadband power spectrum (frequency content from DC to 1 GHz) enables it to couple to electrical and electronic systems in general, regardless of the length of their cables and antenna lines. Induced currents range into the thousands of amperes and exposed systems may be upset or permanently damaged.

- The second "slow-pulse" phenomenon, is referred to as magnetohydrodynamic (MHD) EMP, or E3, and is caused by the distortion of Earth's magnetic field lines due to the expanding nuclear fireball and the rising of heated, ionized layers of the ionosphere. The change of the magnetic field at the Earth's surface induces a field in the tens of volts per kilometer, which, in turn, induces low-frequency currents of hundreds to thousands of amperes in long conducting lines only (a few kilometers or longer) that damage components of long-line systems, including the electric power grid and long-haul communication and data networks.

By over- and under-emphasizing realistic consequences of EMPs, policymakers may delay actions or dismiss arguments altogether. **The six misconceptions about EMPs that are perhaps the most harmful involve: (a) exposed electronic systems; (b) critical infrastructure systems; (c) nuclear weapons; (d) cost of protection; (e) type of EMPs; and (f) fiber-optic networks.**

Misconception 1

EMP Will Cause Every Exposed Electronic System to Cease Functioning

Based on the U.S. Department of Defense (DOD) and Congressional EMP Commission's EMP test databases, small, self-contained systems, such as motor vehicles, hand-held radios, and unconnected portable generators, tend not to be affected by EMPs. If there is an effect on these systems, it is often temporary upset rather than component burnout.

On the other hand, threat-level EMP testing also reveals that systems connected to power lines are highly vulnerable to component damage requiring repair or replacement. Because the strength of EMP fields is measured in volts per meter, the longer the conducting line, the more EMP energy will be coupled into the system, and the higher the probability of damage. As such, the electric power-grid network and landline communication systems are almost certain to experience component damage when exposed to an EMP with cascading effects to most other (dependent) infrastructure systems.

Misconception 2

EMP Effects Will Have Limited, Easily Recoverable, "Nuisance" Effects on Critical Infrastructure Systems

Although an EMP would not affect every system, widespread failure of a significant fraction of electrical and electronic systems will cause large-scale cascading failures of critical infrastructure networks because interdependencies among affected and unaffected systems. Mathematician Paul Erdos's "small-world" network theory applies, which refers to most nodes – equipment attached to a network – being accessible to all others through just a few connections. The fraction of all nodes changes suddenly when the average number of links per single network connection exceeds one. For example, a single component failure, where the average links per node is two, can affect approximately half of the remaining "untouched" network nodes.

For many systems, especially unmanned systems, loss of control is tantamount to permanent damage, in some cases causing machinery to self-destruct. Examples include:

- Lockup, or not being able to change the "on" or "off" state, of long-haul communication repeaters;
- Loss of remote pipeline pressure control in supervisory control and data acquisition (SCADA) systems, which communicate with remote equipment;
- Loss of generator controls in electric power plants; and
- Loss of machine process controllers in manufacturing plants.

Misconception 3

Megaton-Class Nuclear Weapons Are Required to Cause Serious EMP Effects

Due to a limiting atmospheric saturation effect in the EMP-generation process, low-yield weapons produce a peak E1 field similar in magnitude to high-yield weapons if they are detonated at altitudes of 50-80 km. The advantage of high-yield weapons is that their range on the ground is affected less significantly when detonated at higher altitudes.

Nuclear weapons with yields ranging from 3 kilotons to 3 megatons (a 3 order of magnitude difference in yield), when detonated at their optimum burst altitudes, exhibit a range of peak E1 fields on the ground differing by only a factor of ~3, viz. 15-50 KV/meter. With respect to the late-time (E3, or low-amplitude, low-frequency components) EMP field, a 30-KT nuclear weapon above 100 km would cause geomagnetic disturbances as large

as solar superstorms, although over smaller regions. It also is worth noting that peak currents on long overhead lines induced by E1 from 10 kiloton-class weapons can range in the kiloamperes with voltages reaching into the hundreds of kilovolts.

Misconception 4

Protecting the Critical National Infrastructure Would Be Cost Prohibitive

Of the 14 critical infrastructure sectors, EMP risk is highest for electric power grids and telecommunication grids because of their network connections and criticality to the operation and recovery of other critical infrastructure sectors. Attention to hardening these infrastructure grids alone would provide significant benefits to national resilience.

The electric power grid is essential for sustaining population "life-support" services. However, some major grid components could take months, or years, to replace if many components are damaged. The primary example is high-voltage transformers, which can irreparably fail during major solar storms and are thus likely to fail during an EMP event. Protection of these large transformers would reduce the time required to restore the grid and restore the necessary services it enables.

According to Emprimus, a manufacturer of transformer protection devices, the unit cost for high-voltage transformer protection is estimated to be $250,000, with the total number of susceptible large, high-voltage units ranging from 300 to 3,000, according to Oak Ridge National Laboratory. The requirement and cost for generator facility protection are still undetermined but are likely to be similar to transformer protection costs. To protect SCADA systems, replacement parts are readily available and repairs are relatively uncomplicated. Protection costs for heavy-duty grid components are in the $10 billion range, which is a small fraction of the value of losses should they fail. When amortized, protection costs to consumers amount to pennies per month.

Misconception 5

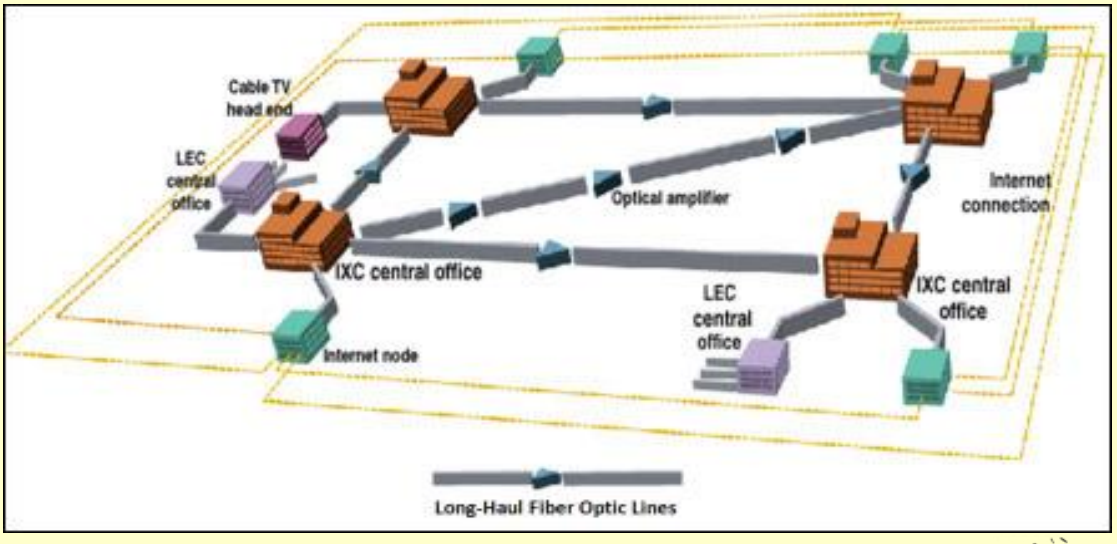
Only Late-Time EMP (E3) Will Damage Electric Power-Grid Transformers

Oak Ridge National Laboratory's January 2010 report on its E1 tests of 7.2-KV distribution transformers produced permanent damage to transformer windings in seven of the 20 units tested. The failures were due to transformer winding damage caused by electrical breakdown across internal wire insulation. As an important side note, transformers with direct-mounted lightning surge arrestors were not damaged during the tests. Similar tests of high-voltage transformers are needed.

Misconception 6

Fiber-Optic Networks Are Not Susceptible to EMP Effects

In general, fiber-optic networks are less susceptible than metallic line networks;



however, fiber-optic multipoint line driver and receiver boxes, which are designed to protect against ground current, may fail in EMP environments. Long-haul telecommunication and regional Internet fiber-optic repeater amplifiers' power supplies are particularly vulnerable

to EMP environments (Figure 1). Terrestrial fiber-optic cable repeater amplifier power is provided by the electric power grid and thus vulnerable to grid failure as well as to direct EMP/E1 effects.
Undersea cable repeater amplifiers also are vulnerable to EMP/E3 effects since they are connected to a coaxial metallic power conductor that runs the length of the line. Because of its low-frequency content, E3 penetrates to great ocean depths, which subjects undersea power amplifiers to high risk of burnout. On the positive side, line drivers/receivers and repeater amplifiers are relatively easy to protect using shielding, shield-penetration treatment, and power-line filters and/or breakers.

Standardized Solutions

From a risk-based priority standpoint, the electric power grid is a high priority for EMP protection. Hardening this infrastructure alone would have major benefits for national resilience – the ability to sustain, reconstitute, and restart critical services. EMP engineering solutions have been implemented and standardized by DOD since the 1960s and are well documented:

- MIL-STD-188-125-1 – "DOD Interface Standard – High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions – Part 1 – Fixed Facilities" (17 July 1998);
- MIL-STD-188-125-2 – "DOD Interface Standard – High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions – Part 1 – Transportable Systems" (3 March 1999); and
- MIL-HDBK-423 – "Military Handbook – High-Altitude Electromagnetic Pulse (HEMP) Protection for Fixed and Transportable Ground-Based C4I Facilities Vol. 1 – Fixed Facilities" (15 May 1993).

With respect to the power grid, the installation of blocking devices in the neutral-to-ground conductors of large electric distribution transformers will significantly reduce the probability of damage from slow EMP/E3. Transformer protection against E1 overvoltages is achievable by installing common metal-oxide varistors (control elements in electrical circuits) on transformers from each phase to ground. Costs for protecting the power grid are small compared to the value of the systems and services at risk.

George H. Baker *is professor emeritus at James Madison University (JMU) and directed JMU's Institute for Infrastructure and Information Assurance. He consults on critical infrastructure assurance, specializing in EMP and other nuclear effects. He is the former director of the Defense Threat Reduction Agency's critical system assessment facility. He also led the EMP group at the Defense Nuclear Agency responsible for development the DoD EMP standards. He served as principal staff on the Congressional EMP Commission and now serves on the board of directors of the Foundation for Resilient Societies and the Congressional Task Force on National and Homeland Security advisory board. He holds a Ph.D. in engineering physics from the U.S. Air Force Institute of Technology.*

X ray Baggage Scanners and radiation

By Firoze Zia Hussain

Source: https://www.linkedin.com/pulse/article/20141121182409-7501738-x-ray-baggage-scanner-s-and-radiation

Recently had an opportunity to see various baggage scanner old and new at few hotels/corporates and airports and the leakage radiation being emitted out

I found that operators are grossly unaware of the radiation risk posed by X-ray baggage scanners to operators standing nearby continuously due to cumulative absorption.

Some of the scanners had very thin lead curtains, few had damaged curtains leading to direct leakage of radiation to the operators or the customer who has gone to the hotel and is placing the items on the scanner conveyor rollers.

Lead curtains are fixed at entry /exit of baggage scanners to minimise the x ray leakage from the inside chamber of the x ray machine to the outside. However some operators were literally pushing the bags through the curtain which is a bad work practice.

Radiation is a well known cause of cancer which can be caused by prolonged access to even low

doses of radiation .for the passengers it may not be so much of a risk as they place and move away but the operators whether private security personnel, police personnel or airport specialised staff are continusly around the machine and hence cumulative occupational doses over a year or lifetime (MREM) needs to be checked using personnel dosimetry. Also with more and more women x ray operators this is an important SHE item as women are more susceptible to x ray.

If a management does install x ray machine they should get periodic leakage radiation tests done and paste the same on the machine for adherence to safety standard. In some cases the leakage was high due to usage of second hand Chinese x ray generators where even protective oil layer was leaking .during maintenance such aspects need to be checked thoroughly

Some manufacturers have not only thickened the lead curtain strips but also provided a double enmeshed type curtain so that even of one curtain is opened due to baggage movement the strips of other curtain adjacent to the first will prevent x-ray radiation leakage.

Airports /Hotels /Corporates need to keep radiation measurement equipment and personal radiation badges for ensuring safety for own personnel

Also if food items are being x rayed or kept nearby one needs to be sure as USFDA has framed norms for safety in this regards.

The government had taken strong initiative for ensuring EURO norms for vehicular emissions .these emissions was effecting environment in general and traffic constables in particular who were manning the traffic islands ..a similar initiative needs to be taken for radiation leakages.

U.S.F.D.A., Center for Devices and Radiation Health performance standards for cabinet X-ray systems (Federal Standard 21-CFR 1020.40). Typical leakage radiation is less than 0.1 mR/hr. However with single line of lead strips the leakage increases significantly

Millimetre wave security inspection machines were installed in large numbers at various airports in USA but later removed out on basis of radiation concerns..

To summarise operators need to be sensitised and the management needs to take responsibility for cumulative radiation dosage for individuals working in such environments. Also best practises in operation and maintenance to be followed.machine manufacturers also need to take steps to work on methodologies to reduce leakage radiation.

References

A study of 8 US airports by NIOSH on x ray radiation and effects on personnel manning the machines
http://www.cdc.gov/niosh/hhe/reports/pdfs/2003-0206-3067.pdf

firstly while ordering a baggage scanner need to check if it is approved by AERB.When a new baggage scanner is rxd from OEM firstly one needs to see the QC certificate which must have details of the radiation measurement at min 4 points around the machine .This should be checked for conformity and compliance annually using a radiation meter one needs to recheck for any degradation and reasons thereof and variance thereof specially if generator has oil leakage or is reconditioned repaired one needs to check for radiation also for torn or bent lead curtains further cumulative radiation absorbtion by individuals need to be seen so that staff rotation is practiced a study done by niosh usa may be seen http://www.cdc.gov/niosh/hhe/reports/pdfs/2003-0206-3067.pdf

Firoze Zia Hussain *is CEO at Totem International Limited (India)*

ISIS Threatens Use of Nuclear Bomb in London; UN Ambassador Warns of 'Weapons of Mass Destruction'

Source: http://au.ibtimes.com/articles/574600/20141202/isis-nuclear-bomb-weapons-mass-destruction-london.htm#.VH3x9MmAOW7

December 02 – **The Islamic State of Iraq and Syria militants have reportedly developed a nuclear weapon from the radioactive material they seized from the Mosul University in Iraq.** ISIS bragged about the nuclear device on social media as a British extremist fighter claimed it would wreak havoc in London when it explodes.

According to media reports, **ISIS militants have stolen 40 kilogrammes of uranium in July and used it to make a "dirty**

bomb." The Mirror noted that British bomb expert Hamayun Tariq was identified as among the militants who issued threats to the West online. In 2012, he left his home in Dudley and went to the Middle East.

On his Twitter account under the Muslim name, Muslim al-Britani, he announced that ISIS has a dirty bomb and revealed they militants found radioactive material at the Iraqi university in Mosul. He went on to say ISIS will study what dirty bombs can do and talk about what happens when it is detonated in a public area.

In what may be viewed as a veiled threat, the British ISIS supporter added that it would be "terribly destructive" if it exploded in London. His account on Twitter has since been suspended after posting his comments. As a show of support, other ISIS fighters also posted on Twitter to confirm that militants have in their possession a bomb from radioactive material in Mosul.

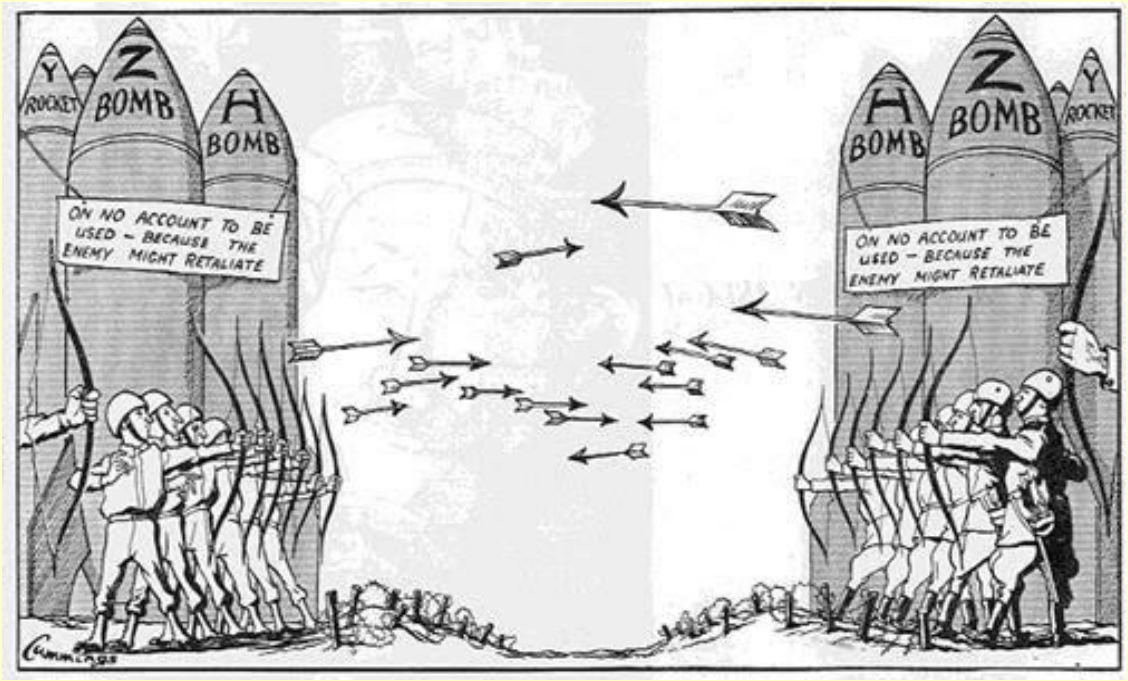
Reports of ISIS having a nuclear device have alarmed the UN Ambassador to Iraq Mohamed Ali Alhakin. He wrote a letter to UN Secretary General Ban Ki-moon and revealed that ISIS has been taking nuclear material from areas where the group has taken over. The ambassador informed the UN that such material can be used to manufacture "weapons of mass destruction." Alhakin warned that nuclear materials, even in limited quantities, can enable terrorist groups like ISIS to use it in the militants' terror campaign with the help a weapons expert.

The Mirror speculates that if ISIS has a nuclear bomb, the group would more likely use it in Iraq or Syria rather than risk being caught when smuggling it into a Western country. Previous reports indicate that if ISIS was confirmed to have weapons of mass destruction or a nuclear bomb, U.S. President Barack Obama would not hesitate to send ground troops to destroy ISIS.

How to keep future cold wars cold: Mind the missiles

By Gregory D. Koblentz

Source: http://www.latimes.com/opinion/op-ed/la-oe-koblentz-nuclear-threats-20141128-story.html



At a time when we are reflecting on the lessons from the Cold War amid growing concern about the current U.S.-Russia relationship, we should be looking ahead to anticipate how changes in technology and geopolitics create new challenges to peace and stability among the world's major powers.

Changes in technology and geopolitics create new challenges to peace and stability among the world's major [nuclear] powers. -

The Cold War stayed cold largely because the United States and the Soviet Union possessed nuclear weapons that raised the risk of an armed conflict between them to an unacceptable level. The destructiveness of nuclear weapons and the lack of effective defenses against them contributed to the strategic stability between the superpowers. Neither side had an incentive to strike first, and this calculation was unaffected by external shocks, false alarms or marginal shifts in the balance of power.

Since the end of the Cold War, three challenges to strategic stability have emerged. The **first** is the increasing complexity of deterrence relations among the nuclear weapon states. Whereas the first nuclear age was shaped by the bipolar global ideological and military competition between the United States and Soviet Union, the second nuclear age has been marked by the emergence of a multipolar nuclear order composed of states linked by varying levels of cooperation and conflict. Rising nuclear powers such as China, India and Pakistan are not party to the web of treaties, regimes and relationships that girded strategic stability between the United States and Soviet Union (and now Russia).

Moreover, **most nuclear weapon states face security threats from more than one source, which breeds a "security trilemma," when actions taken by a state to defend itself against one state have the effect of making a third state feel insecure.** As a result, changes in one state's nuclear posture can have a cascading effect on the other nuclear-armed states. The trilemma helps explain Russian and Chinese reactions to American missile defenses aimed at Iran and North Korea.

The **second** challenge is the emergence of a suite of advanced nonnuclear military technologies that have the potential to replicate, offset or mitigate the strategic effects of nuclear weapons. Missile defenses and long-range precision weapons, for example, reduce strategic stability by endangering the ability of nuclear-armed states to credibly threaten retaliation following a surprise attack. Anti-satellite weapons and cyberweapons pose threats to the integrity of early-warning and command-and-control systems.

The potential for rapid advances in these technologies will make it more difficult for states to accurately assess others' capabilities, which may foster worst-case analyses and arms races. This dynamic reinforces the "zero-sum" mentality that feeds the security trilemma.

The **third** challenge is found in South Asia, which is the region most at risk of a breakdown in strategic stability. India and Pakistan face more severe security challenges than those of the other nuclear weapon states because of their geographic proximity, history of conflict, higher levels of domestic instability, the dispute over Kashmir and the threat of cross-border terrorism.

The two countries have been engaged in a nuclear and missile arms race since 1998 that shows no signs of abating. Pakistani development of short-range nuclear-armed missiles and India's pending deployment of sea-based nuclear weapons raise further concerns about command and control and the heightened vulnerability of these weapons to accidents and terrorism.

Furthermore, because of the security trilemma, the deterrence relationship between India and Pakistan is intertwined with that of China. This trilateral linkage increases the region's susceptibility to outside shocks and amplifies the risk that regional developments will have far-reaching effects.

Each of these dynamics is worrisome on its own, but the combination of them could be particularly destabilizing. The United States should proactively shape the second nuclear age before it finds itself trapped in a new nuclear order that is less stable, less predictable and less susceptible to American influence.

Working in concert with the other established nuclear weapon states, the United States should promote transparency and confidence-building measures to mitigate the destabilizing influences of advanced nonnuclear military technologies, encourage strategic dialogue among China, India and Pakistan, build capacity in India and Pakistan to engage in such dialogue, and establish a multilateral forum that includes India and Pakistan in discussions among the established nuclear weapon states on issues affecting strategic stability.

Gregory D. Koblentz *is an associate professor in the School of Policy, Government and International Affairs at George Mason University and author of the Council on Foreign Relations report,* "Strengthening Strategic Stability in the Second Nuclear Age."

Accident Took Place At Ukraine Nuclear Power Plant, Prime Minister Reveals

Source: http://www.zerohedge.com/news/2014-12-03/accident-took-place-ukraine-nuclear-power-plant-prime-minister-reveals

December 03 – Several days ago we heard rumors, unsubstantiated, of an accident at

in fact, the PM waited almost a week before revealing it to the world.

Ukraine's Zaporozhye nuclear power plant, *Europe's largest* and the 5th biggest in the world. Considering Ukraine's history with nuclear accidents, and resultant panics, we decided it would be prudent to wait for an official confirmation before proceeding with a report. We got the confirmation about an hour ago, when Ukraine's new/old Prime Minister Arseny Yatseniuk, or "Yats" as his puppetmaster Victoria Nuland likes to call him, said "**on Wednesday an accident had occurred at the Zaporizhye nuclear power plant (NPP) in south-east Ukraine and called on the energy minister to hold a news conference**."

A "minor" accident that is, which remains a rather nebulous term on the continuum of nuclear power plant "malfunctions." So minor,

From Reuters:

"I know that an accident has occurred at the Zaporizhye NPP," Yatseniuk said, asking new energy minister Volodymyr Demchyshyn to make clear when the problem would be resolved and what steps would be taken to restore normal power supply across Ukraine.

News agency Interfax Ukraine said the problem had occurred at bloc No 3 - a 1,000-megawatt reactor - and the resulting lack of output had worsened the power crisis in the country. Interfax added that the bloc was expected to come back on stream on Dec. 5.

Just like Fukushima is expected to come back on line in a few years ago.

So is this just another Chernobyl? According to Ukraine, "the radioactive meltdown is contained." RT has more:

"There is no threat ... there are no problems with the reactors," Ukraine's Energy Minister Volodymyr Demchyshyn said at briefing, adding the accident affected the power output system and "in no way" was linked to power production itself.

The incident was not made public until Wednesday, when PM Yatsenyuk asked the energy minister to report on what happened and how the ministry is handling the situation.

The accident left several dozen towns and villages without electricity, Russian media reported, citing local officials.

Of course, there is no way to actually know what is happening on the ground as the NPP is located close enough to the "fog of war", that its status, and updates thereof, could merely be part of the fog of war. That said, if there is an unspoken message here by Ukraine, which recently handed over its gold to unknown "Western" interests, and suddenly feels neglected by its western allies (as its central bank head is about to find out personally), it is targeted directly at the IMF: "hand over more loans, or the nuclear power plant gets it."

▶ **UPDATE:** No radiation escape; one worker died and another severely burnt.

Risks of terrorists attacking, or using materials from, a nuclear power plant are low: Experts

Source: http://www.homelandsecuritynewswire.com/dr20141204-risks-of-terrorists-attacking-or-using-materials-from-a-nuclear-power-plant-are-low-experts

Energy analysts who support new nuclear power plants construction insist that the probability of a terrorist nuclear attack by land, sea, or air is extremely low. They reject arguments by nuclear power opponents that terrorist groups may one day attack a nuclear plant, or build an improvised nuclear bomb using materials stolen from a nuclear power plant – and that governments should, therefore, end construction of new nuclear power plants.

A recent article published by The Energy Collective examines the probability and real hazard of a terrorist attack on a nuclear plant, and the hazards and probabilities of other available nuclear attack options for terrorists.

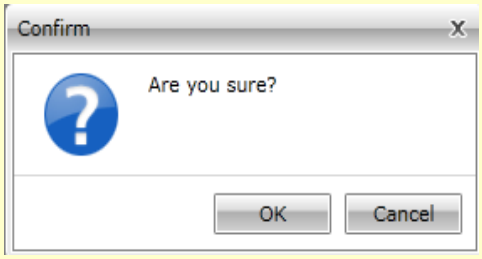
Terrorist organizations may attack a nuclear plant to prompt a meltdown, but a nuclear meltdown from a reactor may result in less damage than most terrorist groups aspire to inflict. The standard radiation dose limit for workers near the Fukushima Daiichi nuclear disaster was 50 millisievert (msv) per year and 100 msv over five years, but in order to allow workers to respond to the accident, the emergency dose was increased to 250 msv per year from 100 msv per year pre-meltdown. One-hundred-and-seventy-six workers at the plant received doses of between 100 and 670 msv during and shortly after the disaster (msv), but only two workers died from the incident.

Attempts to steal nuclear materials for use in an improvised nuclear bomb from nuclear power plants are likely to fail because the radioactive materials, such as spent fuel rods in nuclear power plants, are effectively untransportable due to "the heat generated by large quantities of such material and the extreme exposure hazard from the intensity of the radiation." Individuals attempting to steal spent fuel rods would be exposed to dangerous radiation levels and are likely to die or fall seriously ill before they could have the chance to use the materials. **Additionally, fuel stolen from a reactor might be poorly enriched, making it relatively useless for an improvised nuclear weapon.** Robert Frost,

president of Nuclear Safety Associates, noted in a 2005 Adelphi Papers that constructing the device itself is practically impossible for terrorist groups, considering the need for advanced equipment, expertise, and facility. Furthermore, the materials considered most practical for use in improvised nuclear bombs, as The *Homeland Security News Wire* reported earlier this year, are used in medical applications, far from any nuclear plant.

The probability of an intrusion of a Western nuclear power plant is extremely low due to intense physical and electronic security. "There has never been [a terrorist attack on a nuclear plant], and there appears to be no evidence that a plan to attack a nuclear power plant has ever moved beyond the basic planning phase in any terrorist group," said Robert Wilson, an energy analyst. **The only reported successful intrusions of a working nuclear facility have been led by activists who sought to send anti-nuclear messages.**

Opponents of new nuclear plants construction have claimed that terrorists could one day crash a jumbo jet loaded with fuel into a nuclear plant's containment dome. Engineers at Entergy, the operator of New York's Indian Point power plant, are confident that a dome's three to six feet concrete walls reinforced with embedded steel bars and a half-inch steel liner could withstand a collision with a large airliner. Should a fire ignite after a jumbo jet collides with a plant's containment dome, a 2006 review by the U.S. Nuclear Regulatory Commission to Congress concluded that the "likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low."



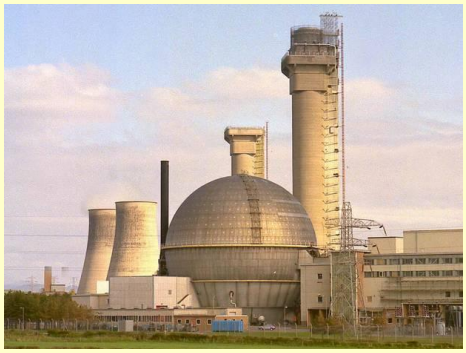
The risk of not building more nuclear power plants means an increasing reliance on fossil fuel which remains a major contributor to climate change. While alternative energy sources like wind and solar have gained popularity, "those energy sources cannot scale up fast enough to deliver cheap and reliable power at the scale the global economy requires," wrote climate scientists Kenneth Caldeira of the Carnegie Institution, Kerry Emanuel at the Massachusetts Institute of Technology, James E. Hansen of Columbia University, and Tom Wigley of the National Center for Atmospheric Research and the University of Adelaide, in a letter to anti-nuclear power policy makers responsible for environmental policy. "There is no credible path to climate stabilization that does not include a substantial role for nuclear power," the scientists added.

EDITOR'S COMMENT: Keep in mind that "LOW" does not equal "ZERO"! As for engineers at Entergy: do not be so concretely sure that the dome will withstand collision just because theoretical models indicate so!

Islamic terrorism could jeopardize nuclear power stations

Source: http://i-hls.com/2014/12/new-threat-islamic-terrorism-jeopardize-nuclear-power-stations/

Following the spread of Islamic terrorist attacks worldwide, causing major concern among the entire population, the West has begun looking for a solution to a new problem which poses a far greater risk than beheadings, namely: the risk of nuclear and radiological terror. One of the institutions looking into this potential danger is the Federation of American Scientists, whose findings and estimates reach all US intelligence bodies.



A paper published by the Federation's nuclear experts, points out several risks posed by the threat of nuclear terror. **The first:** 'non-territorial terrorist organizations such as ISIS, Hamas, Hezbollah and others. Such organizations, which have unlimited financial means, can simply acquire nuclear arms in the black market

through criminal organizations with the proper knowhow. The **second risk** is posed by the threat of a terrorist organization capable of acquiring uranium ore and create an IND (Improvised nuclear device). Also named 'dirty bomb', this charge could be detonated using conventional explosive to spread radioactive fallout across a major radius.

The third, new risk, is posed by the threat of an attack on nuclear power stations which abound across the globe. The essence of this threat: a relatively small bomb could cause widespread damage.

It is important to note, cautions the Federation's paper, that nuclear power plants generate about 20% of the world's electricity. **Some 31 states across the US and numerous countries from Europe to the Far East have about 435 active nuclear power stations.** The major threat is posed by their relative proximity to civilian, urban centers. In this context, it is also important to note many of these reactors are old, so they could be tampered with using conventional means – not necessarily nuclear means.

The Federation's paper recommends applying the most advanced radiation monitoring means available in all numerous US border checkpoints. Nevertheless, they also recommend control, monitoring and security of routes leading to and from nuclear facilities, including naval and aerial routes used for transporting various cargo.

One of the Federation's paper's most interesting recommendations, is to reduce terrorist organizations' motivation to disrupt the West by delivering data and information through sophisticated means that the West could, for his part, perpetrate a major attack on important Muslim centers and wreak irrevocable radiation damage.

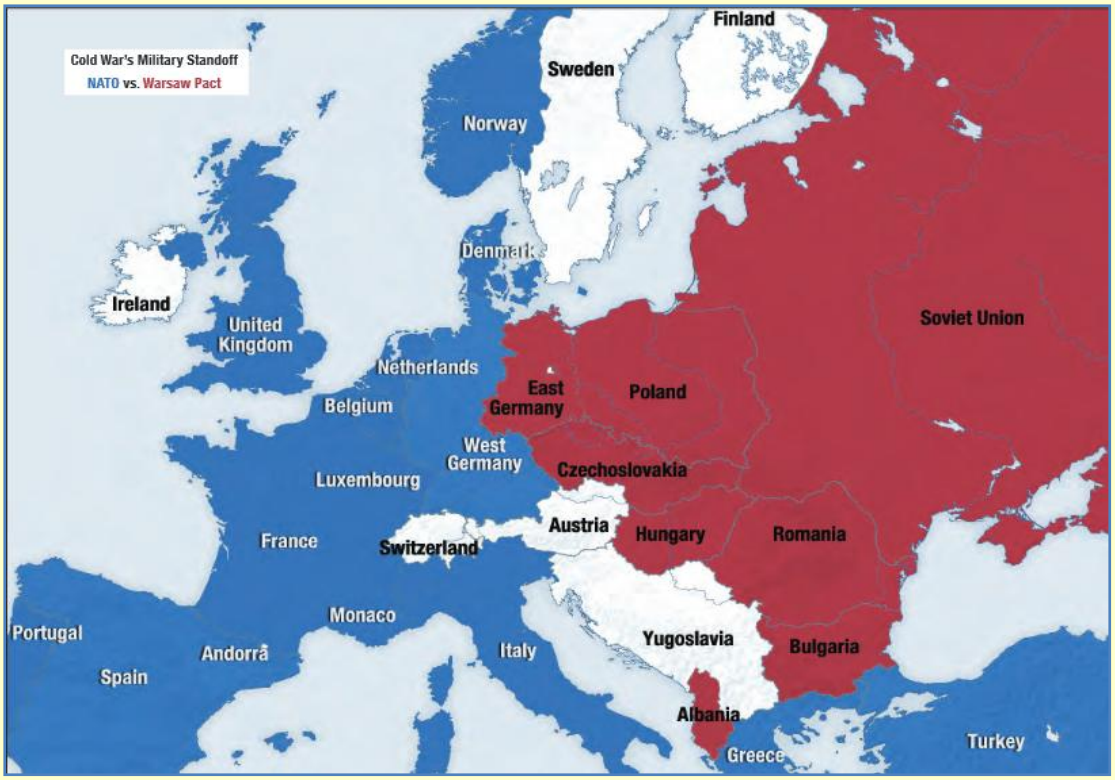
Rethinking the Unthinkable

Source: http://www.lanl.gov/discover/publications/national-security-science/2014-december/rethinking_the_unthinkable.php

December 03 – By 2021, 98 percent of Russia's intercontinental ballistic missile forces will be composed of newly designed and manufactured warheads and delivery systems. Their modernization efforts are already 50 percent complete. (Photo: Open Source)

The end of the Cold War brought many changes including the unification of Germany, the expansion of democracy into Eastern Europe, and the integration of Russia into the global economy. It also removed the previous five-decades-long worry about a nuclear war. "Thinking about the unthinkable," that is, seriously contemplating nuclear war, has all but vanished from the minds of most people.

But given Vladimir Putin's annexing of Crimea last spring and his boast in September that he could



invade five NATO capitals inside two days, a Cold War 2.0 may be just around the corner. Putin's actions come on the heels of the modernization of Russia's nuclear weapons program. In stark contrast, the nuclear weapons research, testing, and production infrastructures of the United States have continued their rapid erosion through elimination and restructuring of organizations and reductions of workforces and budgets. These trends must be examined and evaluated.

Read more at:
http://www.lanl.gov/discover/publications/national-security-science/2014-december/_assets/doc/NSS-december2014-rethinking_the_unthinkable.pdf

Chinese man accused of smuggling Massachusetts-made parts for nuclear weapons to Iran extradited to Boston

Source:http://www.masslive.com/news/boston/index.ssf/2014/12/chinese_man_accused_of_smuggli.html

A Chinese man was extradited to Boston and will face federal charges for allegedly smuggling Massachusetts-made parts to Iran that can be used to make nuclear weapons, according to the office of U.S. Attorney Carmen Ortiz.

Sihai Cheng arrived at Logan Airport on Friday, after he was arrested at the request of the United States by British authorities on a trip to the United Kingdom.

Cheng is a Chinese citizen who also goes by the names Chun Hai Cheng and Alex Cheng. He was charged, along with Iranian national Seyed Abolfazl Shahab Jamili and Iranian companies Nicaro Eng. Co., Ltd. and Eyvaz Technic Manufacturing Company, with smuggling, exporting and conspiring to export American goods with nuclear applications to Iran. The United States has implemented sanctions against Iran, prohibiting the export of anything that can help Iran manufacture nuclear weapons.

Jamili remains a fugitive.

According to the charges laid out in the indictment, Cheng operated a trading company in China and Hong Kong. Cheng began supplying Chinese parts, which

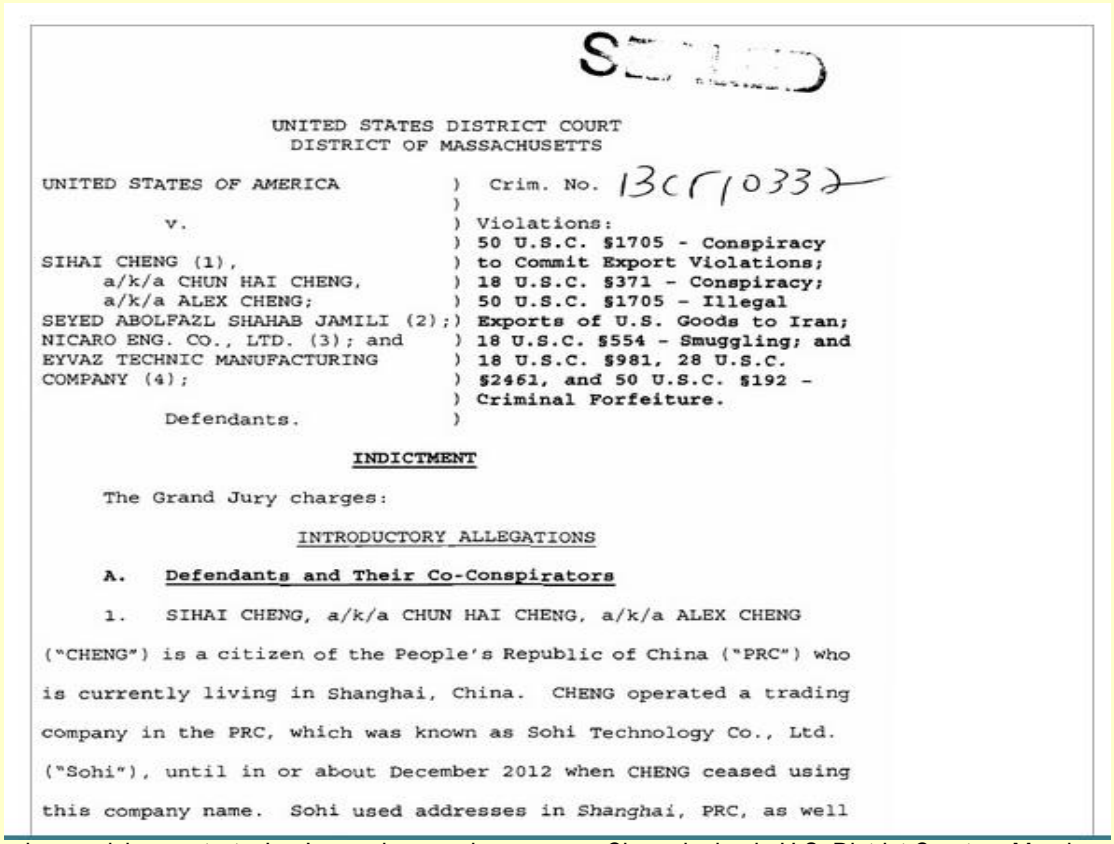
could be used to manufacture nuclear weapons, to Jamili in 2005. Jamili operates the Iranian trading company Nicaro, which supplied parts to Eyvaz – an Iranian company against which the United States and the European Union have imposed sanctions because of its role supplying parts to Iran's uranium nuclear enrichment facilities.

Jamili told Cheng the parts were going to Iran and were being used for "a very big project and secret one."

In 2009, Jamili asked Cheng for help procuring pressure transducers – sensors used to measure pressure, which can be used in centrifuges to convert natural uranium into a form that can be used in nuclear weapons.

Cheng then contacted the Shanghai office of MKS Instruments, an American company headquartered in Andover, Mass., that manufactures pressure transducers. With the help of unnamed employees at MKS in Shanghai, Cheng and an unnamed co-conspirator set up front companies to disguise the transactions and then fraudulently obtained U.S. export licenses, ordered the transducers from the U.S. to China, then shipped them from China to Eyvaz in Iran, violating U.S. export laws.

Between 2009 and 2011, Cheng ordered more than 1,000 MKS pressure transducers, which had a value of over $1.8 million, according to the indictment. Photographs have shown MKS pressure transducers being used at the Natanz nuclear facility in Iran.



SEALED

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	Crim. No. 13CR10332
v.	)	Violations:
SIHAI CHENG (1),	)	50 U.S.C. §1705 - Conspiracy
a/k/a CHUN HAI CHENG,	)	to Commit Export Violations;
a/k/a ALEX CHENG;	)	18 U.S.C. §371 - Conspiracy;
SEYED ABOLFAZL SHAHAB JAMILI (2);	)	50 U.S.C. §1705 - Illegal
NICARO ENG. CO., LTD. (3); and	)	Exports of U.S. Goods to Iran;
EYVAZ TECHNIC MANUFACTURING	)	18 U.S.C. §554 - Smuggling; and
COMPANY (4);	)	18 U.S.C. §981, 28 U.S.C.
	)	§2461, and 50 U.S.C. §192 -
Defendants.	)	Criminal Forfeiture.

INDICTMENT

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

A. Defendants and Their Co-Conspirators

1. SIHAI CHENG, a/k/a CHUN HAI CHENG, a/k/a ALEX CHENG ("CHENG") is a citizen of the People's Republic of China ("PRC") who is currently living in Shanghai, China. CHENG operated a trading company in the PRC, which was known as Sohi Technology Co., Ltd. ("Sohi"), until in or about December 2012 when CHENG ceased using this company name. Sohi used addresses in Shanghai, PRC, as well

Cheng is due in U.S. District Court on Monday. The charges carry maximum sentences of 10 to 20 years in federal prison.

A grand jury issued the indictment in November 2013, and the Boston Globe reported that it was unsealed in April 2014.

Kathleen Burke, general counsel for MKS, told The Republican/MassLive.com that the company has been cooperating with the United States government since an investigation was first announced in 2012.

"We have cooperated with the government authorities the entire time," Burke said.

Burke said MKS is not the target of the investigation.

She declined to discuss what actions, if any, the company has taken related to any employees in Shanghai. "It's a U.S. government action," Burke said. "We've cooperated entirely with them, and they're taking action."

▶ **Read the indictment document at source's URL.**

Sunken Soviet Submarines Threaten Nuclear Catastrophe in Russia's Arctic

Source: http://www.themoscowtimes.com/business/article/sunken-soviet-submarines-threaten-nuclear-catastrophe-in-russias-arctic/511150.html

While Russia's nuclear bombers have recently set the West abuzz by probing NATO's air defenses, a far more certain danger currently lurks beneath the frigid Arctic waters off Russia's northern coast — a toxic boneyard for Soviet nuclear ships and reactors whose containment systems are gradually wearing out.

Left to decay at the bottom of the ocean, the world is facing a worst case scenario described as "an Arctic underwater Chernobyl, played out in slow motion," according to Thomas Nilsen, an editor at the Barents Observer newspaper and a member of a Norwegian watchdog group that monitors the situation.

According to a joint Russian-Norwegian report issued in 2012, there are 17,000 containers of nuclear waste, 19 rusting Soviet nuclear ships and 14 nuclear reactors cut out of atomic vessels at the bottom of the Kara Sea.

When the Soviets first began dumping the spent nuclear fuel, the disposal method was standard practice across the globe.

"Most nuclear states had similar practices before the early 1970s," including the U.S. navy, Dr. Eugene Miasnikov, head of the Moscow-based Center for Arms Control, Energy and Environmental studies told The Moscow Times.

But while other nations abandoned the practice of dumping radioactive waste at sea, the Soviet Union continued to do so until its collapse in 1991, and did so in larger volumes than other nuclear powers.

Dr. Nils Bohmer, the managing director of the Bellona Foundation — a prominent Norwegian environmental NGO that works Arctic nuclear waste issues — explains this discrepancy by the fact that the Soviet navy experienced significantly more nuclear incidents than anyone else.

Some of the thousands of containers have already shown signs of leakage, according to Nilsen of the Barents Observer. But the threat posed by these small objects pales in comparison with the spent reactor fuel housed in the rusting carcasses of three Soviet-era nuclear submarines and a number of individual reactor compartments torn from their original vessels and dropped in the ocean.

"Counted in radioactivity, you could say that one single reactor compartment with spent nuclear fuel inside contains much more radioactivity than all the thousands of containers combined," Nilsen said.

Because their hulls are thick, the reactor compartments won't rust as quickly as the containers, but they will eventually rust open and their cargo — spent uranium fuel — is of great concern.

K-27 — The Biggest Threat

The experts polled by The Moscow Times agreed the greatest and most immediate environmental threat posed by Soviet nuclear dumping comes from the carcass of the K-27 Soviet nuclear submarine.

The K-27 was sunk in the early 1980s after the Soviets tried to tame its dangerous reactors for a decade before sinking it in the Kara Sea.

The Bellona Foundation's Bohmer, a nuclear physicist, said the K-27's two experimental liquid-metal cooled reactors pose a significant threat to the Arctic ecosystem. If the reactor's casing fails and exposes its highly enriched uranium fuel to the water, it may go critical, a 2012 Norwegian government report on the submarine said.

Bellona Foundation – The K-159 with a rusted and shoddy hull and pontoons welded to its side before being towed to the town of Polyarny.

In the case of a nuclear reaction, this does not mean that a nuclear explosion may take place in the Kara Sea, but instead create a Chernobyl-like event in which super-hot nuclear fuel will escape its reactor and emit massive levels of radiation into the environment.

Beyond the Kara Sea, there are at least two more Soviet nuclear submarines with dangerous reactors. The K-159 in the Barents Sea and the K-278 in the Norwegian Sea. The K-278, also known as the Komsomolets, is considered to have settled too deep for salvage.

The K-159 went down in 2003 while it was being towed to the town of Polyarny — home of Russia's primary shipyard used for servicing and decommissioning nuclear powered vessels — for dismantling. Nine sailors died trying to keep it afloat when a storm hit, ripping off makeshift pontoons welded to the side to ensure the porous rusting hull didn't sink en route. Estimates place around 800 kilograms of spent uranium fuel aboard the K-159, according to Bellona.

"Unfortunately, to my knowledge, there are currently no concrete plans to raise [radioactive] objects, and potentially raising the submarine is a Russian responsibility," said Ingar Amundsen, head of the section for international nuclear issues at the Norwegian Radiation Protection Authority (NRPA), a governmental body tasked with keeping watch over the nuclear threats in the Arctic.

Uncertain Outcome

Despite the dire warnings of environmentalists, the reason that the submarines have not yet been lifted is that no one knows if it is possible to do so safely, and the consequences of leaving them at the bottom are yet unknown.

Raising a submarine is also an expensive and highly technical operation that Russia would likely have to outsource, as it did with the raising of the Kursk nuclear submarine in 2001 for $150 million.

Alexander Shestakov, head of the World Wildlife Fund's Global Arctic Program, said in 2012 that changing ocean currents, resulting from Arctic thaws propelled by global warming, could end up carrying Soviet radioactive waste — when the reactors and containers are breached by corrosion — far beyond the Arctic, according to one Bellona report.

For Nilsen, a resident of Norway, the threat hits closer to home.

"For those of us living along Norway's Arctic coastline, the dumped nuclear reactors in the Kara Sea cause great concern. We share the Arctic cod and other marine resources with Russia, and any leakages of radioactivity in the Kara Sea will scare everyone that eats fish from the nearby Barents Sea," Nilsen said.

The Barents Sea alone accounts for some 1 million to 3.5 million tons of fishing each year, and is the world's largest remaining source for Atlantic cod. The size of the Barents fishing industry in 2013 was valued at $2 billion, leaving the Norwegian and Russian fishing industries deeply reliant on the area, and vulnerable to the effects of contamination. Even a false alarm could cause a health scare that would hit fishermen hard.

However, Bellona's Bohmer said it is far from clear how best to handle the situation. "I think it is important the Russian authorities take the initiative to do a risk evaluation: What are the risks of having the reactors sitting at the bottom and rusting away compared with the risk of raising the submarines? Raising the submarines could also be a risky operation because the K-159 especially is in a very bad condition. There will be a risk either way, and I think its important to do that evaluation."

While some cite the raising of the Kursk as a technological precedent for raising other submarines, the Kursk was in significantly better condition than the K-159 or the K-27. A similar attempt to raise a Russian submarine off the Pacific Ocean floor in 1974 — the CIA's infamous Project Azorian — ended up losing half of the submarine when one of the claws grasping the submarine failed.

Nilsen of the Barents Observer said the risk of leaving the reactors on the bottom far outweighs the risk of lifting them.

Russia's Next Steps

The Moscow Times was unable to reach state nuclear agency Rosatom or the Natural Resources and Environment Ministry or clarification on their position, characterization of the ecological threat, and plans to raise the submarines.

However, Russia's marine ecology watchdog, Roshydromet, which took part in September's expedition to the K-159 gravesite, said in an official statement that "the content of radioactive substances in the vicinity of the submarine does not differ from baseline values characteristic of the Barents Sea."

Roshydromet said that "the available data to date suggests that the leakage of radioactive substances from the reactors of the boat into the marine environment has not occurred," but added that final conclusions will be released after lab analysis in Norway and Russia has concluded on the most recent data.

In the meantime, the advent of the Arctic oil rush — focused heavily on the Kara Sea — has forced the Russian authorities to pay greater attention to the threat of nuclear waste in the area. But although awareness is rising, there is not yet any impetus to conduct salvage operations in the near term as the risk of a drilling operation sparking a contamination event is considered to be remote.

Rosatom, which has been busy in recent years decommissioning still-floating Soviet era nuclear submarines, has expressed interest in retrieving both submarines,

Bellona has said — but so far no timeline for this has emerged.
The Bellona Foundation estimates that the first incidents may begin taking place around 2020 or, in the best-case scenario, 2030.

And so for the moment, the radioactive waste across the Arctic seabed remains safely contained in their casings. But "sooner or later, the radiation will leak out," Nilsen said.

Read also:

A radiological disaster waiting to happen in the Arctic waters
Source: http://www.cbrneportal.com/ibc-threat-assessment-december-2014/

The Fukushima Endgame: The Radioactive Contamination of the Pacific Ocean

By Prof Michel Chossudovsky
Source: http://www.globalresearch.ca/the-fukushima-endgame/5420188

Nuclear radiation resulting from the March 2011 Fukushima disaster –which threatens life on planet earth– is not front page news in comparison to the most insignificant issues of public concern, including the local level crime scene or the tabloid gossip reports on Hollywood celebrities.

The shaky political consensus both in Japan, the U.S. and Western Europe is that the crisis at Fukushima has been contained.
The truth is otherwise. Known and documented, the ongoing dumping of highly radioactive water into the Pacific Ocean constitutes a potential trigger to a process of global radioactive contamination.

This water contains plutonium 239 and its release into the Ocean has both local as well as global repercussions. A microgram of plutonium if inhaled, according to Dr. Helen Caldicott, can cause death:
Certain isotopes of radioactive plutonium are known as some of the deadliest poisons on the face of the earth. A mere microgram (a speck of darkness on a pinhead) of Plutonium-239, if inhaled, can cause death, and if ingested, radioactive Plutonium can be harmful, causing leukemia and other bone cancers.
"In the days following the 2011 earthquake and nuclear plant explosions, seawater meant to cool the nuclear power plants instead carried radioactive elements back to the Pacific ocean. Radioactive Plutonium was one of the elements streamed back to sea." (decodescience.com).
It would appear that the radioactive water has already penetrated parts of the Japanese coastline:
Environmental testing of shoreline around the nuclear plant (as well fish, especially Tuna) showed negligible amounts of Plutonium in the seawater. The Plutonium, from what little is reported, sank into the sediments off the Japanese coast." (Ibid)
A recent report suggests that the Japanese government is intent upon releasing the remaining radioactive water into the Ocean. The proposed "solution" becomes the cause of radioactive contamination of both the Japanese coastline as well as the Pacific Ocean, extending to the coastline of North America.
While the chairman of the Nuclear Radiation Authority recognizes that the water in the tanks is heavily "tainted", a decision has nonetheless been taken to empty the tanks and dump the water into the Ocean:
The head of Japan's nuclear watchdog said contaminated water stored at the crippled Fukushima No. 1 nuclear power plant should be released into the ocean to ensure safe decommissioning of the reactors.
Shunichi Tanaka, the chairman of the Nuclear Regulation Authority,

made the comment Dec. 12 after visiting the facility to observe progress in dismantling the six reactors. The site was severely damaged in the tsunami generated by the 2011 earthquake.

"I was overwhelmed by the sheer number of tanks (holding water tainted with radioactive substances)," Tanaka told reporters, indicating they pose a danger to decommissioning work. "We have to dispose of the water."

With regard to expected protests by local fishermen over the discharge, Tanaka said, "We also have to obtain the consent of local residents in carrying out the work, so we can somehow mitigate (the increase in tainted water)."

Tanaka has said previously that to proceed with decommissioning, tainted water stored on the site would need to be released into the sea so long as it had been decontaminated to accepted safety standards.

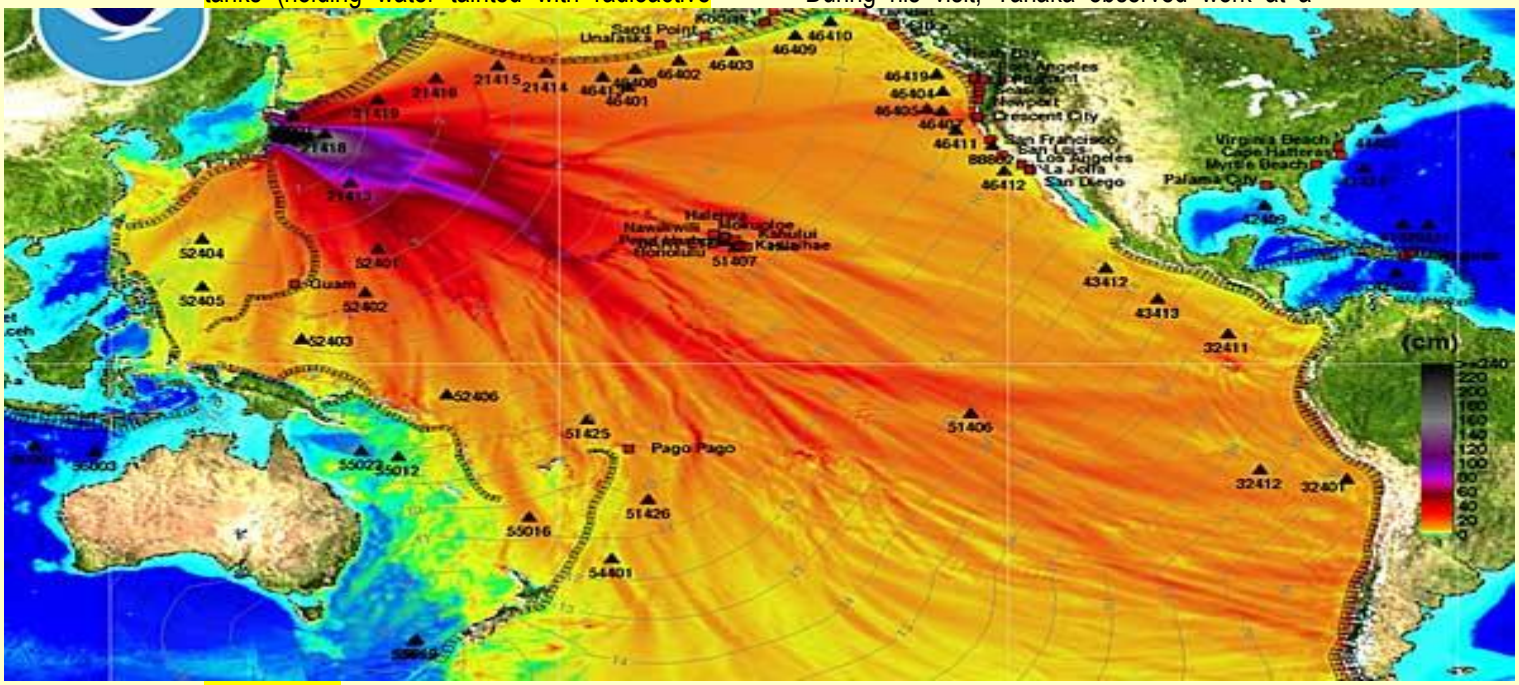
"While (the idea) may upset people, we must do our utmost to satisfy residents of Fukushima," Tanaka said, adding that the NRA would provide information to local residents based on continuing studies of radioactive elements in local waters.

The inspection tour was Tanaka's second since he became NRA chief in September 2012. He last visited in April 2013.

During his visit, Tanaka observed work at a trench on the ocean side of the No. 2 reactor building, where highly contaminated water is being pumped out. He also inspected barriers set up around the storage tanks to prevent leaks of tainted water.

Tanaka praised the completion in November of work to remove all spent nuclear fuel from the No. 4 reactor building, as well as changes to work procedures that he said allows for the completion of the work at the No. 2 reactor trench. Hiromi Kumai , NRA Head Signals Massive Release of Tainted Water to Help Decommission Fukushima Site Asahi Shimbun December 13, 2014

The contradictory statements of the NRA chief avoid addressing the broader implications, by giving the impression that the issue is local and that local fishermen off the Fukushima coast will be consulted.



Michel Chossudovsky *is an award-winning author, Professor of Economics (emeritus) at the University of Ottawa, Founder and Director of the Centre for Research on Globalization (CRG), Montreal and Editor of the globalresearch.ca website. He is the author of The Globalization of Poverty and The New World Order (2003) and America's "War on Terrorism"(2005). His most recent book is entitled Towards a World War III Scenario: The Dangers of Nuclear War (2011). He is also a contributor to the Encyclopaedia Britannica. His writings have been published in more than twenty languages.*

TEXT BOX

Nuclear Radiation: Categorization

At Fukushima, reports confirm that alpha, beta, gamma particles and neutrons have been released: "While non-ionizing radiation and x-rays are a result of electron transitions in atoms or molecules, there are three forms of ionizing radiation that are a result of activity within the nucleus of an atom. **These forms of nuclear radiation are alpha particles (α-particles), beta particles (β-particles) and gamma rays (γ-rays). Alpha particles** are heavy positively charged particles made up of two protons and two neutrons. They are essentially a helium nucleus.

Beta particles are just electrons that have been ejected from the nucleus. This is a result of sub-nuclear reactions that result in a neutron decaying to a proton. The electron is needed to conserve charge and comes from the nucleus. It **is not** an orbital electron. β-particles are positrons ejected from the nucleus when a proton decays to a neutron. A positron is an *anti-particle* that is similar in nearly all respects to an electron, but has a positive charge.

Gamma rays are photons of high energy electromagnetic radiation (light). Gamma rays generally have the highest frequency and shortest wavelengths in the electromagnetic spectrum. There is some overlap in the frequencies of gamma rays and x-rays; however, x-rays are formed from electron transitions while gamma rays are formed from nuclear transitions.

"**A neutron** is a particle that is found in the nucleus, or center, of atoms. It has a mass very close to protons, which also reside in the nucleus of atoms. Together, they make up almost all of the mass of individual atoms. Each has a mass of about 1 amu, which is roughly 1.6×10-27kg. Protons have a positive charge and neutrons have no charge, which is why they were more difficult to discover."

"Many different **radioactive isotopes** are used in or are produced by nuclear reactors. The most important of these are described below:

1. Uranium 235 (U-235) is the active component of most nuclear reactor fuel.

2. Plutonium (Pu-239) is a key nuclear material used in modern nuclear weapons and is also present as a by-product in certain reprocessed fuels used in some nuclear reactors. Pu-239 is also produced in uranium reactors as a byproduct of fission of U-235.

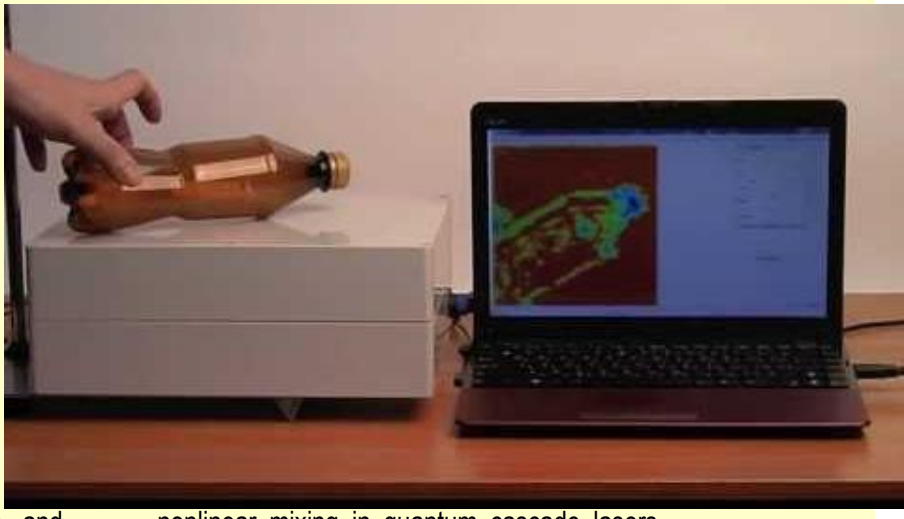
3. Cesium (Cs-137) is a fission product of U-235. **It emits beta and gamma radiation** and can cause radiation sickness and death if exposures are high enough. …

4. Iodine 131 (I-131), also a fission product of U-235, **emits beta and gamma radiation**. After inhalation or ingestion, it is absorbed by and concentrated in the thyroid gland, where its beta radiation damages nearby thyroid tissue (SOURCE: Amesh A. Adalja, MD, Eric S. Toner, MD, Anita Cicero, JD, Joseph Fitzgerald, MS, MPH, and Thomas V. Inglesby MD, Radiation at Fukushima: Basic Issues and Concepts, March 31, 2011)

New terahertz device could strengthen security

Source: http://www.homelandsecuritynewswire.com/dr20141124-new-terahertz-device-could-strengthen-security

We are all familiar with the hassles that accompany air travel. We shuffle through long lines, remove our shoes, and carry liquids in regulation-sized tubes. Even after all the effort, we still wonder whether these procedures are making us any safer. **Now a new type of security detection that uses terahertz radiation is looking to prove its promise. Able to detect explosives, chemical agents, and dangerous biological substances from safe distances, devices using terahertz waves could make public spaces more secure than ever.**



Current terahertz sources, however, are large, multi-component systems that sometimes require complex vacuum systems, external pump lasers, and even cryogenic cooling. The unwieldy devices are heavy, expensive, and hard to transport, operate, and maintain.

"A single-component solution capable of room temperature and widely tunable operation is highly desirable to enable next generation terahertz systems," said Manijeh Razeghi, Walter P. Murphy Professor of Electrical Engineering and Computer Science at Northwestern University's McCormick School of Engineering and Applied Science.

A Northwestern university release reports that Razeghi, director of Northwestern's Center for Quantum Devices, and her team have been working to develop such a device. In a recent paper in *Applied Physics Letters*, they demonstrate a room temperature, highly tunable, high power terahertz source. Based on nonlinear mixing in quantum cascade lasers, the source can emit up to 1.9 milliwatts of power and has a wide frequency coverage of 1 to 4.6 terahertz. By designing a multi-section, sampled-grating distribution feedback and distributed Bragg reflector waveguide, Razeghi and her team were also able to give the device a tuning range of 2.6 to 4.2 terahertz at room temperature.

The device has applications in medical and deep space imaging as well as security screening.

"I am very excited about these results," Razeghi said. "No one would believe any of this was possible, even a couple years ago."

— Read more in Q. Y. Lu et al., "Widely tunable room temperature semiconductor terahertz source," Applied Physics Letters *105, 201102 (2014)*

Dogs trained on pseudo-explosives could not reliably identify genuine explosives

Source: http://www.homelandsecuritynewswire.com/dr20141125-dogs-trained-on-pseudoexplosives-could-not-reliably-identify-genuine-explosives

When it comes to teaching dogs how to sniff out explosives, there is nothing quite like the real thing to make sure they are trained right. This is the message from William Kranz, Nicholas Strange, and John Goodpaster of Indiana University-Purdue University Indianapolis (IUPUI), after finding that **dogs that are trained with so-called "pseudo-explosives" could not reliably sniff out real explosives** (and vice versa). Their findings are published online in Springer's journal *Analytical and Bioanalytical Chemistry*.

A Springer release reports that genuine explosive materials are traditionally used to train dogs to detect explosives and to test their performance later on. However, challenges arising from the acquisition, storage, handling, and transport of explosives have motivated the development of "pseudo-explosive" or "pseudo-scent" training aids. These products attempt to mimic the odor of real explosives, yet remain non-hazardous. The intent is that a canine trained on a pseudo-explosive would be able to detect its real-life analog, and vice versa.

Using randomized blind testing, Goodpaster's research group tested how well a group of seventeen dogs were able to locate three types of explosives and their pseudo-versions: single-base smokeless powder, 2,4,6-trinitrotoluene (commonly known as TNT), and a RDX-based plastic explosive (Composition C-4).

In general, **the dogs trained on simulated explosives could sniff out the genuine article only 14 percent of the time.** **Similarly, dogs trained on real explosives responded to pseudo-explosives only 16 percent of the time.** In fact, on the whole, the animals only had a nose for

the materials upon which they were trained. **For example, dogs trained on real explosives were able to locate them 81 percent of the time.** Dogs trained with the pseudo-explosive versions had a very similar success rate of 88 percent.

The failure of the dogs to be "cross-trained" does not mean that the pseudo-explosives contain the wrong ingredients. Goodpaster's group determined via chemical analysis that the volatile compounds given off by pseudo-explosives consist of various solvents, additives and common impurities that are present in authentic explosives.

Ultimately, Goodpaster's group states that "the exceptional sensitivity of the canine's nose and the impressionable nature of its temperament have made canines a valuable tool when it comes to sweeping for hidden bombs and explosives. **However, dogs trained on pseudo-explosives performed poorly at detecting all but the pseudo-explosives they were trained on. Similarly, dogs trained on actual explosives performed poorly at detecting all but the actual explosives on which they were trained."**

— Read more in W. D. Kranz et al., "'Fooling fido' — chemical and behavioral studies of pseudo-explosive canine training aids," Analytical and Bioanalytical Chemistry *(2014)*

Bird Bomb? Afghan Police Kill Bird Bearing Antenna, Explosives

Source: http://www.nbcnews.com/news/world/bird-bomb-afghan-police-kill-bird-bearing-antenna-explosives-n258216

Afghan police said they are investigating how a wild bird came to bear an antenna, electronic devices and explosives. Police came across the strange sight around 8 a.m. in the northern Faryab province, a volatile region ravaged by Taliban violence. When police spotted the white bird — which isn't native to the area and appeared larger than an eagle — walking along a highway, they noticed it had an antenna and decided to shoot it, provincial police chief Maj. Gen. Abdul Nabi Ilham told NBC News on Saturday. The bird then exploded, he said, and "suspicious metal stuff" scattered around.

"We are gathering all the stuff, but found parts of what looks to be GPS and a small camera," Ilham said. He added that this was the first time police have made such an encounter. Police added that it is possible the bird had been "deployed" on a surveillance

mission. Using animals in warfare or for suicide missions is unusual but not unheard of.

Hamas militants reportedly put explosives on a donkey and pushed it in the direction of Israeli soldiers as fighting intensified this summer in Gaza.

EDITOR'S COMMENT: Dedcated to all those who claim to be smarter than terrorists! As long as they do not think like terrorists, they are NOT!

Improving nuclear power plant safety by looking at nature

Source: http://www.homelandsecuritynewswire.com/dr20141205-improving-nuclear-power-plant-safety-by-looking-at-nature

Taking inspiration from nature, researchers have created a versatile model to predict how stalagmite-like structures form in nuclear processing plants — as well as how lime scale builds up in kettles.

"It's a wonderful example of how complex mathematical models can have everyday applications," said Dr. Duncan Borman, from the School of Civil Engineering at the University of Leeds, a co-author of the study.

A University of Leeds release reports that the main aim of the research, which is published in print today in the journal *Computers & Chemical Engineering*, is to reduce the number of potentially harmful manual inspections of nuclear waste containers.

"We were approached by the National Nuclear Laboratory and Sellafield Ltd to solve the problem of predicting the shapes that precipitates from nuclear process solutions can form in containment chambers," said Dr. Borman.

Study co-author Professor Daniel Lesnic from the School of Mathematics at the University of Leeds, added: "Our first thought was to find a suitable analogy in nature. At first we looked at how lava flows from a volcano to the ocean, but the formation of stalagmites in caves mimics the process much more closely.

"Geologists have well-established models for the formation of stalagmites. So we are taking models from one field of science and applying them to a completely different discipline."

Within the nuclear industry, hazardous salt solutions can arise within industrial containment vessels. The salt solution precipitates out, forming structures with strange morphologies that bear a resemblance to stalagmites. If left unchecked, they could build up and cause a problem in the nuclear containment chamber. Currently, these containment chambers are checked regularly to prevent this from happening.

In the study, the researchers used an existing model for predicting stalagmite growth over millions of years as a starting platform. To take into account the full complexity of the mechanism by which the solid is formed, the model was then adapted to

include the chemical and physical properties of the particular salt solution of interest to the nuclear industry, a more realistic fluid flow, and to consider the sensitivity of results to varying temperature.

Lead author of the study, Dr. Mike Dawson from the School of Chemical and Process Engineering at the University of Leeds, who started the research during his Ph.D. studies, said: "It took many months of intensive research to develop the model. The big test came when we tested the model against real data from the National Nuclear Laboratory.

"Our model stood up to the test. For the first time it was possible to predict the morphology of these complex crystallizing flows reliably."

Dr. Borman said: "This breakthrough provides a new tool for the National Nuclear Laboratory and Sellafield Ltd, with the potential to save both money and continue to ensure they are at the forefront of world-leading safety technology."

The new model also has wider application to other industrial and domestic situations where a salt solution precipitates out and causes problems, such as forecasting the precise shape and location of build-up in pipes or heat exchangers — or how lime scale will collect within a kettle.

Dr. Borman said: "The processes underlying the build up of lime scale in a kettle are remarkably similar: the flow of a liquid containing a dissolved mineral — in this case calcium carbonate from hard water — over a surface of changing temperature, can result in solids precipitating out and leaving the build up of solid material behind.

"Using the model we have developed, manufacturers could improve the design of kettles such that these unwanted build-ups are minimised by repositioning filaments or designing them so that deposits form in locations that are easy to clean."

▶ **Read the full paper at:** http://www.sciencedirect.com/science/article/pii/S0098135414002701

Studying the long-term aging of electronics in nuclear weapons

Source: http://www.homelandsecuritynewswire.com/dr20141205-studying-the-longterm-aging-of-electronics-in-nuclear-weapons

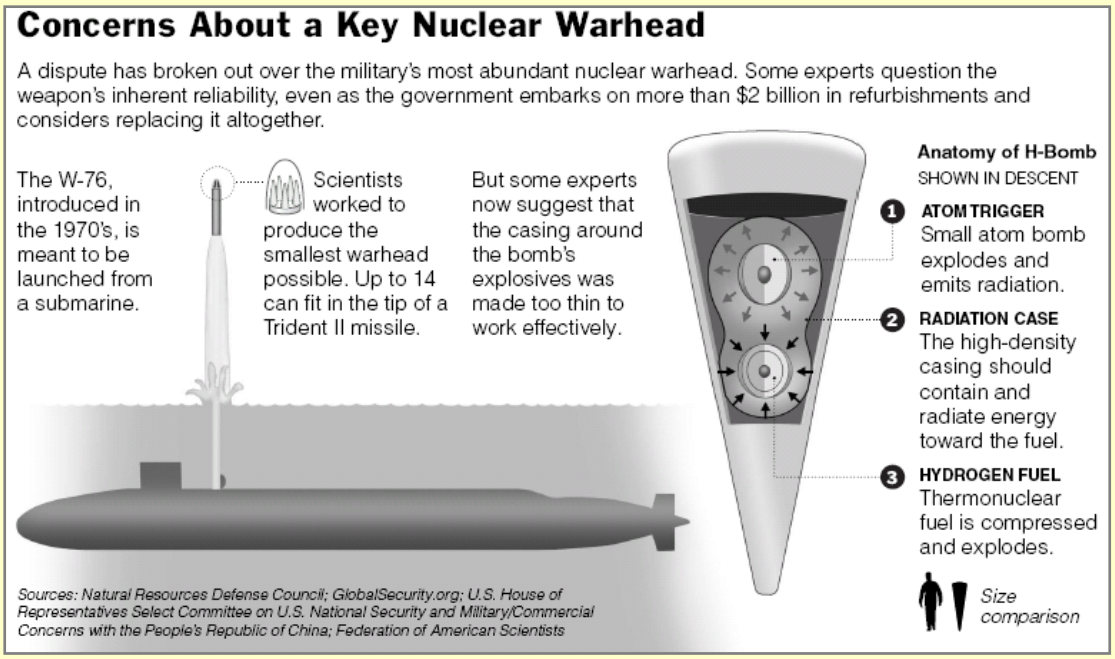
Sandia National Laboratories is studying how environments, including radiation which originates from a nuclear weapon itself, could affect the performance of electronics in the W76-1 warhead as they age.

Sandia, which is responsible for most non-nuclear components in U.S. nuclear weapons, is helping replace W76 warheads in the U.S. stockpile with a refurbished version under the W76-1 Life Extension Program (LEP). **The ballistic missile warhead is carried on the Trident II D5 missile aboard Ohio-class Navy submarines.**

A Sandia Lab release reports that researchers have studied radiation effects since the early days of nuclear weapons, but a 30-year program, which begun in 2006, will provide real-time data for the first time on how electronics age within the weapon. Studies in the past used techniques that artificially accelerated the aging process based on a range of assumptions resulting from experiments and previous research.

"There has always been the question with accelerated aging data, how reliable is it?" said principal investigator Rachelle Thompson.

The long-term project combines experiments, also known as physical simulation, with computational simulation and analysis. The approach developed as part of this project can be used in future LEPs, said Steve Wix, manager of Sandia's Component and Systems Analysis Department. Costs should be reduced for future stockpile surveillance and monitoring as well, since such lab-based studies cost less than accelerated aging techniques, which require using large environmental test facilities.



Study important in moving more toward predictive models

The project by Sandia's Electrical Sciences Group is important for science-based stockpile stewardship because new devices, or electronic parts, have been introduced into the W76-1 system since production began in 2008. These new parts must function with assured reliability and performance throughout the life of the system. The project also is moving such evaluations toward more predictive models of aging for stockpile stewardship, Wix said. Stockpile stewardship assures the safety, security and reliability of weapons in the absence of the underground nuclear tests the United States halted in 1992.

Most of the experiments and analysis are done in a small laboratory full of racks of test and computer equipment and in an adjacent room packed with small test chambers, square white boxes that resemble miniature refrigerators. Each test chamber contains parts in a unique environment that is continually monitored to control temperature, relative humidity and vibration frequency to ensure consistent levels of the multiple aging processes that will take decades. The experiments are overseen by test engineer Monica Espinosa.

Researchers develop and use advanced, physics-based computational simulations to predict how the electronics will perform as they age. They verify their predictions with experiments on the electronics to improve their understanding of the underlying physics engaged during the aging process. This research then guides further development of these critical simulation capabilities to resolve differences between the computer simulations and the aging experiments.

The researchers monitor thousands of devices that fall into six families of transistor and diode types. Hundreds are removed annually from the test chambers to determine their electrical performance under various operating conditions. The long-range test schedule was developed to assure that an adequate number of devices remain available for testing over the entire three decade-long study.

The parts under study were pristine when the project started eight years ago. Wix and Thompson said no significant aging changes were expected in these early years, and what they have seen matches those predictions. Currently, only simple electrical devices are being tested, but

researchers hope to add more complex parts later in the project.

Project exposes aged devices to laser-based testing

Once devices have aged in the predetermined storage environments, the team uses a sophisticated laser-based technique to expose each one to more hostile short-duration operating environments, Thompson said.

Researchers take basic electrical measurements on the aged transistors and diodes, then repackage them in preparation for evaluation with a benchtop laser-based simulated radiation environment source. They expose the parts to two different types of lasers: a broad beam that sweeps the entire device and a focused laser beam to expose it in specific areas. This process evaluates the performance of aged devices in more harsh environments.

It takes up to fifteen to twenty minutes for each laser study of a part, and the project studies hundreds of parts per year, Thompson said. "There is a lot of handling of parts and data analysis involved," she said.

The release notes that unless the part is damaged or fails during testing, it goes back into the appropriate aging environment for future testing. A damaged or failed part is evaluated to better understand the underlying cause.

The techniques Sandia is developing will help officials make future stockpile decisions based on an improved understanding of the impact of aging on how parts perform in multiple environments, Wix said.

The science of airport bomb detection: chromatography

By Martin Boland

Source: http://www.homelandsecuritynewswire.com/dr20141212-the-science-of-airport-bomb-detection-chromatography

As the holidays draw near, many of us will hop on a plane to visit friends and family — or just get away from it all. Some will be subjected to a swab at the airport to test clothes and baggage for explosives. So how does this process work?

The answer is chromatography — a branch of separation chemistry — along with mass spectrometry (which I will address in a later article).

The word "chromatography" is roughly translated from Greek as "the science of colors." The reason for the name becomes obvious when you realize that most people have accidentally performed a simple chromatography experiment.

If you've ever spilled water onto a hand-written shopping list, then held it up to let the water run-off, you've probably noticed the ink diffuses across the paper, and that the pen's color is made up from several pigments (if you've not, you can do the experiment — try it with a couple of pens of different brands, but the same color). This separation is chromatography.

There are several different types of chromatographic separation. What they all have in common is that a mixture of materials that need to be separated (the analytes) is washed over a solid material (called the matrix), causing the analytes to separate.

That may sound like chromatography is just filtration, or separation by particle size. In some cases, that is almost exactly what happens (size exclusion chromatography is often referred to as gel filtration chromatography).

But most chromatography methods work by some other chemical effect than just the size of the materials being separated, including (but not limited to):

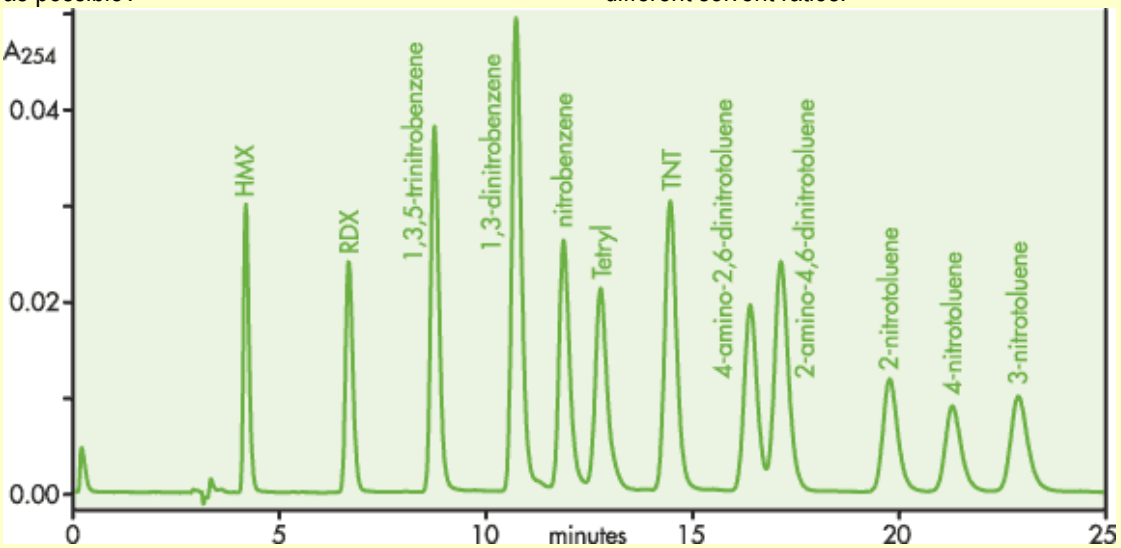
- **normal-phase chromatography**, such as ink on paper
- **reverse-phase chromatography**, often used in university lab experiments
- **gas chromatography**, seen in airport bomb detectors
- **capture chromatography**, used to purify drugs.

Each of these can be performed with one solvent, such as dropping water on your shopping list – known as isocratic (Greek for "equal power") or with a changing mixture of solvents (known as a gradient).

So how does it work?

Technically speaking, it is the differential affinity of the analyte for the solvent and the solid

matrix that drives chromatographic separation. So what does that mean, really?
You'll need to bear with me here.
Have you ever been shopping with someone who stops to look at things while you're trying to move though the store as quickly as possible?



That differential attraction to the stuff surrounding you — that's what drives chromatography. You walk through the aisles only rarely interacting with the goods on sale, while your shopping partner has much greater affinity for the shelves and stops frequently. By the time you're at the exit they are still only halfway through the shop — you've separated!
That is what happens to molecules. The solvent flows over the matrix (in the shopping list case, the paper) carrying the analytes. The relative affinity of the analyte for the matrix compared with the solvent determines the separation.
If a compound is totally insoluble in the solvent, it stays fixed to the matrix (you may have seen this when spilling water on a shopping list written in pencil). If the analyte is very soluble, it may move as fast as the solvent.
The shopping list example is called planar chromatography. The running ink seems to defy gravity, moving up the paper due to the capillary effect. More common in high-performance chromatography, the matrix is a column with the solvent forced over it, by gravity or pumping.
Using a column makes it easier to change the ratio of solvents by using a pump that can mix multiple materials (usually a mixture of water and a soluble organic solvent such as acetonitrile).

In the case of a gradient separation, the analyte has much higher affinity for the matrix than for the initial solvent mixture. As the solvent mix is changed, the analyte dissolves in the solvent and is carried out of the column separated from materials that are soluble in different solvent ratios.

Sometimes it's a gas, gas, gas

For gas chromatography, the set-up is a little different. The analytes are gases or volatile liquids (think petrochemicals, plant oils, chemical weapons). Such compounds are usually non-polar and hydrophobic – in other words, they don't mix well with water.
The compounds are evaporated into an inert carrier gas (analogous to dissolving in a solvent). The carrier gas transports the compound over a hydrophobic matrix contained in a coiled column (often tens of meters long but only micrometers wide).
To improve separation, and allow analysis of materials with a higher boiling point (up to around 300C), the column is placed in an oven. Changing the temperature of the oven affects separation in a similar way to changing the mixture of solvents in liquid chromatography.

Quality control

When separating colored compounds it's pretty obvious when the process has worked. But how do you know if you've separated two colorless compounds, or separated microscopic amounts of analyte?
There are several ways to detect the analytes depending on their chemical and/ or physical properties. Among the more common are:

- ultraviolet or infrared (non-visible but optical wavelength) absorbance
- non-visible fluorescence
- conductivity or pH (how acidic the solution is)
- collect samples and perform chemical tests
- mass spectrometry.

Probably the most useful of these is mass spectrometry as it allows the analyst to work out exactly what compound they are seeing without needing prior knowledge of what was in the original analyte mixture.

An ever-developing world

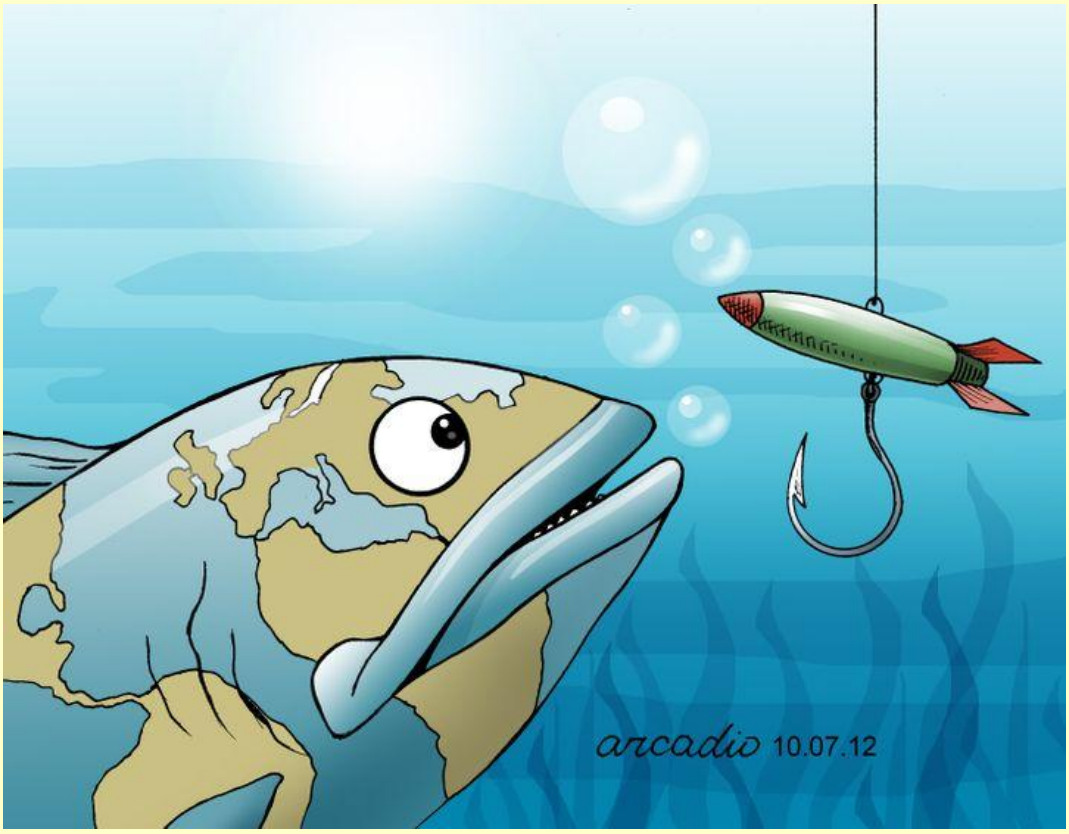
Although instrumental chromatography is a mature technology (the first instruments were produced just after WWII), new applications frequently pop up.

Some are a matter of scale. Pharmaceutical companies that produce monoclonal antibodies (often used in cancer treatments) make use of capture chromatography to purify their products. On an industrial scale these can be tens of centimeters in diameter and meters in length (typical lab scale systems are a few millimeters diameter and 5-30cm long).

Other uses can either be in a specific new application, such as detecting cocaine on bank notes using the gas chromatography systems often seen at airports as bomb and drug detectors.

And even more exciting experiments are being done by chromatography instruments on board the Philae probe that detected organic chemicals on the comet 67P/Churyumov–Gerasimenko.

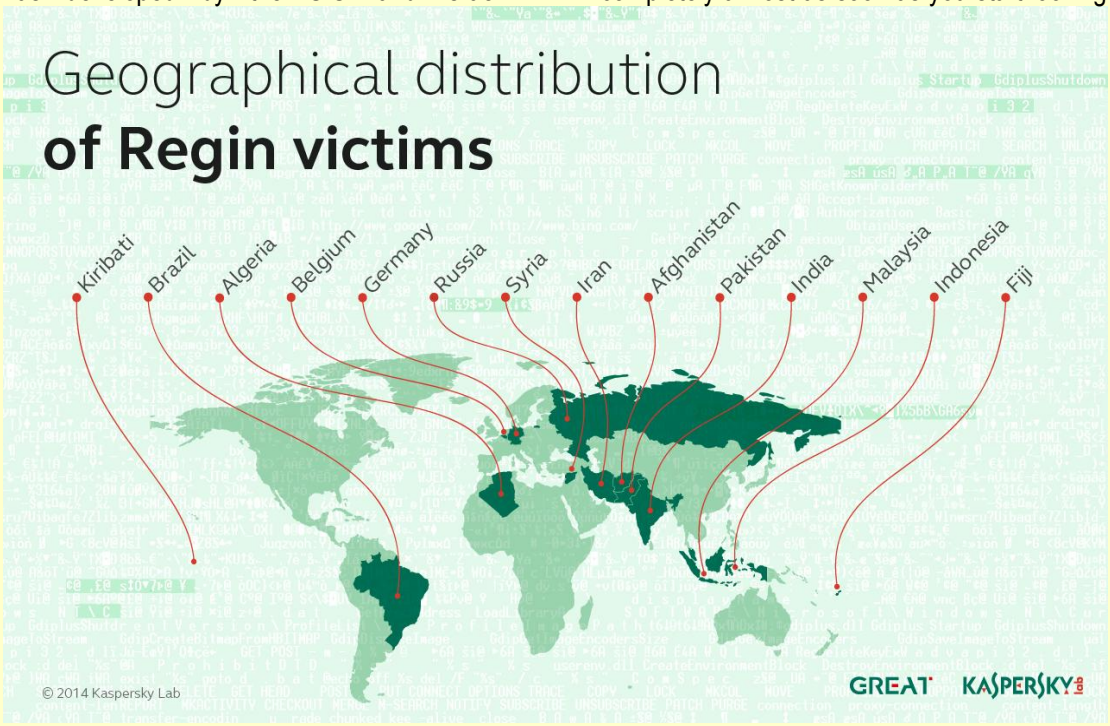
Martin Boland *is Senior Lecturer of Medicinal and Pharmaceutical Chemistry at Charles Darwin University.*



A malware more sophisticated than Stuxnet discovered

Source: http://www.homelandsecuritynewswire.com/dr20141125-a-malware-more-sophisticated-than-stuxnet-discovered

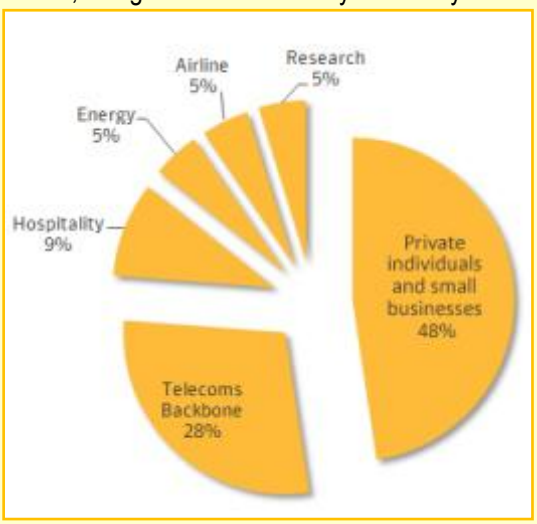
November 25 – **Security experts at Symantec have discovered the world's most sophisticated computer malware, Regin.** Thought to have been created by a Western intelligence agency, and in many respects more advanced than Stuxnet — which was developed by the U.S. and Israeli government in 2010 to hack the Iranian nuclear program — **Regin has targeted Russian, Saudi Arabian, Mexican, Irish, and Iranian Internet service providers and telecoms companies. "Nothing else comes close to this … nothing else we look at compares,"** said Orla Cox, director of security response at Symantec.



One Western security official told CNBC News that it is difficult to ascertain the origins or purpose of Regin. "It's dangerous to assume that because the malware has apparently been used in a given country, it did not originate there," the official said. "Certain states and agencies may well use tools of this sort domestically."

Regin's attacks begin with a Trojan horse that exploits a security vulnerability while avoiding detection. Soon after, customized frameworks are built within a system to take control of targeted functions. Regin has already hacked Microsoft e-mail exchange servers and mobile phones on major global networks.

"We are probably looking at some sort of western agency," Cox said. "Sometimes there is virtually nothing left behind — no clues. Sometimes an infection can disappear completely almost as soon as you start looking at it, it's gone. That shows you what you are dealing with."



Regin infections occurred between 2008 and 2011, then a new version resurfaced in 2013.

Eugene Kaspersky, chief executive of Kaspersky Labs, the Russian company that helped uncover Stuxnet, recently told the *Financial Times* that criminals not sponsored by governments are now also hacking industrial control systems for financial gains. Criminal cyberattacks go beyond the credit card breaches at U.S. banks and retailers, they also include bypassing security at ports. Last year, Europol disrupted a drug ring that was hacking into the control systems of the Port of Antwerp to move containers hiding drugs away from customs inspectors.

Still, Liam O'Murchu, a security researcher at Symantec, insists that Regin is primarily used for espionage. "We see both companies and individuals targeted. The ultimate goal is to listen in on phone calls or something like that. [Regin's operators] target individuals and spread the attack to find whatever it is they're looking for. All of these things together make us think that a government wrote it," she told *Time Magazine*.

On Monday, security industry sources told *The Intercept* that European Union computer systems and Belgacom, a Belgian telecommunications company, were victims of Regin attacks carried out by the National Security Agency and the British spy agency, Government Communications Headquarters (GCHQ). Ronald Prins, a security expert with Fox IT, hired to remove the malware from Belgacom's networks, told *The Intercept* that he was "convinced Regin is used by British and American intelligence services."

U.S. Army creates a Cyber branch

Source: http://www.homelandsecuritynewswire.com/dr20141126-u-s-army-creates-a-cyber-branch

November 25 – Soldiers who want to defend the nation in cyberspace, as part of the U.S. Army's newest and most technologically advanced career field, now have an Army branch to join that will take its place alongside infantry, artillery and the other Army combat arms branches.

The insignia of the U.S. Army cyber command // Source: army.mil

Army Secretary John McHugh and Chief of Staff Gen. Raymond Odierno approved the creation of the Cyber branch in September, as one of the first official steps in establishing a 17-series career field specifically dedicated to managing the careers and professional development of officers. The remainder of the 17-series career field management program is expected to be implemented by October 2015, with both enlisted and warrant officer career paths.

"This is a historic development for our Army, for the soldiers who are already defending the nation in cyberspace, and for those who will do so in years to come," said Maj. Gen. Stephen G. Fogarty, commanding general of the Cyber Center of Excellence. "Creation of the Cyber branch acknowledges the critical role that our cyber warriors play in the armed forces of today and tomorrow, and it will provide us with the structure to make certain that the highly skilled Soldiers who are selected for these positions are well-trained, professionally developed and appropriately assigned."

The Army says that to support these goals, both the U.S. Army Cyber Center of Excellence, or CoE, at Fort Gordon, and the Human Resources Command created personnel career management and proponent offices to lead and shape the future development of this new Army career field.

"The establishment of a Cyber Branch shows how important and critical the cyber mission is to our Army, and allows us to focus innovative recruiting, retention, leader development, and talent management needed to produce world-class cyberspace professionals," said Lt. Gen. Edward Cardon, the commanding general of Army Cyber Command.

Cyber CoE officials say the U.S. military networks evolved from providing communication systems

and services to a warfighting weapons system. All of cyberspace is now considered a warfighting domain and an operational environment in which the Defense Department will conduct cyberspace operations. This new warfighting domain brings the need for a new type of Soldier capable of understanding cyberspace as an operational environment, just as an infantryman understands the land domain and a pilot the air domain.

"Every day, newspaper headlines underscore the importance of cyber defense to national security," said Col. Gregory Conti, director of the Army Cyber Institute at the U.S. Military Academy at West Point. "The creation of the branch lays the foundation for a professional cyber force to best protect the Nation."

The Cyber branch already reached a milestone accepting the first six officers for duty as cyber operations officers, in the 17A area of concentration. Five of the six will be assigned to the 780th Military Intelligence Brigade (Cyber), at Fort Meade, Maryand, with the sixth assigned to the Cyber Protection Brigade at Fort Gordon.

By October 2015, enlisted Soldiers joining the career field will be designated as military occupational specialty 17C, cyber operations specialist, while warrant officers will become 170A cyber operations technicians. The process for Warrant Officers and NCOs to transfer to career field 17 is under development.

According to Col. Jennifer Buckner, commandant of the U.S. Army Cyber School, within the Cyber CoE, the branch will form in two phases, with a target of bringing almost 1,200 officers, warrant officers and enlisted Soldiers into the branch during the first phase, through 2016. In the second phase, the cyber branch will incorporate electronic warfare Soldiers in the 29-series Military Occupational Specialty.

"Much of the infrastructure of the branch is still under development," Buckner said. "For example, for the time being, officers selected for the branch will attend either signal or military intelligence officer education courses. However, the Army needs outstanding young men and women with these qualifications now, so we will start to build the branch with the available institutional training and plan to evolve to cyber-specific courses in fiscal year 2016."

As the proponent for the Army's newest career field, the Cyber CoE is developing the accession standards and strategies for filling positions in the branch. Although the Army is currently accepting applications from second lieutenants through colonels, the Cyber CoE is still working on firm standards for entry into the branch, Buckner said. In order to be eligible, Buckner said. In order to be eligible, applicants must be able to obtain a top secret clearance and be able to pass and maintain a counter-intelligence polygraph and National Security Agency access. She added that a bachelor's degree in a science, technology, engineering or mathematics discipline would be a plus.

"Beyond that, we're still developing standards," Buckner said. "So my advice is, if you can meet the basic requirements, feel you have something to offer to our Cyber branch and are motivated to join what will truly be an elite corps of professionals in our Army, then go ahead and apply."

The Army notes that once accepted into the career field, officers, warrant officers and enlisted soldiers will fill a wide variety of positions with cyber mission force units and traditional Army formations, including: cyber operator, analyst and planner positions. The branch will also include traditional leadership, command and staff positions.

Although a significant number of cyber positions will be located at Forts Gordon and Meade as the majority of cyber elements are assigned there, cyber Soldiers will have assignment opportunities across the force. The Army's total force approach to cyber includes significant growth in the Army National Guard and Army Reserve's cyberspace capabilities and capacities.

"We believe the branch will attract high quality talent to the Army and many of those people, once they experience the opportunities available in the cyber branch will choose to stay," Conti said.

"I think membership in the cyber branch presents an exciting, cutting-edge opportunity for the right Soldiers," Buckner said. "It will be a unique gathering of professionals, using skills that have become associated with the bad guys in our popular culture. But we'll be wearing the white hats — good Soldiers, doing good work in cyberspace for a great nation. I can't think of a more interesting

and rewarding opportunity to serve than that."
For information on joining the Cyber branch as an officer, contact the Human Resources Command Cyber branch at (502) 613-5398/6614. Enlisted and warrant officer branch contact information will be released as it is established.

US-UK Cybersecurity initiative launched

By Emily Hough
Source: http://www.crisis-response.com/news/news.php?article=807

In a partnership supported by the UK Home Office on behalf of the UK Government, the US Department of Homeland Security's (DHS) Science & Technology Directorate has teamed up with the UK Science and Technology Facilities Council (STFC) to look at innovative ways to protect infrastructure from the growing risk of cyber attack. The new initiative, known as the Collaboration on Resilience and Security, or ColoRS, was launched in November at a two-day working meeting in Washington DC, writes Andy Marshall, *CRJ* Advisory Panel Member, who attended the meeting.
The ColoRS meeting was hosted by the Department of Homeland Security and it brought together 35 experts from the US and the UK, drawn from academia, government and emergency

practitioners, to take a closer look at the main cybersecurity challenges facing both countries.
Opening the event, Douglas Maughan, Director of the DHS' Cyber Security Division, outlined the key benefits that it is hoped ColoRS will bring: "From a cybersecurity perspective, we need to identify research needs and encourage multi-domain and multi-disciplinary teams to better anticipate threats to cyber infrastructure and mitigate the impact infrastructure failures would have on our societies."
A collection of detailed papers will now be developed, with the intention of publishing these in a single volume in Spring 2015.

***Emily Hough** is the Editor-in-Chief at Crisis Response Journal (UK).*

Handling Cyber Incidents & Cyber Crises: Terminology, Perspective and Attribution

By Michel Herzog
Source: http://isnblog.ethz.ch/intelligence/49634

"*Cyber incidents are a bit like a bar brawl – you might have a pretty good idea who started it, but you will never be absolutely sure*".
When it comes to managing contemporary cyber incidents and crises, the above statement couldn't be more accurate. National cybersecurity strategies and international

regimes are not only becoming increasingly common, they're also proving difficult to implement and enforce. In this respect, some of the most pressing concerns are associated with key cybersecurity aspects like 'terminology', 'perspective' and 'attribution'.

Crisis vs. Emergency

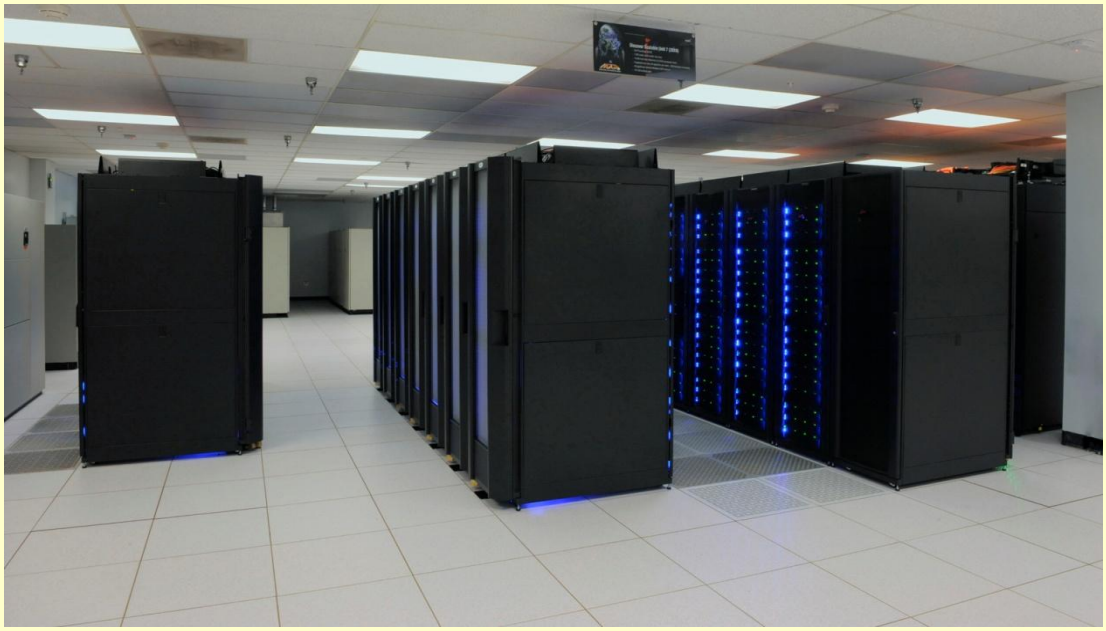
When it comes to terminology and definitions, the cyber realm undoubtedly suffers from the same type of problems as other domains. For instance, one look at a newspaper will often reveal the very liberal use of the word 'crisis'. However, this ubiquity yields little clarity about what actually constitutes a 'crisis' and how these are different from 'emergencies'. For purposes of clarification, an 'emergency' is a situation that can be handled via business continuity management procedures in the private domain or, in the case of the state and public sector, the emergency and security services. Emergencies should not result in any mid- or long-term damage to critical infrastructures or societies. However, should the aforementioned procedures and resources prove to be insufficient or ineffective, then the potential exists for a 'crisis' to develop.

Crises usually occur as a result of unfolding dilemmas and events. A lack of capacities or capabilities often means that extraordinary measures are required to deal with increasingly uncertain and unstable conditions. In this respect, uncertainty is typically caused by information deficiencies that complicate efficient decision making.

A lack of quality and reliable information, in turn, complicates a decision-maker's ability to respond to events in an appropriate and timely manner. Slower response times risk increased financial costs, a loss of public trust and confidence, as well as mounting pressure from the media, civil society and other stakeholders. In severe cases, this can result in profound reputational damage.

Consequently, the challenges associated with crisis management in all domains can be attributed in no small part to the complexity of modern society. In this respect, social networks, a growing number of media outlets, the relative ease of travelling and other factors all help to ensure that today's crises are typically of a complex nature, and information about them (or lack thereof) is quite often contradictory. Moreover, the variety of stakeholders and vested interests that can be attributed to a crisis undoubtedly complicates institutional responses and solutions. Competing political interests by their very nature tend to slow down decision-making processes.

The NASA Supercomputer "Discover"



A Question of Perspective

This immediately feeds into problems associated with 'perspectives'. Making sense of a situation and taking appropriate actions tends to be influenced by psychological phenomena like group thinking and cognitive dissonances – and responding to

cyber 'crises' is no different. For instance, many private sector actors frame cyber crises as 'extended business continuity management situations'. By contrast, international organizations tend to classify a cyber crisis as a strategic issue with global implications. And let's not forget that states are likely to view a potential cyber crisis as a matter of national security with severe ramifications for critical infrastructure and populations.

One way to overcome this divergence of opinion might be to restrict the use of the term 'cyber crisis' for the most severe cyber 'incidents'. Apart from clearing up any misunderstandings, a clearer definition as to what actually constitutes a 'cyber crisis' might also result in a quicker and better coordinated response to the crisis at hand. This might even help to promote 'best practice' and information sharing between academia, public institutions and the private sector.

Handling Cyber Incidents and Crises: The Attribution Dilemma

The perception that a 'cyber crisis' is basically the same as a general crisis (albeit with a cyber- component) is common. The same can also be said of comparisons between managing a 'cyber crisis' and general crisis management. For instance, the Swiss National Cyber Security Strategy does not use the term "cyber crisis" as such, but promotes instead "national crisis management for crises with a cyber-characteristic". This statement, in turn, implies that managing a crisis isn't scenario-driven, but process-oriented. In addition, a crisis only becomes a 'crisis' once it exceeds the capabilities of emergency responses and requires decision making on a strategic level. However, this perspective isn't uncontested. There are several issues concerning the assumptions implicit in this broader conception that merit further consideration regarding cyber-related incident and crisis scenarios:

- It fails to address the need for increased stakeholder coordination and cooperation in the context of interdependence and connectivity between the public and private sphere in the cyber domain, as well as the centrality of information systems in modern society
- It overlooks that stakeholders might not share the same goals and priorities when dealing with a 'cyber crisis'
- Not only might the availability of information be compromised, but also its confidentiality and integrity
- A 'cyber crisis' is likely to be more dynamic than a conventional crisis. For example, a malicious actor may use stolen information to escalate or steer a crisis according to their goals, giving it an element that might not exist in a typical non-cyber crisis

Finally, as Rid wrote: "Intention may be the only line separating the attack from the accident." Determining who was responsible for the attack and his/her motivations ("personal attribution" and "motivation attribution") is undoubtedly a complex and time-consuming task. However, having time to think long and hard about these factors is not usually an option during a crisis situation. Consequently, the logical implications of attribution difficulties in a cyber 'crisis' include increased pressure, higher costs and the possible escalation of what was once thought to be a 'normal' crisis situation into something even more complex.

Looking Ahead

Two trends regarding cyber-security are noteworthy within the context of managing cyber 'emergencies' and 'crises': the increasing sophistication of cyber-attacks and the substantial capabilities of nation states in the cyber domain. These two aspects alone increase the potential for cyber-incidents to develop into full-blown cyber-crises. Fortunately, there are ways to address the issues related to the management of these 'events'. The establishment of collaboration networks, formulation of common terminology, and other confidence building measures will help to address some of the ambiguity associated with cyber issues. Additionally, increasing knowledge and experience in dealing with cyber-incidents will help establish functioning response procedures. Enhancing an organization's intelligence and investigative capabilities is another key factor – both in the private and public sectors. Ultimately, these 'counter' strategies imply that the most effective responses to cyber crises need to be well organized and supported by strong internal situational awareness. Failure to implement these mechanisms to tackle cyber-related and non-cyber related challenges could result in the creation of a crisis 'from within' that exacerbates the

external pressure coming from the original 'event'.

Michel Herzog is a researcher in the field of critical infrastructure protection and cyber-security in the Risk and Resilience Research Group at the Center for Security Studies (CSS). His main research interests are the management of political risks, early warning and crisis management, especially in the field of critical infrastructure protection and cyber-security.

UK Labels Facebook A Terrorist 'Haven'

Source: http://www.govinfosecurity.com/uk-labels-facebook-terrorist-haven-a-7616

A new U.K. government report has accused social networks of serving as a "safe haven for terrorists," inflaming what some observers see as already tense relations between the British government and Silicon Valley.

The report, issued by Parliament's Intelligence and Security Committee, comes in response to the murder of British solider Lee Rigby in 2013 by British citizens Michael Adebolajo and Michael Adebowale. The two men attacked Rigby on the streets of Woolrich - a district in southeast London - as he was returning to his Army barracks, first running into him from behind with their car, and then attacking him with knives.

Parliament's report says an unnamed social network - later revealed in multiple press reports to be Facebook - "could have made a difference" in preventing the attack, if only it had flagged a December 2012 discussion, conducted using the social network, in which Adebowale told an extremist overseas codenamed "Foxtrot" that he wanted to kill a soldier "in the most graphic and emotive manner - because of U.K. military action in Iraq and Afghanistan."

A variety of U.K. government officials have blamed Facebook for not preventing the attack. "This company does not appear to regard itself as under any obligation to ensure that its systems identify such exchanges, or to take action or notify the authorities when its communications services appear to be used by terrorists," says MP Malcolm Rifkind, who chairs the Intelligence and Security Committee. "There is therefore a risk that, however unintentionally, it provides a safe haven for terrorists to communicate within."

But the committee doesn't hold the intelligence services responsible for failing to prevent Rigby's murder, despite cataloging a string of investigatory errors. "We do not consider that any of these errors, taken individually, were significant enough to have made a difference," Rifkind says.

Prime Minister David Cameron, who issued a statement in response to the report, says Internet firms must devote more resources to combating terrorism. "Terrorists are using the Internet to communicate with each other. We must not accept that these communications are beyond the reach of the companies," Cameron says. "We expect the Internet companies to do all they can ... It is their social responsibility to act on this." Cameron also announced that the U.K. government would spend an additional £130 million ($200 million) over the next two years to combat "lone wolf" terrorists.

Reached for comment, Facebook declined to discuss the report's conclusions or Cameron's comments. "Like everyone else, we were horrified by the vicious murder of Fusilier Lee Rigby," a Facebook spokesman tells Information Security Media Group. "We don't comment on individual cases, but Facebook's policies are clear. We do not allow terrorist content on the site and take steps to prevent people from using our service for these purposes."

Google and Twitter, whose monitoring practices were also discussed in the committee's report, didn't respond to a similar request for comment.

Silicon Valley Outrage

But the blame game has reportedly incensed many Silicon Valley executives. Furthermore, the report comes when relationships between U.S. technology firms and the British government are already strained, after Edward Snowden's leaks revealed that the National Security Agency and GCHQ -

respectively U.S. and U.K. intelligence agencies - were hacking directly into the systems of Internet giants such as Facebook as part of a mass surveillance campaign. Earlier this month, meanwhile, the new director of GCHQ blasted social networks for facilitating crime, terrorism and child abuse.

"Given all the information they have, with and without our permission, it is outrageous that they should try and blame Facebook," one Silicon Valley executive tells the *Guardian*, speaking on condition of anonymity. "The conclusion of the report was: if only Facebook had been doing our job here."

Define Social Responsibility

Richard Barrett, a former counter-terrorism chief at MI5 and MI6 - which respectively focus on domestic and foreign intelligence - disagrees with the committee's finding that Facebook should have done more, noting that the social network's systems had automatically deleted eight accounts used by Adebowale, after flagging them as being used to "promote terrorism."

"I think it's very hard to talk about the social responsibility of a multinational company," he tells the *Guardian*. "I mean Facebook is operating in probably almost all countries in the world, so will that social responsibility vary do you think from the United Kingdom to, I don't know, Russia or Myanmar or countries like that? I think it's quite a burden to put on Facebook to decide where their social responsibility lies in all different circumstances."

Furthermore, should the U.K. government compel Facebook to give it direct access user data, Barrett says it's likely that terrorists would easily sidestep that monitoring by using encryption.

U.K. Seeks Direct Access

The committee's report notes that U.K. law enforcement and intelligence agencies say they have difficulty obtaining all of the data they want from U.S. social networks in relation to investigations. But Ross Anderson, professor of security engineering at Cambridge University, says the U.K. government's decision to blame Facebook for Rigby's murder may kill the government's chance of fostering a better working relationship, and finding ways to work around the logjam of requests for mutual legal assistance that are now sitting with the U.S. Department of Justice, owing to lack of funding from Congress.

"The spooks' approach reminds me of how Pfizer dealt with Viagra spam, which was to hire lawyers to write angry letters to Google," Anderson says. "If they'd hired a geek who could have talked to the abuse teams constructively, they'd have achieved an awful lot more."

Anderson says Parliament's report also conveniently ignores the fact that Facebook's investment in fighting crime trumps what the U.K. government spends, while Google and Microsoft outspend the U.K. government by a factor of five. "If GCHQ really cares, then it could always pay the Department of Justice to clear the backlog," he says. "The fact that all the affected government departments and agencies use this issue for posturing, rather than tackling the real problems, should tell you something."

Cyberattack on Civil Aviation

Source: http://acdemocracy.org/cyberattack-on-civil-aviation/

The holiday season brings new “traditional” threats to airline passenger from al Qaeda, to nontraditional threat from wireless communication devices that carried and used on board the planes. Would be terrorists may be discoverer before detonating sophisticated hidden explosives, but would not come under any suspicion for using their smart phones, tablets and PCs during flight.

However, **a well trained martyr could hack into the plane’s computer system, take over all or part of the controls, commandeering its communication, or air system to shut down, etc.** “When the plane is air-side, you can insert a set of commands and codes that may initiate, on signal, a set of processes,” the former scientific adviser to the British Home Office, Sally Leivesley. He went on to describe how someone familiar with sophisticated systems engineering, could hack into the plane’s controls by sending a radio signal from a small device.

In the aftermath of Malaysia Airlines Flight MH370 disappearance, aviation experts have been considering the possibility of hacking into an airplane and gaining complete control of on-board systems, "including plane navigation and cockpit systems."
Today's airplanes are very sophisticated systems. They are comparable to a complex network in which each system runs its software component that could be compromised exactly like the information exchanged by the parts.
According to Pierluigi Paganini, the Editor-in-Chief at Cyber Defense magazine, "Security is fundamental for the aviation industry. Considering the availability of numerous tools on the market that could be exploited in a hypothetical attack against a plane, cyber security is becoming even more crucial. It's time to adopt for civil uses the same technologies designed for a military environment

Hacking alert over Android WATCHES: Experts reveal gadgets can be infiltrated to read messages sent to your wrist

Source: http://www.dailymail.co.uk/sciencetech/article-2870710/Hacking-alert-Android-WATCHES-Experts-reveal-gadgets-infiltrated-read-messages-sent-wrist.html

They are touted as the next bit thing in technology - smartwatches that can keep you up to date right from your wrist.
However, experts have warned they could also be the next big target for hackers.
A video reveals just how easy it is to read messages sent to a smartwatch running Google's Android software.

For this proof-of-concept, a Nexus 4 Android phone equipped with Android L Developer Preview and Samsung Gear Live (pictured) were used - and hackers could read messages sent to the watch.

How they did it
For this proof-of-concept, a Nexus 4 Android device equipped with Android L Developer Preview and Samsung Gear Live were used.
Using special software the team was able to 'brute force' a six digit passcode used to link the phone to the watch - and then read messages sent to it.

'Smartwatches, bands and devices all have a lack of security.
'We trust these devices with everything from messages and Facebook updates to biometric information,' said Liviu Arsene of Bitdefender, which uncovered the issue.
'Everything from SMS messages to Facebook or Google Hangouts

chats are constantly being forwarded to your smartwatch.'
He found that Google's Android Wear software relies on a six digit pin code to link to watches.
'This six digit pin code can be easily bruteforced,' he said.
'It was not all that that difficult to do.'
'Because the Android Wear obfuscation relies on a pin code of only six digits during the initial pairing, an attacker wouldn't take long to brute-force number and start reading your conversations in plain-text,' he wrote.
'Of course, this means an attacker would have to be fairly near the victim and log all intercepted Bluetooth data packets, but the large-scale adoption of such an exploit could be fueled by the increasing number of smartwatches or smartbands.
'Weaponizing it could only be a matter of time.'
For the proof-of-concept, a Nexus 4 Android device equipped with Android L Developer Preview and Samsung Gear Live were used.
'The implications of these recent findings are only moderately surprising – we know from past experience that adoption of new technologies does not always go hand-in-hand with better security practices.'
Android Wear watch was unveiled by Google at its developer conference in San Francisco earlier this year.
The firm showed off the latest watches running Android wear, a version of Android designed for wearable computers.
'It's finally possible to make a powerful computer small enough to wear on your body,' said Google's David Singleton.
It showed off the LG G watch, which shows the users the most relevant alert at the time - for instance, a flight they are about to get or an upcoming meeting.
Google also revealed apps for its watches, including a food ordering app from Eat that allows users to order favourite food directly from their wrist, and a recipe app called allthecooks that walks users through recipes on the watch face.
Using special software the team was able to 'brute force' a six digit passcode used to link the phone to the watch - and then read messages sent to it.
LG said the G Watch would initially be made available to 12 countries including the US, UK, France, Germany and Japan, adding that it would announce its price and shipping date shortly.
'As one of the first Android Wear devices to market, we see this as the beginning of a long-term commitment to making wearables running Android Wear a household name,' said Dr. Jong-seok Park, president and CEO of LG.
'We're confident that once consumers see how useful and compelling LG G Watch can be, it will be integrated into their daily lives, just as smartphone have done.'

Can a hacker stop your car or your heart? Security and the Internet of Things

By Temitope Oluwafemi
Source: http://www.homelandsecuritynewswire.com/dr20141215-can-a-hacker-stop-your-car-or-your-heart-security-and-the-internet-of-things

An ever-increasing number of our consumer electronics is Internet-connected. We're living at the dawn of the age of the Internet of Things. Appliances ranging from light switches and door locks, to cars and medical devices boast connectivity in addition to basic functionality. The convenience can't be beat, but the security and privacy implications cannot and should not be ignored. There needs to be a concerted effort to improve security of future devices. Researchers, manufacturers and end users need to be aware that privacy, health and safety can be compromised by increased connectivity. Benefits in convenience must be balanced with security and privacy costs as the Internet of Things continues to infiltrate our personal spaces.

An ever-increasing number of our consumer electronics is Internet-connected.

We're living at the dawn of the age of the Internet of Things. Appliances ranging from light switches and door locks, to cars and medical devices boast connectivity in addition to basic functionality.
The convenience can't be beat. But what are the security and privacy implications? Is a patient implanted with a remotely

controllable pacemaker at risk for security compromise? Vice President Dick Cheney's doctors worried enough about an assassination attempt via implant that they disabled his defibrillator's wireless capability. Should we expect capital crimes via hacked Internet-enabled devices? Could hackers mount large-scale terrorist attacks? **Our research suggests these scenarios are within reason.**

Your car, out of your control

Modern cars are one of the most connected products consumers interact with today. Many of a vehicle's fundamental building blocks – including the engine and brake control modules – are now electronically controlled. Newer cars also support long-range wireless connections via cellular network and Wi-Fi. But hi-tech definitely doesn't mean highly secure.

Our group of security researchers at the University of Washington was able to remotely compromise and controls a highly computerized vehicle. They invaded the privacy of vehicle occupants by listening in on their conversations. **Even more worrisome, they remotely disabled brake and lighting systems and brought the car to a complete stop on a simulated major highway.** By exploiting vulnerabilities in critical modules, including the brake systems and engine control, along with in radio and telematics components, our group completely overrode the driver's control of the vehicle. The safety implications are obvious.

This attack raises important questions about how much manufacturers and consumers are willing to sacrifice security and privacy for increased functionality and convenience. Car companies are starting to take these threats seriously, appointing cybersecurity executives. But for the most part, automakers appear to be playing catchup, dealing with security as an afterthought of the design process.

Home insecurity

An increasing number of devices around the home are automated and connected to the Internet. Many rely on a proprietary wireless communications protocol called Z-Wave.

Two U.K. researchers exploited security loopholes in Z-Wave's cryptographic libraries — that's the software toolkit that authenticates any device being connected to the home network, among other functions, while providing communication security over the Internet. **The researchers were able to compromise home automation controllers and remotely controlled appliances including door locks and alarm systems.** Z-Wave's security relied solely on keeping the algorithm a secret from the public, but the researchers were able to reverse engineer the protocol to find weak spots.

Our group was able to compromise Z-Wave controllers via another vulnerability: their web interfaces. Via the web, we could control all home appliances connected to the Z-Wave controller, showing that a hacker could, for instance, turn off the heat in wintertime or watch inhabitants via webcam feeds. We also demonstrated an inherent

danger in connecting compact fluorescent lamps (CFL) to a Z-Wave dimmer. These bulbs were not designed with remote manipulations over the Internet in mind. We found an attacker could send unique signals to CFLs that would burn them out, emitting sparks that could potentially result in house fires.
Our group also pondered the possibility of a large-scale terrorist attack. The threat model assumes that home automation becomes so ubiquitous that it's a standard feature installed in homes by developers. An attacker could exploit a vulnerability in the automation controllers to turn on power-hungry devices — like HVAC systems — in an entire neighborhood at the same time. With the A/C roaring in every single house, shared power transformers would be overloaded and whole neighborhoods could be knocked off the power grid.

Harnessing hackers' knowledge

One of the best practices of designing elegant security solutions is to enlist the help of the security community to find and report weak spots otherwise undetected by the manufacturer. If the internal cryptographic libraries these devices use to obfuscate and recover data, amongst other tasks, are open-source, they can be vetted by the security community. Once issues are found, updates can be pushed to resolve them. Crypto libraries implemented from scratch may be riddled with bugs that the security community would likely find and fix – hopefully before the bad guys find and exploit. Unfortunately, this sound principle has not been strictly adhered to in the world of the Internet of Things.

Third party vendors designed the web interfaces and home appliances with Z-Wave support that our group exploited. **We found that, even if a manufacturer has done a very good job and released a secure product, retailers who repackage it with added functionality — like third party software — could introduce vulnerabilities.** The end-user can also compromise security by failing to operate the product properly. That's why robust multi-layered security solutions are vital – so a breach can be limited to just a single component, rather than a successful hack into one component compromising the whole system.

Level of risk

There is one Internet of Things security loophole that law enforcement has taken notice of: thieves' use of scanner boxes that mimic the signals sent out by remote key fobs to break into cars. The other attacks I've described are feasible, but haven't made any headlines yet. **Risks today remain low for a variety of reasons.** Home automation system attacks at this point appear to be very targeted in nature. Perpetrating them on a neighborhood-wide scale could be a very expensive task for the hacker, thereby decreasing the likelihood of it occurring.
There needs to be a concerted effort to improve security of future devices. Researchers, manufacturers and end users need to be aware that privacy, health and safety can be compromised by increased connectivity. Benefits in convenience must be balanced with security and privacy costs as the Internet of Things continues to infiltrate our personal spaces.

Temitope Oluwafemi *is Ph.D. Student in Electrical Engineering at University of Washington.*

Sony hackers threaten attacks against movie goers who plan to see "The Interview"

Source: http://www.homelandsecuritynewswire.com/dr20141217-sony-hackers-threaten-attacks-against-movie-goers-who-plan-to-see-the-interview

The hackers who attacked Sony networks are now threatening an attack on people who plan to go to see the movie "The Interview." The hackers write in their message that they "recommend you to keep yourself distant" from movie theaters showing the movie.

The *New York Daily News* reports that the hackers earlier promised to deliver a

"Christmas gift." It was not clear what they had in mind – some suggested they would release another batch of embarrassing data from Sony's files — but it now looks as if the "gift" might well be a cyberattack on movie theaters.

"Warning[.] We will clearly show it to you at the very time and places 'The Interview' be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to," the hackers' note says. The hackers also make a reference 9/11 in the note.

The full note reads:

Warning
We will clearly show it to you at the very time and places "The Interview" be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to.
Soon all the world will see what an awful movie Sony Pictures Entertainment has made.
The world will be full of fear.
Remember the 11th of September 2001.
We recommend you to keep yourself distant from the places at that time.
(If your house is nearby, you'd better leave.)
Whatever comes in the coming days is called by the greed of Sony Pictures Entertainment.
All the world will denounce the SONY.

The *Daily News* notes that the threat was release along with another set of e-mails, this time said to be those of Sony Entertainment CEO Michael Lynton. Cyber experts note that the hackers post Sony information they release anonymously, and are making contact with reporters through reusable e-mail addresses, it may well be the case that a separate group is behind this latest threat.

One way to find out whether the latest warning comes from the original hackers or a different group is to check to authenticity of Lynton's e-mails: If they are authentic, this will mean that the new batch – and the latest warning – were released by the original hackers.

North Korea is suspected to have played a role in the hacking of Sony, with indications pointing to the reclusive regime. North Korea has denied any involvement, and cyber experts note that the evidence implicating North Korea may ultimately not be convincing enough to know for sure who was behind it.

The cyberattack on Sony began in late November, when the company's computer systems around the world were shut down. A group calling itself "Guardians of Peace" has taken credit for the attack, and over the past week it has begun to release stolen Sony data, including the e-mails of top executives. Around 47,000 Social Security numbers were also released, and some of those whose Social Security numbers were release are now suing Sony for failing to protect that data.

UPDATE (Dec18): "Sony Pictures has no further release plans" for "The Interview," a company spokesperson tells CNN's Brian Stelter, discouraging speculation that it might release the movie digitally. Sony on Wednesday canceled the December 25 release of the film, which depicts the assassination of North Korea's leader, following a threat from hackers that people should avoid going to theaters to see it.

2008 Turkish oil pipeline explosion may have been Stuxnet precursor

Source: http://www.homelandsecuritynewswire.com/dr20141217-2008-turkish-oil-pipeline-explosion-may-have-been-stuxnet-precursor

The August 2008 Baku-Tbilisi-Ceyhan (BTC) oil pipeline explosion in Refahiye, eastern Turkey, was ruled at the time to be an accident resulting from a mechanical failure, which itself was a result of an oversight by Turkish government's supervisors. The Kurdistan Workers' Party (PKK), a militant pro-Kurdish organization, claimed credit for the explosion — which was plausible, because of the PKK's history of bombing pipelines and other Turkish infrastructure assets.

For some Western intelligence agencies, however, the explosion was beyond the capabilities of the PKK, and not likely the result of an accident. Instead, these intelligence services concluded, the explosion was the result of a cyberattack. According to people familiar with an investigation of the incident, hackers had infiltrate the pipeline's surveillance systems and valve stations, and super-pressurized the crude oil in the pipeline, causing the explosion.

In 2010 U.S. and Israeli intelligence agencies were credited with the first major cyberattack against a foreign power via the Stuxnet malware which crippled uranium-enrichment centrifuges in Iran's nuclear weapons program.

The revelation of a possible cyberattack against the BTC pipeline, however, "rewrites the

history of cyberwar," said Derek Reveron, a professor of national security affairs at the U.S. Naval War College in Newport, Rhode Island.

Companies with major interest in the BTC pipeline have denied rumors of an attack. "We have never experienced any kind of signal jamming attack or tampering on the communication lines, or computer systems," Huseyin Sagir, a spokesman for Botas International Ltd., the state-run company which operates the pipeline in Turkey, said in an e-mail to *Bloomberg News*. In its 2008 annual report, British Petroleum — majority owner of the pipeline — said the temporary shutdown of the BTC pipeline was due to a fire.

The *Sydney Morning Herald* reports that investigators working with the Turkish, British, Azerbaijani, and other governments have been examining why the security control systems designed to detect oil leaks or fires failed to work moments before the explosion. Investigators eventually discovered that hackers infiltrated the system via the surveillance cameras, the communications software of which had backdoors used by the hackers to gain entry into the system's internal network. Once inside the network, the hackers could have manipulated the pipeline pressure by cracking into small industrial computers at a few valve stations.

Roughly sixty hours of pipeline surveillance footage were erased by the hackers, but a single infrared camera operating on an independent network captured images of two men with laptops near the pipeline days before the explosion. The men wore black military-style uniforms without insignias, similar to those worn by troops considered to have been working on behalf of Russia in Crimea during Russia's invasion of Ukraine earlier this year. Investigators have also matched the time-stamp of the infrared image of the two men to data logs that showed the pipeline's security system had been breached by an outsider.

In lieu of the investigation, many intelligence analysts now believe that the BTC pipeline explosion was not an accident, as the Turkish government claimed in 2008. Regarding the PKK's involvement, leaked U.S. State Department cables note that the PKK has in the past received arms and intelligence from Russia; therefore it is possible that the group might have arranged in advance with the actual attackers to take credit for the explosion.

It is unlikely that the PKK orchestrated the BTC explosion, analysts say. Sophisticated hacking does not fit the profile of the PKK, said Didem Akyel Collinsworth, an Istanbul-based analyst for the International Crisis Group. "That's not their modus operandi," she said. "It's always been very physical, very basic insurgency stuff." Additionally, investigators involved with the incident claim that no evidence of a physical bomb was found near the explosion site.

The construction of the BTC pipeline, which connects Baku, the capital of Azerbaijan and Ceyhan, a port on the south-eastern Mediterranean coast of Turkey, via Tbilisi, the capital of Georgia, dealt a major blow to Russia as it aimed to reassert power over former Soviet territories. "Given Russia's strategic interest, there will always be the question of whether the country had a hand in it," said Emily Stromquist, an energy analyst for Eurasia Group, a political risk firm based in Washington, D.C.

Days after the explosion, Russia invaded Georgia, and according to Georgia's then-prime minister Nika Gilauri, Russian fighter jets dropped bombs meters away from the BTC line near the city of Rustavi, missing their target. It seemed a cyberattack was the better weapon.

McAfee: More Small Nation-States, Terror Groups Will Use Cyber Warfare In 2015

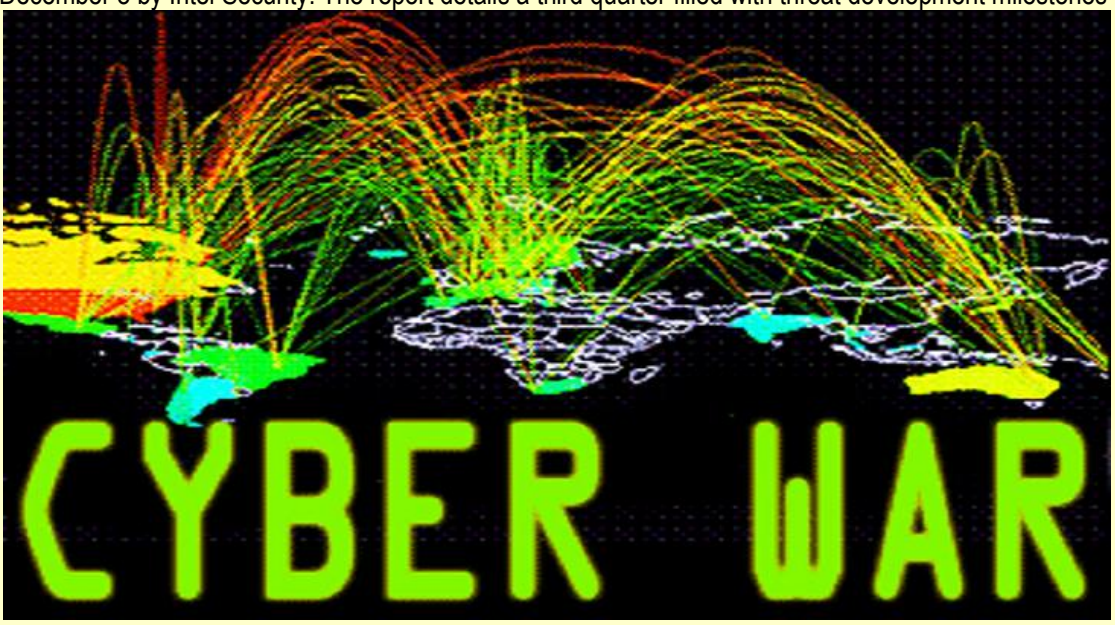
By Kylie Bull (Managing Editor HSToday.com)

Source: http://www.hstoday.us/single-article/mcafee-more-small-nation-states-terror-groups-will-use-cyber-warfare-in-2015/ea5a48c0b7b6cd08e89509e8edeb99ab.html

McAfee Labs has forecasted a 2015 threat landscape shaped by more attacks exploiting long-established Internet trust standards, new attack surfaces in mobile and the Internet of Things (IoT) and increasingly sophisticated cyber espionage capabilities, including techniques capable of evading sandboxing detection technologies.

In 2015, McAfee Labs predicts malicious parties will seek to extend their ability to avoid detection over long periods, with non-state actors increasingly adopting cyber espionage capabilities for monitoring and collecting valuable data over extended targeted attack campaigns. The researchers predict more aggressive efforts to identify application, operating system, and network vulnerabilities, and an increasing focus on the limitations of sandboxing technologies as hackers attempt to evade application- and hypervisor-based detection.

These threat predictions form part of the McAfee Labs *November 2014 Threats Report*, released on December 8 by Intel Security. The report details a third quarter filled with threat development milestones



and cyber events exploiting long-established Internet trust standards.

In the third quarter, McAfee Labs detected more than 307 new threats every minute, or more than five every second, with mobile malware samples growing by 16 percent during the quarter and overall malware surging by 76 percent year over year. The researchers also identified new attempts to take advantage of Internet trust models, including secure socket layer (SSL) vulnerabilities such as Heartbleed and BERserk, and the continued abuse of digital signatures to disguise malware as legitimate code.

"The year 2014 will be remembered as 'the Year of Shaken Trust,'" said Vincent Weafer, senior vice president, McAfee Labs, part of Intel Security. "This unprecedented series of events shook industry confidence in long-standing Internet trust models, consumer confidence in organizations' abilities to protect their data, and organizations' confidence in their ability to detect and deflect targeted attacks in a timely manner. Restoring trust in 2015 will require stronger industry collaboration, new standards for a new threat landscape, and new security postures that shrink time-to-detection through the superior use of threat data. Ultimately, we need to get to a security model that's built-in by design, seamlessly integrated into every device at every layer of the compute stack."

Looking ahead in detail, McAfee Labs foresees the following trends in 2015:

Increased use of cyber warfare and espionage tactics. Cyber espionage attacks will continue to increase in frequency as long-term players will become stealthier information gatherers, while newcomers to cyber attack capabilities will look for ways to steal sensitive information and disrupt their adversaries.

- Established nation-state actors will work to enhance their ability to remain hidden on victim systems and networks.
- Cybercriminals will continue to act more like nation-state cyber espionage actors, focusing on monitoring systems and gathering high-value intelligence on individuals, intellectual property, and operational intelligence.
- McAfee Labs predicts that more small nation states and terror groups will use cyber warfare.

Greater Internet of Things attack frequency, profitability, and severity. Unless security controls are built-in to their

architectures from the beginning, the rush to deploy IoT devices at scale will outpace the priorities of security and privacy. This rush and the increasing value of data gathered, processed, and shared by these devices will draw the first notable IoT paradigm attacks in 2015.

- The increasing proliferation of IoT devices in environments such as health care could provide malicious parties access to personal data even more valuable than credit card data.

Privacy debates intensify. Data privacy will continue to be a hot topic as governments and businesses continue to grapple with what is fair and authorized access to inconsistently defined "personal information."

- In 2015 we will see continued discussion and lack of clarity around what constitutes "personal information" and to what extent that information may be accessed and shared by state or private actors.
- We will see a continued evolution in scope and content of data privacy rules and regulations, we may even see laws begin to regulate the use of previously anonymous data sets.
- The European Union, countries in Latin America, as well as Australia, Japan, South Korea, Canada, and many others may enact more stringent data privacy laws and regulations.

Ransomware evolves into the cloud. Ransomware will evolve its methods of propagation, encryption, and the targets it seeks. More mobile devices are likely to suffer attacks.

- We predict ransomware variants that manage to evade security software installed on a system will specifically target endpoints that subscribe to cloud-based storage solutions.
- Once the endpoint has been infected, the ransomware will attempt to exploit the logged-on user's stored credentials to also infect backed-up cloud storage data.
- We expect the technique of ransomware targeting cloud-backed-up data to be repeated in the mobile space.
- We expect a continued rise in mobile ransomware using virtual currency as the ransom payment method.

New mobile attack surfaces and capabilities. Mobile attacks will continue to grow rapidly as new mobile technologies expand the attack surface.

- The growing availability of malware-generation kits and malware source code for mobile devices will lower the barrier to entry for cybercriminals targeting these devices.
- Untrusted app stores will continue to be a major source of mobile malware. Traffic to these stores will be driven by "malvertising," which has grown quickly on mobile platforms.

POS attacks increase and evolve with digital payments. Point of sale (POS) attacks will remain lucrative, and a significant upturn in consumer adoption of digital payment systems on mobile devices will provide new attack surfaces that cybercriminals will exploit.

- Despite current efforts by retailers to deploy more chip-and-pin cards and card readers, McAfee Labs sees continued growth in POS system breaches in 2015 based on the sheer numbers of POS devices that will need to be upgraded in North America.
- Near field communications (NFC) digital payment technology will become an entirely new attack surface to exploit, unless user education can successfully guide users in taking control of NFC features on their mobile devices.

Shellshock sparks Unix, Linux attacks. Non-Windows malware attacks will increase as a result of the Shellshock vulnerability.

- McAfee Labs predicts that the aftershocks of Shellshock with be felt for many years given the number of potentially vulnerable Unix or Linux devices, from routers to TVs, industrial controllers, flight systems, and critical infrastructure.
- In 2015, this will drive a significant increase in non-Windows malware as attackers look to exploit the vulnerability.

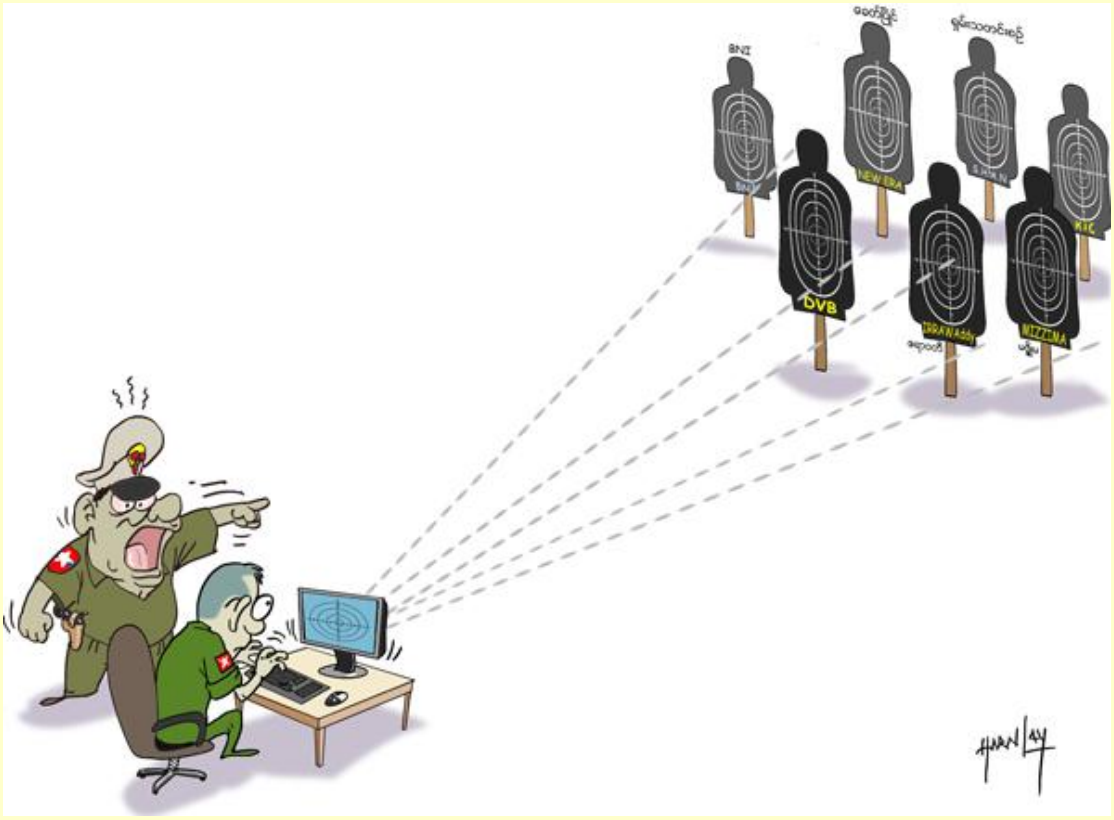
Growing exploitation of software flaws. The exploitation of vulnerabilities is likely to increase as new flaws are discovered in popular software products.

- McAfee Labs predicts that exploitation techniques such as stack pivoting, return- and jump-oriented programming,

and a deeper understanding of 64-bit software will continue to drive the growth in the number of newly discovered vulnerabilities, as will the volume of malware that exploits those newly discovered vulnerabilities.

New evasion tactics for sandboxing. Escaping the sandbox will become a significant IT security battlefield.

- Vulnerabilities have been identified in the sandboxing technologies implemented with critical and popular applications. McAfee Labs predicts a growth in the number of techniques to exploit those vulnerabilities and escape application sandboxes.
- Beyond application sandboxing, McAfee Labs predicts that 2015 will bring malware that can successfully exploit hypervisor vulnerabilities to break out of some security vendors' standalone sandbox systems.



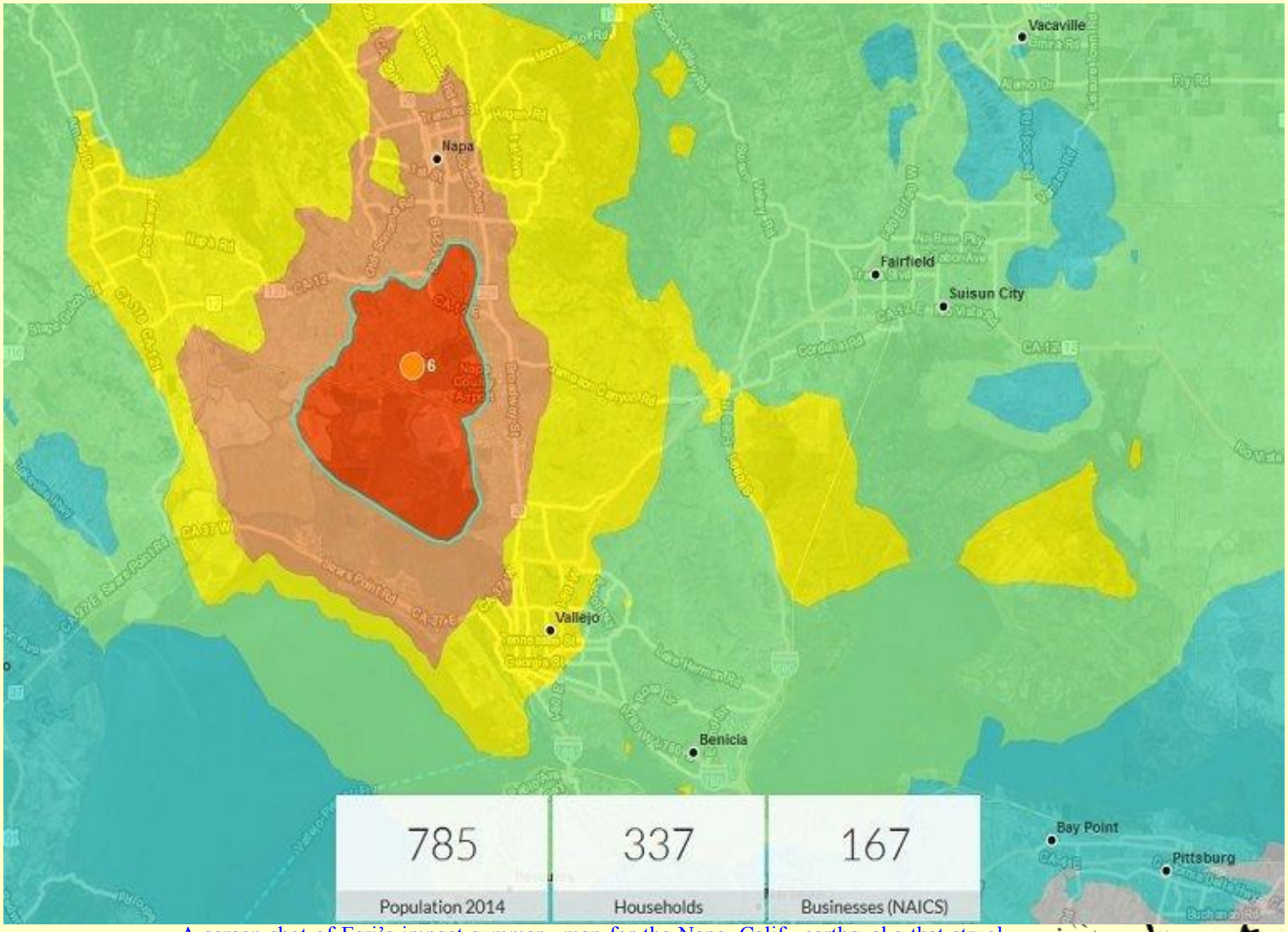
How GIS Can Aid Emergency Management

By Eric Holdeman

Source: http://www.emergencymgmt.com/disaster/How-GIS-Can-Aid-Emergency-Management.html

Susan L. Cutter is a Carolina Distinguished professor of geography at the University of South Carolina where she directs the Hazards and Vulnerability Research Institute. Her primary research interests are in the area of disaster vulnerability/resilience science — what makes people and the places where they live vulnerable to extreme events and how vulnerability and resilience are measured, monitored and assessed.

Cutter is a GIS hazard mapping guru who supports emergency management functions. I posed a series of questions about mapping and asked her to respond in writing. In Cutter's responses she reminds us to ask the "why of the where" question when looking at maps.



A screen shot of Esri's impact summary map for the Napa, Calif., earthquake that struck on Aug. 24, 2014.

What has been the evolution of hazard mapping in the United States, and how does that compare with what is being done in other countries?

Hazard mapping has a long history here in the U.S. going back to the 1960s with the work of Gilbert F. White and his insistence that we map not only where the hazards are, but where people live and work relative to the risks, what he called the human occupance of hazardous areas. Hazard mapping has evolved hand-in-hand with the understanding that we can never truly control nature. Mapping has shifted from a focus on the event itself (modeling physical processes) toward a focus on understanding interactions between people and the environment. The U.S., because of the large diversity in possible hazard threats to the nation, has become a leader in hazard mapping and the integration of new tools and technologies (such as GIS, remote sensing, GPS) into the emergency management cycle.

Besides mapping hazards — such as flood zones, seismic areas and the like — how else do you see a GIS map being useful to emergency managers?

GIS is more than mapping. It is also an analytical, data management and visualization tool. GIS can be used for situational awareness, for identifying ideal locations for prepositioning assets ahead of an impact, for understanding the relationship between hazard exposure and social vulnerability as part of the hazard mitigation planning process. GIS models and simulation capabilities enable decision-makers to both exercise response and recovery plans during non-disaster times and also understand near real-time possibilities during an event. Essentially, if you have data, it can be mapped, analyzed and utilized to make better decisions in a measureable amount of time.

The best thing that emergency managers can do is identify local partners who could assist with mapping and analysis needs. This could be a local community college, college or university. One place to start that is specific to hazard assessment would be the local or state HAZUS user's group, which would likely include qualified and interested geospatial experts focused on hazards. The other option is to work through the local planning departments and county councils of government. Rather than focusing on the master planning process, work with them on emergency management topics such as hazard mitigation and risk assessment.

There are many forms of social data — information about people such as age, income, ethnicity drawn from sources likes the U.S. census, or data derived from social media. The former is used to assess the location of vulnerable and special needs populations within a community. Knowing about the landscape of this social vulnerability helps to identify which populations may need assistance in preparing for, responding to and recovering from events.

Social data from social media is currently used to disseminate messages and information from emergency management in a top-down approach. Steps are being made in research circles to utilize "citizens as sensors" to create a more realistic real-time picture for situational awareness to aid decision-makers.

The choice of software will be a function of the resources and expertise that is locally available. If you don't have a dedicated GIS person, it may not make sense to have the full complement of Esri software. In these instances use of "best available" data from online sources may be the appropriate choice. On the other hand, Web-mapping, mobile data collection and analysis, and desktop modeling using Esri software is now approachable and very useful for the less than hard core GIS users, like myself.

You as a university support the South Carolina Emergency Management Division (SCEMD). Do you think that is a good model for others to try to establish? If so, how would you advise states and universities to find a mechanism for partnering?

The partnership we formed with SCEMD has been beneficial — students see the real-world application of the work they are doing; SCEMD gets cutting-edge science infused into its programs and in some cases becomes a model for the nation. It is a win-win situation. Each state will have a different mechanism for partnering. Not all emergency managers may be amenable, nor will all universities. The key is identifying people who are willing to work together for a common goal and take it from there. If there is willingness to work together for the betterment of the state, mechanisms can be found to formalize collaborations.

Mobile technology like smartphones and tablets along with higher connection speeds are revolutionizing how we access data. What impact do you see this having

on computer mapping, its use and how we can adapt that to emergency management purposes?
These technologies are revolutionizing emergency management and mapping as well. For example, we now collect field data on recovery using iPads and directly upload data to the cloud and our servers at the university. This technology not only cuts down on processing time (and errors) but it also means we can generate maps much more quickly. Real-time damage data could be collected using this method post-disaster, meaning that detailed preliminary damage assessments can be produced in hours, not days. Add in citizen sensor data from social media and the possibilities of crowdsourced damage and recovery information becomes a reality.

Social media continues to increase in the way it is being used to impact people's daily lives. What general uses for mapping can be applied to leverage social media use by average citizens that might benefit community resilience?
Mobile devices have geocoding within them. Currently we can, as an example, look at Twitter and see what is being said and (more importantly) where tweets are coming from on the ground. Maps of the tweets and content provide a better picture of the situational awareness, impacts and citizen status in a truly ground-up rather than top-down approach. It is an exciting and new field that is relatively unexplored at present.

You have provided some good advice as to how to use GIS to improve emergency management programs. What mistakes have you seen people make in using GIS in emergency management, and what should we do to avoid them?
One of the biggest issues has to do with cartography (the science of making maps). Just because you can use the GIS software, doesn't mean you understand the fundamental nature of spatial (or geographic) relationships. Once they see the map, emergency managers need to ask additional questions as to why (or what I like to call, the why of the where). The map shows the distribution of shelters and occupancy, for example, but a further question is why are some shelters over-subscribed while others are not? Also GIS personnel should become aware of the pitfalls of using certain classification or symbolization schemes so as to avoid misrepresenting data or displaying data out of context.

Is there anything you would like to add?
It is important to me personally and professionally that research be used to improve the human condition by being relevant, useful to practitioners and providing the empirical basis for sound public policies. To find out how we go about doing this, y'all come for a digital visit to HVRI at www.webra.cas.sc.edu/hvri.

Eric Holdeman *is a contributing writer for* Emergency Management *and is the former director of the King County, Wash., Office of Emergency Management.*

Emergency Management Researchers and Practitioners Team up for FEMA Publication

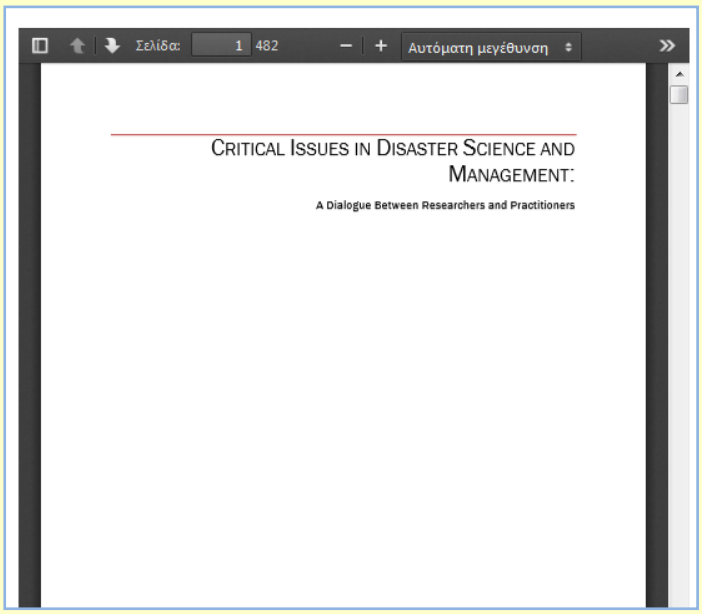
By Jim McKay
Source: http://www.emergencymgmt.com/training/Emergency-Management-Researchers-Practitioners-FEMA-Publication.html

The FEMA Higher Education Program has released a new book that combines the knowledge and experience of emergency management practitioners and researchers, the result of which is a dialogue between the two sectors about the top issues in emergency management.

Critical Issues in Disaster Science and Management: A Dialogue Between Researchers and Practitioners includes 12 sections written from the views of more than 20 emergency management practitioners and researchers. The 12 sections are dialogues on:

- Whole community — state, local and federal relationships
- Volunteers and nonprofits in disaster
- Public-private partnerships

- Access and functional needs
- Public health preparedness
- Planning and improvisation
- Reflections on the National Incident Management System
- Long-term recovery
- After-action reporting for exercises and incidents
- Social media
- Professionalization of emergency management
- Unmet needs and persistent problems



Co-editors, Joe Trainor and Tony Subbio, received from their queries 150 responses from emergency management practitioners and researchers about what the respondents thought were the most important topics. Trainor and Subbio spent a couple of full days narrowing down the topics to the dozen above and matched researchers/academicians with practitioners to author each section.

The book was conceived mostly with students in the Higher Education Program in mind but was written for practitioners as well. "We wanted an approach that would hopefully stimulate a broader conversation about emergency management practice and research and what each has to offer the other," Trainor said.

"What we've done was to illustrate not only that the divide exists but most importantly, how to go about bridging that divide between academics and the practitioners so the two can move forward together," Subbio said.

Each of the authors, a researcher and a practitioner for each topic, penned a part of a section and then, their sections and collaborated on a summation or conclusion. The conclusion talked about areas of agreement, areas of disagreement and ways to bridge the gaps.

"We expected there would be differences, and in some chapters you see differences but for the most part where we expected huge differences the author teams pointed out that the differences weren't that significant and the real challenge was sharing the information between academia and practice," Subbio said.

As an example in the social media discussion, the academic section focused on the concepts around social media, participation in social media, citizen feedback and the idea of how social media changes the ability to share information and develop partnerships.

The practitioner side discussed the pragmatics of social media, rumor control and how to get feedback from citizens but in the context of having to do it with limited resources.

The public health preparedness section revealed an evolution of ideas coming together where they hadn't in the past, say the editors.

"There's a real synergy between what's going on between the academic side and the practitioner side," Trainor said. "Ten years ago, pre-anthrax, H1N1, etc., emergency managers and public health people didn't work together, they didn't know each other and the same is true of emergency management researchers and public health research. They didn't connect."

In the end, what the book tries to accomplish say its editors, is to bring researchers and practitioners together to bridge the gaps.

▶ Read full document at source's URL.

Jim McKay is the editor of Emergency Management. *He lives in Orangevale, Calif., with his wife, Christie, daughter, Ellie, and son, Ronan. He relaxes by fly fishing on the Truckee River for big, wild trout.*

Newly Released Map Data Shows Frequency of Small Asteroid Impacts, Provides Clues on Larger Asteroid Population

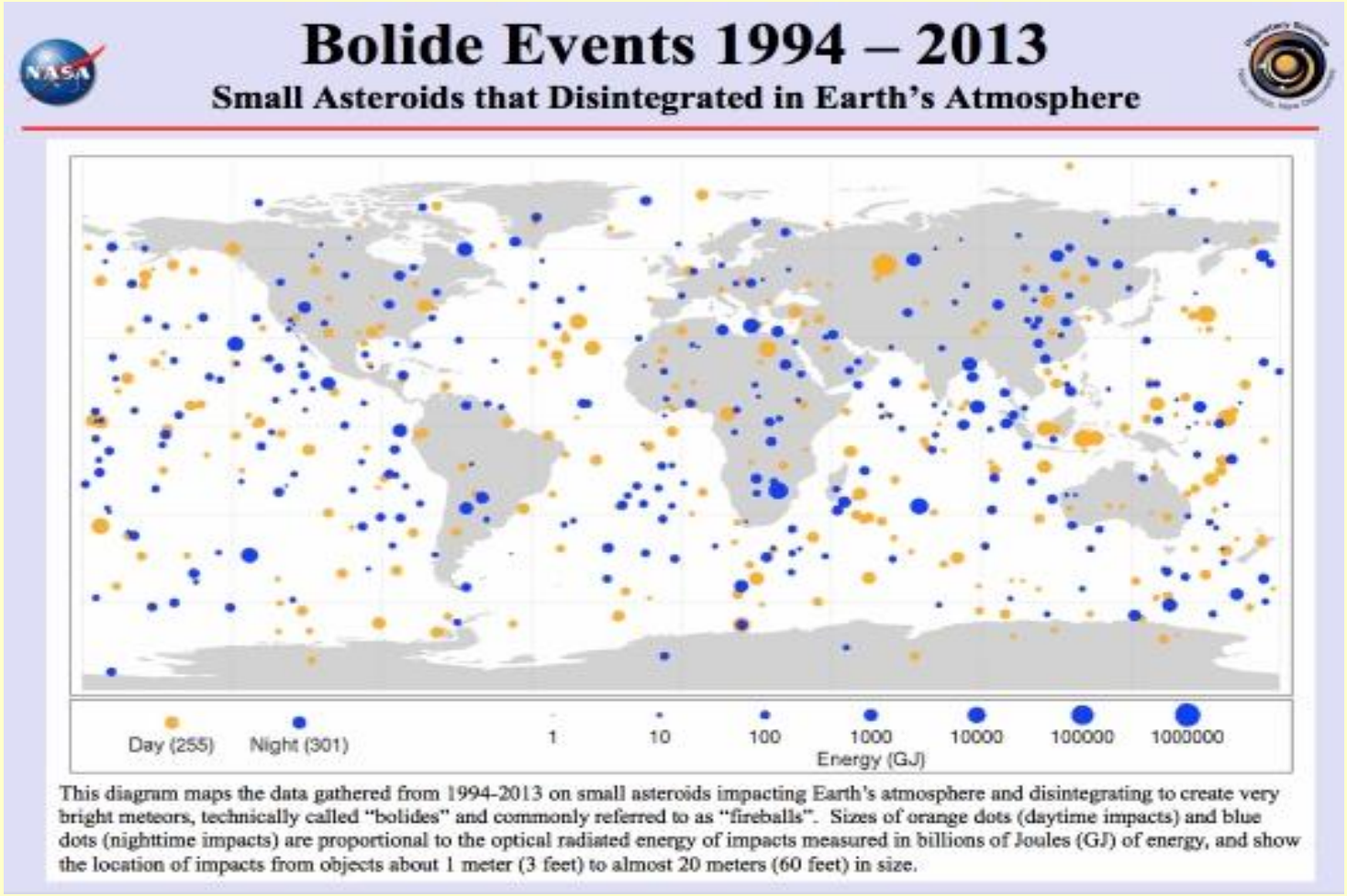
Source: http://neo.jpl.nasa.gov/news/news186.html

November 14 – It happens all the time: small asteroids impact Earth's atmosphere

Small asteroids near Earth, with sizes of only about a meter, hit the atmosphere and disintegrate with surprising frequency - around every other week, new data show.

Data gathered by U.S. government sensors and released to NASA for use by the science community reveal that these small impact events are frequent and random. A map of these small impact events - known as fireballs or bolides - recently released by NASA shows the frequency and approximate energy released by bolide events detected from 1994 through 2013. It dwarfs a data-base of small impacts based on infra-sound detections released last fall, but it does not contain all fireballs - objects less than a meter in size - that impacted the Earth during this period.

Over this 20-year interval, U.S. Government assets recorded at least 556 bolide events of various energies. On this world map illustration, the size of the orange dots (daytime events) and blue dots (nighttime events) are proportional to the optical radiated energy of the impact event measured in billions of Joules (GJ) of energy. An approximate conversion between the measured optical radiant energy and the total impact energy can be made using an empirical relationship provided by Peter Brown and colleagues in 2002. For example the smallest dot on the map represents 1 billion Joules (1 GJ) of optical



This diagram maps the data gathered from 1994-2013 on small asteroids impacting Earth's atmosphere and disintegrating to create very bright meteors, technically called "bolides" and commonly referred to as "fireballs". Sizes of orange dots (daytime impacts) and blue dots (nighttime impacts) are proportional to the optical radiated energy of impacts measured in billions of Joules (GJ) of energy, and show the location of impacts from objects about 1 meter (3 feet) to almost 20 meters (60 feet) in size.

radiant energy, or when expressed in terms of a total impact energy the equivalent of about 5 tons of TNT explosives. Likewise, the dots representing 100, 10,000 and 1,000,000 Giga Joules of optical radiant energies correspond to impact energies of about 300 tons, 18,000 tons and one million tons of TNT explosives respectively.

The largest impact energy recorded during this 20-year interval was the recent daytime Chelyabinsk event (440,000 - 500,000 tons of TNT) recorded over central Russia on February 15, 2013. This small asteroid that exploded in the atmosphere near Chelyabinsk, Russia was about 20 meters in size before it hit the Earth. While that impact focused public attention on the potential hazards of NEO impacts with Earth, space scientists have long known that such events are just a part of Earth's geologic history.

NASA's Near Earth Object (NEO) Observations Program finds, tracks, and characterizes asteroids whose orbits bring them within approximately 50 million kilometers (31 million miles) of Earth's orbit about the sun.

"We now know that Earth's atmosphere does a great job of protecting Earth from small asteroids", said NASA NEO Observations Program Executive Lindley Johnson. The new data will be extrapolated to estimate more precisely the frequency of impacts by asteroids large enough to cause ground damage. "How big is the population of larger asteroids we really need to worry about? We need to better understand that." Johnson said.

While the new data emphasize that small asteroid impacts with Earth are not unusual, the risk of future impacts is not to be taken lightly. "The aim is to find potentially hazardous asteroids before they find us," said Donald Yeomans, manager of NASA's NEO Program Office at the Jet Propulsion Laboratory.

NASA's Asteroid Initiative features a Grand Challenge to the community "to create a plan to find all asteroid threats to human populations and know what to do about them."

The NEO Observations Program already has identified more than 96 percent of the estimated population of nearly one thousand one-kilometer or larger sized asteroids. The Program's current objective is to identify 90 percent or more of the far more numerous NEOs larger than 140-meters in diameter. It is estimated they may be as much as 25 times more numerous than 1 kilometer asteroids.

Every day, Earth is bombarded with more than 100 tons of dust and sand-sized particles from space. About once a year, an automobile-sized asteroid hits Earth's atmosphere, creating a spectacular fireball (bolide) event as the friction of the Earth's atmosphere causes them to disintegrate - sometimes explosively.

Studies of Earth's history indicate that about once every 5,000 years or so on average an object the size of a football field hits Earth and causes significant damage. Once every few million years on average an object large enough to cause regional or global disaster impacts Earth. Impact craters on Earth, the Moon and other planetary bodies are evidence of these occurrences.

Meteor Crater near Winslow, Arizona, is evidence of the impact with Earth's surface of a 50-meter asteroid about 50,000 years ago. Impact of the metal-rich object released energy equivalent to a 10 megaton explosion and formed a 1.2 kilometer-diameter crater. Scientists have identified several dozen impact craters in North America alone, most masked by erosion and vegetation.

Scientific assessments of the risk of, as well as the hazards posed by, future asteroid impacts with Earth vary. In a 2013 paper published in Nature, Peter Brown and his colleagues reported that "telescopic surveys have only discovered about 500 near-Earth asteroids that are 10-20 meters in diameter (comparable to the Chelyabinsk asteroid) of an estimated near-Earth asteroid population of around 2×10^7 [20 million], implying that a significant impactor population at these sizes could be present but not yet cataloged in the discovered near-Earth asteroid population."

"These newly released data will help NEO scientists construct a more complete picture of the frequency and scope of asteroid impacts with Earth," said Johnson.

In conducting its work, the NEO Observations Program collaborates with other U.S. government agencies, other national and international entities, and professional and amateur astronomers around the world. NASA works closely with the Federal Emergency Management Agency and other federal government departments and agencies on NEO impact warning, mitigation and response planning. The Program is responsible for facilitating communications between the astronomical

community, the federal government and the public about NEO impact hazards and risks. The NEO Observations Program is a lead participant in a newly organized International Asteroid Warning Network.

EPC are delighted to announce Volume 2 of the Emergency Management Review

Source: http://www.epcollege.com/epc/news/epc-are-delighted-to-announce-volume-2-of-the-emer.aspx

We are delighted to announce that Issue 2 of the Emergency Management Review is now published. This is a peer-reviewed journal published for the UK emergency management community by the EPC (Emergency Planning College). It is edited by EPC Fellow, Eve Coles.

It contains an insightful editorial by Eve and a research digest on future city and community resilience. There is also a paper on social media in emergency management by Julia Meaton (Huddersfield University Business School) and Lisa Stringer (Public Health England). Eve Coles supplies another article that should interest all practitioners, on professionalism and professionalisation in the emergency management business. The book review section features reviews of key publications carried out by Nigel Kay (EPC Lecturer), Mark Leigh (EPC Faculty Director) and Dr Robert MacFarlane (CCS).

This journal is funded by the EPC and the CCS, the national thought leaders and policy makers in civil protection and emergency management, as a free service to the resilience community.

COSMIC Project (EU-funded)

Source: http://www.cosmic-project.eu/

Recent years have marked a watershed in the use of new communication media during crisis situations and disasters. Citizen journalism has proliferated around the world, where news, events and oddities are recorded by ordinary people and shared globally through mediums such as YouTube, Twitter, Facebook and other outlets.

COSMIC project will identify the most effective ways in which these new technologies and applications are being used by citizens and governments. The project will also provide instruments for all relevant stakeholders to use new

information and communication technologies for the benefit of the security of all citizens.
The COSMIC project is an EU-funded project from the European Commission's Seventh Framework Programme FP7-SEC-2012 under grant agreement no. 312737. The COSMIC project's total budget is 1,2 million Euros, of which EU funding accounts for 997 thousand Euros. The project runs for the period of 24 months, ending in March 2015.

▶ **NEW: First set of COSMIC guidelines now available!!!**
Guidelines for the use of new media by the public in crisis situations
Guidelines for the use of new media by public and private organisations

Fire Trucks: What are the different types?

Source: http://d4h.org/blog/post/20141216-fire-trucks-what-are-the-different-types

A typical modern fire truck carries equipment for a wide range of firefighting and rescue tasks. Fire apparatus are often adapted to their areas of operation. Compiled is a brief overview of some of the variations available.
A fire truck also known as a fire apparatus, fire engine, or fire appliance, is a specific vehicle designed primarily for firefighting. Many organizations employ fire engines for various other uses including EMS, hazmat, auto extrication and technical rescue. Its main roles include transporting firefighters, along with a supply of water and a full compliment of equipment.
Here is a quick overview of some of the types of appliances in operation today:

Conventional Fire Appliance

The conventional fire apparatus which can also be called a fire appliance, fire tender, fire engine, water ladder, pumper or pump-ladder has several methods of pumping water onto the fire. The most common method is to pass water from a pump through hoses to the fire.

Airport Crash Tender

An airport crash tender is a fire engine designed for use at aerodromes in aircraft accidents. The features include good acceleration, ability to move on rough terrain outside the runway and airport area, large water capacity, a foam tank and a high-capacity pump.

Turntable Ladder

A turntable ladder is perhaps the best-known form of special purpose aerial apparatus, and is used to gain access to fires occurring at height using a large telescopic ladder, where conventional ladders carried on conventional appliances might not reach.

Command Support Unit

The advancement of technology and potential for very large-scale incidents has led to many fire departments utilizing or increasing their use of mobile command support units. A fundamental advantage of such an appliance is to accommodate the many different types of communication equipment needed at major incidents.

Tower Ladder

Some turntable ladders may have a basket mounted at the top of the ladder, as on a hydraulic platform and these are called tower ladders. These appliances can provide a secure place for a firefighter to operate equipment from.

Hydraulic Platform

A hydraulic platform, also known as articulating booms, snorkels and platform trucks,is a specialized aerial work platform designed for firefighting use. They have a number of functions, which follow the same principles as the turntable ladder, providing high level access and elevated water pump positions. Some hydraulic platforms are articulated, which allows the arm to bend in one or more places, giving it the ability to go "up and over" an obstacle.

Heavy Rescue Vehicle

A heavy rescue vehicle, sometimes referred to as a Rescue Company, Rescue Squad or Technical Rescue, is a type of specialty firefighting or EMS apparatus. Essentially giant toolboxes on wheels, they are primarily designed for technical rescue situations such as vehicle extrications following traffic collisions, confined space rescues, rope rescues, swiftwater rescues, or building collapses.

Hazardous Materials Apparatus

Many fire departments covering large metropolitan areas or those containing many high-risk hazards keep specialist appliances for dealing with hazardous materials (HAZMAT). These are of several types, from those used to clean spilled oil on streets and highways, to full decontamination units, designed to clean victims and rescuers of contaminants after an incident.

Tanker Truck

A tanker truck is a specialist fire appliance with the primary purpose of transporting large amounts of water to an emergency to make it available for extinguishing operations. These are especially useful in rural areas where fire hydrants are not available and natural water resources are insufficient or difficult to exploit.

Foam Tender

Foam tenders carry large amounts of foam to be used at incidents where water is ineffective or cannot be used to tackle a blaze. They may take the form of a tanker, or a truck carrying foam packets or barrels.

Climate Change and EU Security - When and How they Intersect

By Gerald Stang

Source: http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?ots591=4888caa0-b3db-1461-98b9-e20e7b9c13d4&lng=en&id=185868

The potential security challenges linked with climate change can make for great headlines. While sensationalist claims about water wars, states collapsing in chaos or the forced migration ofhundreds of millions cannot be completely discounted for the long term, intelligent mitigation and adaptation efforts can help avoid the worst of these – and manage the rest. **Planning these efforts, however, requires that the likelihood and time frame of climate change impacts are well understood (as much as they can be); that security challenges associated with these impacts are placed in their proper context; and that resilience mechanisms, including security and defence systems, are appropriately organized to withstand potential shocks.** And while much analysis is necessarily focused on potential climate-related threats abroad – climactic stressors that can change the calculus of potential conflicts in far-off lands – climate change will also impact security and defence considerations closer to home.

A US pivot

While Washington is often seen as slow to respond to the challenge of climate change, the surprise announcement of a joint climate accord between China and the US signifies agreement between the world's two largest carbon emitters (and major geostrategic competitors) on the need to share the burden of emission mitigation. It has shown that, despite discord in Congress, the American executive branch takes climate change very seriously and retains the capacity to take significant action.

The American security establishment has also been quick to incorporate the potential risks of climate change into its strategic planning. The recent release of the latest version of the Climate Change Adaptation Roadmap by the US Department of Defense highlights the potential impacts of climate change on the department's infrastructure, logistics support, training and operations. A few months before, a group of retired US officers produced a paper for the CNA Corporation, a US Navy-affiliated research organisation, taking a broader view by looking at the threat of climate change to the political, military, social, infrastructure, and information systems that constitute American 'national power'. Climate change has clearly become relevant for the strategic thinking of the US intelligence and defence communities, moving beyond its status as a mere environmental issue.

The updated Adaptation Roadmap focuses on how climate change will impact military capabilities. Other strategic documents (including the 2014 National Intelligence Strategy and

2014 Quadrennial Defense Review) describe climate change as a 'threat multiplier' which will affect strategic calculations about security and conflict in various corners of the world. This viewof climate change is widely spread, having been expressed by both the UN secretary general in a 2009 report and by the EU high representative for foreign affairs and security policy in a 2008 paper on climate change and international security.

The Global Security Defense Index on Climate Change lists 110 countries which have identified climate change as a security threat, including most regional leaders but with notable exceptions such as Brazil, India and Egypt. This apparent threat perception has seen climate change added to lists of complex, non-traditional and transnational threats (often including energy security, arms proliferation, terrorism, the continued rise of non- state actors and cyber attacks) in the national security policies of many states, though detailed analysis of the expected impacts, and how to respond to them, are rarer.

Although most European states acknowledge the potential threats posed by climate change, its impacts have yet to be deeply integrated into their strategic planning (though the UK is expected to do so over the next year). The EU has increasingly mainstreamed climate change issues in its work across multiple sectors, with at least 20% of its near-trillion euro 2014-2020 budget expected to be spent on climate change-related action. But Europeans have not engaged with climate change as a security issue as comprehensively as the US has, potentially due to the international exposure of the US with its globe-spanning range of responsibilities and military facilities.

Cutting emissions, but not enough

While climate security issues have been raised in international fora in recent years, including at the UN Security Council, international climate discussions have been primarily, and rightly, focused on emission mitigation. When world leaders met in September for the UN Climate Summit, China reiterated its goals of reducing the carbon intensity of its economy, already achievable on a business-as-usual trajectory, while other countries announced forest protection efforts (Norway), automobile emission standards (Canada) or green energy goals (India). The EU, a world leader in mitigation efforts but still hesitant to take drastic action until others also do, shared the centerpiece of its 2030 framework policy for climate and energy, a plan to cut emissions by 40% by 2030 compared to 1990 levels.

This mixed bag of announcements is a reflection of how politicised and complex climate issues are for every nation. In the remaining months before the 2015 Conference of Parties (COP 21) climate summit in Paris, negotiators will struggle to reconcile a vast range of national negotiating positions in order to push the globe towards the deep decarbonisation pathways which are necessary to avoid the worst long-term climate impacts.

Unfortunately, no matter how quickly mitigation efforts proceed, significant climate change impacts will be unavoidable. These impacts can generally be split into two categories: slow onset (changing rainfall patterns, rising sea levels) vs. rapid onset (extreme weather, flash floods). The worst slow onset impacts are expected to hit some of the world's most vulnerable areas hardest. In several parts of both northern and southern Africa, agriculture-dependent populations with limited economic and infrastructure capacities will likely face major temperature rises and significant changes in rainfall later this century. The driest areas in the Middle East may become drier still, while changing monsoon patterns may wreak havoc on agricultural production in impoverished and densely populated parts of South Asia, particularly if poor water management practices continue.

The most recent predictions from the Intergovernmental Panel on Climate Change (IPCC) indicate that the global mean sea level will continue to rise at an increasing pace and, by 2081-2100, could range from 0.26 to 0.82m above the mean for 1986-2005. Low-lying coastal regions will thus increasingly be threatened withflooding, erosion and loss of wetlands. The expected slow pace of sea level rise over the coming decades should allow for the development of resilience mechanisms in Europe, but adaption will be a greater challenge for poorer states with significant areas of low-lying territory, notably in South Asia, the Caribbean and the western Pacific Ocean.

For all countries, however, even slow increases in sea level could be problematic if combined with an increase in rapid impact weather events such as cyclones,

storm surges, and flash floods. With a third of its population living within 50km of the coast, and as much as a trillion dollars in assets located within half a kilometre of the sea, Europe has plenty of reason to keep an eye on sea levels and storm surges.

But it is early days yet. The IPCC predicts that for another two or three decades, increases in climate extremes may be difficult to differentiate from the normal year-to-year variations, but in the decades that follow, storms and disasters will become increasingly likely to challenge Europe's disaster protection and response systems. In terms of slow onset impacts, the IPCC predicts comparatively modest impacts for Europe over the coming century, including gradually increasing precipitation in northern Europe but decreasing precipitation in the south, with attendant impacts in agricultural production in the two regions.

With its urban population and limited reliance on agriculture for jobs and growth, Europe is better placed to adapt to slow onset events than other parts of the world. But climate change is still expected to impact European security by focusing attention on rapid onset climate impacts, changing the nature of international threats, and influencing Europe's capacity to respond accordingly.

Domestic impacts on security

While Europe generally has calmer weather systems than the hurricane-plagued Caribbean or the typhoon-haunted north Pacific, planning for weather-related disasters will become increasingly important. The EU's 2013 Adaptation Strategy is focused on 'climate-proofing' EU action, ensuing that Europe's infrastructure is made more resilient, promoting the use of disaster insurance, providing funding for cross-border water and flood management, and expanding protection of areas with high drought, desertification or fire risks. Europe has already made disaster management an important part of its adaptation efforts with the EU Emergency Response Coordination Centre (ERCC) monitoring emergencies around the world and coordinating responses both within and outside the EU.

With the likelihood and severity of climate-related disasters expected to increase over the coming decades, the role of European militaries in disaster prevention and response may also grow. The military can provide important search and rescue capacity, logistical support, manpower and material resources. Within individual countries, troops have often responded to disasters – and the Lisbon Treaty has solidarity and mutual assistance clauses to allow joint defence action to face attacks or natural catastrophes – though no formal operational mechanisms have yet been putin place to facilitate cross-border military cooperation using these clauses.

While grateful publics will always laud soldiers who lend a hand in disaster response at home, increased use of militaries for disaster response may potentially divert resources from other priorities. Climate change may also reduce the fighting ca pability of military forces by putting security logistics, infrastructure, and transportation systems at risk (notably in coastal areas), and by changing the environmental conditions in which they train and operate.

Following the American lead, climate change adaptation strategies for European militaries are likely to become increasingly common in the next few years as national security establishments are called upon to develop appropriate capabilities, priorities, and responses.

External security challenges

But it is the possibility of climate-related security challenges abroad which can cause security analysts to react, or overreact. In recent years, conflicts from Syria to Darfur have been highlighted as models of what the future may hold, as droughts and mass migration increase the likelihood of instability and violence. Climate change impacts can be seen as additional stressors which may contribute to conflict risks in a number of ways.

First, increased frequency of droughts or floods could disrupt agricultural livelihoods, rural incomes and local systems of ensuring food security, thereby triggering conflicts over water and land. Second, increases in the severity and frequency of extreme weather events could lead to ocial and state instability. Third, various climate impacts could trigger potentially destabilizing mass migration, as migrants flee across borders or to cities that lack the infrastructure or job opportunities to accommodate them.

Finally, if potential climate change impacts are perceived as requiring responses from security

institutions, the 'securitisation' of responses to climate change may occur, providing a pretext for militarisation, inhibiting cooperative efforts to adapt to climate change. This could be especially worrying in areas where maritime borders are unclear and coastlines are changing due to rising seas.

Prevention and response

The likelihood of these risks turning into major security problems will depend on the severity of the impacts, the vulnerability of those impacted, and the response when they occur. Reducing the severity of future climate impacts can only be done through improved emission mitigation to slow the pace of global warming, an immense challenge on a global scale. Reducing vulnerability to climate change impacts will require local improvements in physical, social and political resilience of populations and states. Richer societies with well-developed infrastructure, low reliance on agriculture for livelihoods, good storm warning and disaster response mechanisms and capable, responsive governments are better equipped to handle climate change. But many societies lack some (or all) of these capacities. A preventative approach, involving all of the development and diplomatic tools at hand, will be important to help build resilience in vulnerable areas and reduce the likelihood of future conflicts arising.

For Europe's security community, decisions over whether and how to respond to future conflict and disaster situations abroad are less likely to be influenced by whether climate change was a factor than by the same political and humanitarian factors that shape such decisions today.

A Europe that is better prepared to respond to the threat of weather-related disasters at home may find itself involved in responding to a larger number of disasters abroad, and in dealing with the associated humanitarian and security consequences. Even without climate change, continuing population growth and changing patterns of human settlement may lead to an increased need to respond.

European security planning may thus increasingly include the possibility of responding to disasters abroad, though political norms for (and public acceptance of) the use of military capabilities for such interventions are in flux. Continued reduction in the capacity and interest of European militaries to project force to distant lands would reduce the likelihood that they would play a dis aster response role in the same theatres – particularly if increasing efforts are made to outsource response capacity by training and equipping local actors through both development and military cooperation programmes. Recent trends toward broadening national security definitions and of using 'whole-of-government' processes for international engagement may also change how security institutions engage with the climate adaptation work already underway, generally led by the development community.

Looking ahead

In the end, addressing the potential security implications of climate change will require action to manage the expected risks, while keeping a sense of perspective about time frames and impacts. Climate impacts are real, growing, and could eventually become catastrophic on a global scale. High impact weather events, in particular, may directly affect the capacities of European security establishments, but for the next 20 or so years, Europe will likely only be experiencing the early stages of climate change. Slow onset climactic changes will eventually change European climates and systems of managing natural resources, but pending any sudden climactic shifts (a real possibility), the continent will be able to manage its adaptation to climate change without major domestic security worries for at least the next few decades.

Internationally, however, too many countries lack resilience, have weak or brittle ruling regimes and are experiencing unsustainable population growth. It has often been stated that preventing conflicts before they start is better than attempting to respond to them once they turn into a crisis. The gradually increasing effects of climate change in the coming century may provide plenty of opportunity to put this idea into practice.

Gerald Stang *holds BSc and MSc degrees in chemical engineering from the University of Saskatchewan and an MA in international affairs from the School of International and Public Affairs at Columbia University. He specialises in energy politics, democratic transitions and foresight in international relations.*

Asymmetry Is Strategy, Strategy Is Asymmetry

By Lukas Milevski

Source: http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?ots591=4888caa0-b3db-1461-98b9-e20e7b9c13d4&lng=en&id=184816

Of all the new descriptors for war, "asymmetric" is among the broadest. It has even been suggested that *asymmetry* does not bear definition: "to *define* the term *defies* its very meaning, purpose, and significance."[1] Some, undeterred by such extreme pronouncements, have attempted at least to categorize various existing and potential concepts of asymmetry. Thus, **Jan Angstrom has identified four different prisms through which asymmetry may be interpreted: "power distribution, organisational status of the actor, method of warfare, and norms."**[2] Yet despite claims of newness, it has also been observed that asymmetry has infused nearly every, if not every, war in recorded history. (Possibly only the hoplite phalanxes of ancient Greece could be considered properly symmetrical in nearly all respects, for geography, demographics, and so forth make all polities fundamentally asymmetrical to some degree.) Misunderstanding asymmetry poses significant dangers: "our misuse of the terms asymmetry and asymmetric distorts those vital processes and leads us to make major strategic blunders. For example, by focusing on threats rather than enemy strategies we fail to understand their strategic nature, goals, and overall concepts of operations."[3]

The question thus arises: how may one fruitfully discuss asymmetry as a separate phenomenon? Perhaps the time has come to abandon the endeavor as unhelpful and rather suggest that asymmetry in war, and even asymmetric strategy, are redundancies. *Asymmetry is strategy, and strategy is asymmetry*. **This article argues the point in three parts. First, it suggests that observations of a novel change are overexaggerated. Second, it maintains that no matter the form war may take, the function of strategy is eternal. Third, it proposes that contemporary asymmetric conflicts are all comprehensible through the lens of strategy.**

Form over Substance

Theorists of contemporary conflict, whether describing asymmetric or unconventional wars, war among the people, or other iterations of modern armed conflict, usually posit significant change in the character, if not actual nature, of war. Many of them accurately identify and analyze the characteristics of modern interventions. In perceiving significant differences between modern war and wars past, however, they caricature historical conflict.

Thus, Rupert Smith argues that "war as cognitively known to most non-combatants, war as battle in a field between men and machinery, war as a massive deciding event in a dispute in international affairs: such war no longer exists."[4] Martin van Creveld propounds the notion that "the demise of conventional war will cause strategy in its traditional, Clausewitzian sense to disappear."[5] Fourth-generation warfare theorists such as T.X. Hammes identify generations of warfare with particular styles of conducting war; third-generation warfare is, for example, maneuver warfare, and fourth-generation warfare "uses all available networks—political, economic, social, and military—to convince the enemy's political decision makers that their strategic goals are either unachievable or too costly for the perceived benefit. It is an evolved form of insurgency."[6]

Yet their theories on the changes in war depend upon caricaturing what came before. They have succeeded somewhat in part because many centers of strategic education similarly caricature historical war. These caricatures rely on a Eurocentric perspective of strategic history. Smith's war as a battle in a field between men and machinery and Hammes's third-generation warfare as maneuver

warfare, for example, both rely on the World Wars, especially World War II. These wars were fought among European or Western polities, all of which have similar strategic cultures. Yet modern interventions primarily take place between Western powers and polities elsewhere in the world, with significant differences in strategic culture. Theorists of change in war are comparing apples with oranges and perceiving change based on such flawed comparisons, which serve only to churn various fashions in strategic thought.

To analyze interventions, comparisons to the Third Afghan War of 1919 or the Rif War of 1919–1926 would much more accurately demonstrate how much war has actually changed. Similarly, conventional war must be compared to conventional war. Notably, Russia's 2008 invasion of Georgia did not trigger a Georgian insurgency against the Russians, or even against the Abkhazians or South Ossetians. The war remained conventional throughout. The Iraq War of 2003 did transform into an insurgency, but not immediately. The period of a few months between the end of conventional operations and the serious beginning of the insurgency was terribly squandered by the United States, which visibly failed to begin righting the country. Although it would be incorrect to say that this great strategic and political failure caused the insurgency, it certainly exacerbated it.

Hew Strachan has suggested that "the real problem may well be that our policy has failed to recognise war's true nature, and so has mistaken changing characteristics for something more fundamental than they actually are."[7] This mischaracterization is frequently manifested in the belief, as apparent before Iraq in 2003 and during some of the advocacy for intervention in Syria in 2013, that war is not adversarial, that enemies do not reciprocally interact with, and against, each other. The character of any war is not unilaterally set by any one implicated polity, but by the reciprocal hostility of all those involved. Thus, in not accounting for the enemy's own initiative against us, the Western powers are blindsided by actions that are then interpreted as integral to the structure of contemporary war rather than as the consequence of something inherent in war, which is more fundamental and eternal.

Asymmetry and Strategy

That which is eternal is strategy, the purposeful threat or use of violence to achieve desired ends. Strategy has no permanent form, although it always retains its enduring substance and function. Strategy has always been practiced, even though before the word's rediscovery in the 1770s, strategies explicitly labeled as such may not have been expressly planned or implemented.[8] The core task of strategy may be identified as Everett Dolman does: "strategy, in its simplest form, is *a plan for attaining continuing advantage*."[9] Dolman rightly observes that the strategist's task is usually aided more by advantage than disadvantage. "Advantage," like strategy, is not defined by a particular form. Advantage may take the form of materiel, political will, a superior grasp of how to translate forces deployed into aims achieved, or so on. Understanding war and all the influences on it is necessarily multidisciplinary; therefore, asymmetry may manifest itself in a similarly wide range.

Strategy may be thus cast in a more absolute manner than merely the achievement of continuing advantage. Rather, strategy may be interpreted as *the generation and exploitation of asymmetry for the purposes of the war*. Roger Barnett complains that:

> *asymmetries arise if opponents enjoy greater freedom of action, or if they have weapons or techniques available to them that one does not. Perpetrators seek to void the strengths of their adversaries and to be unpredictable. They endeavor to take advantage of an ability to follow certain courses of action or to employ methods that can be neither anticipated nor countered effectively.*[10]

Yet this is the very essence of strategy. Strategy is an adversarial act; the enemy also has a will, a capability, and a vote in the outcome. This reciprocal nature of strategy is a primary source of strategy's nonlinearity, for defeat may beget renewed defiance and alternative attempts to achieve one's goals, rather than the desired submission. Thus, Edward Luttwak, for instance, identifies the very pinnacle of strategic performance as "the suspension, if only brief, if only partial, of the entire predicament

of strategy."[11] The predicament of strategy is the enemy. The pinnacle, therefore, is the removal of the enemy's ability, however temporarily, to influence outcomes. Suffering from a position of weakness in an asymmetric relationship restricts one's abilities to influence outcomes based on that relationship. To generate asymmetry effectively is to be, although not necessarily the only way to be, a skilled strategist.

The generation of asymmetry is the basis of much, if not most, strategic theory, particularly power-specific theories such as those pertaining to seapower or airpower. Command of the sea or of the air cannot mean anything other than the generation of a major operational asymmetry in either of those warfighting domains relative to the enemy. Similarly, the very idea of massing and applying one's forces against the decisive point, a theme in both Antoine-Henri Jomini's and Carl von Clausewitz's works, is to generate asymmetry in a particular location, to achieve the desired wider effects. The debates about the revolution in military affairs and transformation are also ultimately about generating significant asymmetry, albeit in the form of a particular silver bullet. Cold War nuclear strategy was similarly meant to establish asymmetries of commitment, even when theorists might not be able to make operational sense of asymmetries of capability, particularly in the theories of Thomas Schelling. The strategic theories of Basil Liddell Hart were so steeped in the generation of asymmetry that it apparently affected his understanding of the moral component of strategy. He focused relentlessly on the indirect approach to create situations in which the enemy would be utterly helpless, therefore hopeless, and so would surrender without undue bloodshed, thereby removing killing from the concept of morality in strategy. Instead, "strategy is the very opposite of morality, as it is largely concerned with the art of deception," in reality not because killing had no place in morality, but because killing had no place in his idea of good strategy.[12]

Asymmetry is thus clearly compatible with conventional warfare, simply because it is good strategy. During World War II, the conventional war par excellence, the Allies ultimately established major asymmetries in military-industrial production and logistics, on the sea, and in the air over all the Axis countries. World War I was a bloody stalemate on the Western Front for so long in large part because until 1918 neither side was able to generate the asymmetries required to break it. The belligerents who generated the most important asymmetries ultimately won. Not all asymmetries are equal; some may be more immediate than others, some may be ultimately more damaging to one's ability to achieve desired goals than others, and so on. Effective asymmetry, like effective strategy, is context-sensitive.

Asymmetry is strategy, strategy is asymmetry. Conrad Crane of the U.S. Army War College is reputed to have suggested that "there are two types of warfare: asymmetric and stupid."[13] Generating effective asymmetry is good strategy. To condemn rhetorically our opponents for generating asymmetry reveals our conditioning born of understanding recent history through the prism of wishful thinking, of expecting one's enemies to be poor strategists such as those faced in 1990–1991, 2001, and 2003. Wishful thinking, operationalized as unrealistically optimistic assumptions, does not usually lead to strategic success, as our experience of the variably labeled "war on terror" or "Long War" clearly indicates.

One might counter that conventional asymmetries on land, sea, and air are far more easily understood than unconventional asymmetries such as guerrilla warfare. This may indeed be the case, but so what? One may understand a threat and still be incapable of countering it. German General Fridolin von Senger und Etterlin, who had participated in the Italian campaign of 1943–1945, once likened operating under Allied air supremacy to playing chess against an opponent who could play three pieces each turn to his one. No amount of understanding of the threat can help alleviate a situation if that understanding cannot be turned into operational plans and successful outcomes. This is just as true of conventional asymmetries as of unconventional ones. In fact, conventional asymmetries are usually the more dangerous of the two for their ultimate political effects are usually greater, as the experience of warlords from Darius III to Napoleon to Adolf Hitler may attest. Each lost his empire to enemies who were ultimately more capable of generating effective asymmetry. Relatively few unconventional asymmetries have had the historical effect equivalent to losing an empire.

One of the few pertinent, albeit inexact, examples is the American Revolutionary War, but even that war was "hybrid" rather than purely unconventional.[14]

Strategy in Contemporary War

Asymmetry today is most commonly associated with insurgency and irregular foes. Contemporary theories on strategies for counterinsurgency also implicitly emphasize the generation of effective asymmetry against the so-called asymmetric enemy. Unlike the generation of conventional asymmetries, many of which tend to be domain-oriented, contemporary counterinsurgency theory emphasizes asymmetry from the perspective of the population's support, through the provision of security and other services, including effective governance. David Galula is frequently identified as the progenitor of this theory. It is nevertheless significant that his proposed strategic blueprint for counterinsurgency only begins with the destruction or expulsion of insurgents as an organized body and ends, after the organization of local communities into effective and self-sustaining political entities, with the destruction of the last of the insurgents.[15]

Force does not lack utility against a foe that is generating unconventional asymmetry. Indeed, the very form of that asymmetry reveals a significant concern about one's own conventional military superiority over the insurgent. Unconventional asymmetry is guerrilla warfare, arising from military weakness and infused with concern for the survival of the insurgent force. Without that force, the insurgency is likely to fail. Galula noted that "in any situation, whatever the cause, there will be an active minority for the cause, a neutral majority, and an active minority against the cause."[16] A neutral majority will acquiesce to whichever party appears most likely to succeed. One of the most publicly visible features of such a measurement is the apparent effectiveness of the respective armed forces. The truism that the counterinsurgent loses if he does not win, but the insurgent wins if he does not lose, is indicative of this. Once the counterinsurgent, superior in strength, fails to win and so withdraws from the conflict, the only remaining viable power in the country will be the insurgent force. This truism is, of course, true only in the context of intervention because the counterinsurgent ultimately *must leave*; it is not an iron law of insurgency as such, as the example of Sri Lanka may attest.

This observation is not new to contemporary war. C.E. Callwell, one of the major luminaries of historical British strategic thought on small wars, offered an explanation at the end of the 19th century: "It is a singular feature of small wars that from the point of view of strategy the regular forces are upon the whole at a distinct disadvantage as compared to their antagonists." In battle, however, regular troops have the tactical advantage: "Since tactics favour the regular troops while strategy favours the enemy, the object to be sought for clearly is to fight, not to manoeuvre, to meet the hostile forces in open battle, not to compel them to give way by having recourse to strategy."[17] The imbalance of military power between intervener and insurgent was, and remains, the basis for the guerrilla's choice of strategy.

It is noteworthy in this context that, of the four great theorists of insurgent warfare, T.E. Lawrence, Mao Zedong, Vo Nguyen Giap, and Ernesto "Che" Guevara, only Lawrence did *not* theorize the eventual transition from guerrilla to relatively, if not absolutely, conventional warfare for the final campaigns definitively to seize power from the government forces. Lawrence, of course, fought as part of a larger conventional operation commanded by General Edmund Allenby and so had no need to turn his fighters into a conventional force. This is not to argue that members of the Taliban are running around the Hindu Kush with Mao's little red book in their pockets, but rather that these authors identified the limits of guerrilla warfare. Thus, not even insurgency may violate the fundamental truth which J.C. Wylie observed: "the ultimate determinant in war is the man on the scene with the gun. This man is the final power in war. He is control. He determines who wins."[18]

The enemy relies upon unconventional asymmetry if he believes himself unable to succeed without it. The Taliban in Helmand Province only turned back to tried-and-tested guerrilla tactics after suffering disastrous casualties in futile frontal assaults on British bases. This adaptation coincided with the loss of widespread local support, as "the cost of aligning themselves with the Taliban turned out to be very high for many communities in terms of destruction and loss of life," as well as with consequent Taliban

attempts to regain some local legitimacy and support.[19] The generation of asymmetry through guerrilla tactics has both advantages and disadvantages, which must be examined with respect to the function of strategy, that is, the conversion of violence into desired political effect for both the insurgent and the counterinsurgent.

The basis of strategy is war, the purpose of which "is some measure of control over the enemy." Control is a rarely defined term whose limits are quite broad, being "neither so extreme as to amount to extermination . . . nor . . . so tenuous as to foster the continued behavior of the enemy as a hazard to the victory."[20] The pattern of events in war is driven by the reciprocal interaction of adversaries, "a contest for freedom of action."[21] Since control pertains to freedom of action, one might identify three different categories of control. The weakest form of control is merely the denial of control, or preventing the enemy from unduly restricting one's own freedom of action. Once a belligerent is relatively strong enough, he may attempt to take control and threaten actively to limit his opponent's freedom of action. The final type of control is its exercise after having taken it, to prosecute the war to a successful conclusion. Much of strategic theory assumes that a belligerent without freedom of action or the ability to pursue his political goals will ultimately abandon his endeavor.

Unconventional asymmetry is capable only of denying control to the superior enemy. Despite being the weakest form of control, it remains potent. A strategy based upon the accumulated effect of minor actions and continued elusiveness to deny control of the operational pattern of the war presents significant difficulties for the opposing side. Presenting no single set of targets and acting against and among civilians across geographies larger than their opponents may completely secure provide the counterinsurgent with a wide array of potential choices, whose strategic worth may be estimated but hardly known. Thus, Harry Summers caustically noted that during the Vietnam War, the United States identified up to 22 different wartime objectives.[22] This plethora of choice encourages unproductive or even counterproductive actions and contradicting policy goals on the part of the conventionally superior force. For instance, in Afghanistan, U.S. policies simultaneously require the local warlords to be liquidated for purposes of state-building and to be preserved to fight the Taliban.[23] Unconventional asymmetry targets the stronger foe's strategy rather than the enemy himself. The counterinsurgent, if unable to bring force or other tools effectively to bear to weaken the insurgency, merely marks time with blood. Time is a precious commodity in strategy and must be used wisely, but the substantial intellectual challenge facing the counterinsurgent places significant obstacles on the path of so doing.

Despite its deleterious effects on the stronger opponent's strategic performance, unconventional asymmetry is a serious strategic gamble. Although it denies control to the enemy, the insurgents themselves also do not gain control over the pattern of the war. Both sides tend to have the maximum freedom of action possible in an otherwise reciprocally adversarial context. The Viet Cong might skulk into Saigon to plant explosives, but the Marines could hold Khe Sanh, within spitting distance of the Ho Chi Minh Trail, which was absolutely vital to the Viet Cong and the North Vietnamese army in South Vietnam. In such a situation, barring any dramatic changes, rarely is there a clear indication of who holds the advantage until the conflict itself actually ends.

Strategy poses a difficult challenge due to the nonlinearities involved, many of which stem from the active presence of an independently acting adversary. Yet on the sliding scale of difficulty, the generation of asymmetry through guerrilla warfare may almost be a leap of faith. Although the skilled guerrilla retains initiative in being able to choose his own battlefields, the power of decision is preserved for his foe. The denier of control has no direct influence on the perception of his efforts in the opposing headquarters; he cannot impose a victory, but can only wait until his opponent acquiesces to defeat. Although today insurgents are able to fight figuratively in the media as well as literally on the ground, the pressure of public opinion seems to count for less in wartime than in peacetime because of the other pressures war generates: "The declaration of war, and more immediately the use of violence, alters everything. From that point on, the demands of war tend to shape policy, more than the direction of policy shapes war."[24]

The generation of asymmetry through use of guerrilla tactics may be a strategy that Western powers find difficult to defeat,

despite more than a decade of constant experience with attempting to combat it. It is nevertheless fundamentally the same phenomenon as generating asymmetry through commanding the sea or the air and may be understood with the same basic toolbox of strategic concepts. British mastery of the seas largely bewildered French attempts to defeat it for over a century and resulted in the French development of a number of methods by which to strike at British command of the sea without directly challenging it, including the *guerre de course* and the later jeune école, which was obsessed with the potential of torpedo boats. Today the roles are reversed, for the weaker belligerent has bewildered the Western powers and left them scrambling to determine how to combat the threat.

Many time-tested methods of defeating guerrillas directly are unacceptable to liberal powers today. As David Kilcullen puts it, "Indeed, any given state's approach to counterinsurgency depends on the nature of the state, and the concept of 'counterinsurgency' can mean entirely different things depending on the character of the government involved."[25] These methods may also be inappropriate for the specific conditions in which Western powers find themselves. Treating counterinsurgency as social work is more amenable to Western sensitivities than treating it as war. Although counterinsurgency definitely is the latter, it may well be both. Violence remains the base coinage of strategy, but this does not rule out the utility of counterfeits or other instruments of political power. One must remember that these tools are merely used as replacements for violence in specific circumstances where they may effectively take the place of force. War is war, but war is also politics. The other instruments of political power do not lose relevance once violence begins, but their utility is tempered by the introduction of force.

Moreover, it may be possible that today, compared to all prior historical experience, it is easiest for liberal powers to track and target insurgents. This is due to a number of factors, including the widespread use of new communications and other technologies, and new techniques to use this technology.[26] Taking the fight directly to the insurgents has become a plausible option for liberal democracies in a way that would not have previously been allowed, with massive cordons and conscription of locals to serve in temporary militias. With an increasing ability to strike desirable insurgent targets directly and relatively precisely comes an opportunity, in theory but also necessarily tempered by the actual circumstances of practice, to render relatively ineffective the generation of asymmetry through guerrilla tactics. The particular character of specific asymmetries does not change the fact that they all may be comprehended through the lens of strategy.

Conclusion

Rupert Smith is skeptical of the idea of asymmetric warfare. He rightly indicates that "the practice of war, indeed its 'art,' is to achieve an asymmetry over the opponent. Labeling wars as asymmetric is to me something of a euphemism to avoid acknowledging that my opponent is not playing to my strengths and I am not winning."[27] Smith's euphemism implies that the opponent is practicing strategy better than the Western powers are; since the practice of strategy determines how any particular polity engages in warfare, the implications of poor strategic practice are grave.

Asymmetry as now commonly used—to denote a supposedly particular new type of war—is not a useful term and, for some, implies strategic ethnocentric hubris that "assumes there is only one truth and model for warfare, and that we alone have it."[28] In fact, today and historically, most strategies seek to generate asymmetry as a way of minimizing the enemy's vote on the character and outcome of the war. Lawrence Freedman once defined strategy as "the art of creating power."[29] Given that power is a necessarily relational quality—for one cannot have power in the absence of an entity on or against which it may be exercised—the generation of asymmetry is the restriction and minimization of the enemy's effective power vis-à-vis oneself and the multiplication and maximization of one's own against that adversary.

Labeling only a certain segment of strategies as asymmetric risks obscuring the enormous real asymmetric advantages liberal democracies have over those insurgents who purportedly employ the asymmetric strategies. This practice threatens conceptually to detach asymmetric warfare from war and strategy by treating it as

something else, and in doing so it contributes toward preventing the Western powers from fully and effectively employing force against weaker challengers, as the popularity of asymmetry in strategic literature is a self-reinforcing symptom of our diluted grasp on strategy. Asymmetry will ever remain strategy, and strategy will ever remain asymmetry.

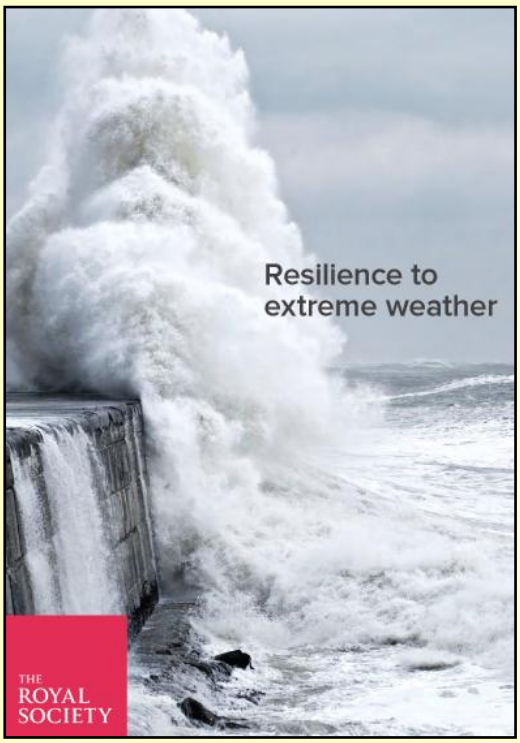
▶ **Notes are available at source's URL.**

Lukas Milevski *is a Ph.D. Candidate in the Graduate Institute of Political and International Studies at the University of Reading, United Kingdom.*

New report highlights "significant and increasing" risks from extreme weather

Source: http://www.homelandsecuritynewswire.com/dr20141201-new-report-highlights-significant-and-increasing-risks-from-extreme-weather

December 01 – **A comprehensive new report, published by the Royal Society, indicates that exposure of human populations to extreme weather is set to increase as global climate and population size, location, and age continue to change.** The report focuses on the risks to people from



floods, droughts, and heatwaves. These are some of the most frequent and damaging extreme events that currently occur and their impacts will change with the changing climate. The report also calls for changes to global financial accounting and regulation to ensure that extreme weather risk is made explicit. At present, these risks are not systematically factored into investors' valuations or assessed by creditors.

University of Exeter researchers have played an important role in creating a comprehensive new report indicating that the global risk from extreme weather is set to intensify.

The critical report, published by the Royal Society, indicates that exposure of human populations to extreme weather is set to increase as global climate and population size, location, and age continue to change. A University of Exeter release reports that a Working Group consisting of fifteen world-leading academics, including Exeter professors Peter Cox and Katrina Brown, were brought together to produce the influential report, published last Thursday, 27 November.

It presents new maps showing the combined impact of climate and demographic changes across the world on the exposure of people to extreme weather. The maps highlight those areas where there is the greatest increased risk of populations being vulnerable towards to end of the century.

The report focuses on the risks to people from floods, droughts, and heatwaves. These are some of the most frequent and damaging extreme events that currently occur and their impacts will change with the changing climate. It shows:

- Increasing numbers of people will live in areas that are exposed to extreme weather events exacerbate the risks from floods and droughts in many regions, but especially East, West, and Central Africa, India, and South-East Asia.

- The number of over-65 year olds is increasing; this is one of the groups most vulnerable to heatwaves. With current numbers, the number of heatwave exposure events this group experiences each year could increase from 0.1 billion today to almost one billion in 2100. If we do nothing to mitigate climate change, and population growth and distribution proceeds as expected, this number could rise to four billion.
- Changes in temperature and humidity could result in significant reductions in ability to work outdoors across much of Africa, Asia, and parts of North, South, and Central America. This could impact on rural communities and food production.

The report calls for action at all levels of government — international, national and local — to make society more resilient to extreme weather events. In 2015 important international agreements will be reached on disaster risk reduction, sustainable development and climate change. These agreements will be much more effective in addressing extreme weather and its impacts if they are linked with, and reinforce, each other.

Professor Peter Cox, from Exeter's Mathematics department said: "We are much more vulnerable to climate change than is normally assumed. For example, it is normal to think about global warming in terms of the global mean temperature increase, which is dominated by the large ocean area that warms much more slowly than the land. Unfortunately people live on the land, so they experience much more than the global average warming.

"This report has highlighted the need to make people and infrastructure much more resilient to climate change. The recommendations include more consideration of ecosystem-based approaches to protection, such as maintaining coastal wetlands or forests, and more explicit consideration of climate risks in company finances."

Professor Katrina Brown from the Environment and Sustainability Institute at the University of Exeter's Penryn Campus in Cornwall added: "Building resilience to climate change and extreme weather must start now. We need to anticipate and plan for events, rather than wait until after them. Our analysis shows that a combination of conventional engineering and ecosystem-based approaches, which harness and enhance the buffering capacity of natural landscapes, are likely to be most effective. Governments should work alongside communities and other groups to find the best ways to keep people safe now and in the future."

Between 1980 and 2004 the total cost of extreme-weather related events came to $1.4 trillion. Populations in countries with a low Human Development Index make up only 11 percent of those exposed to hazards but account for 53 percent of disaster mortality.

The report compares various practical options for the most effective and affordable defense against the impacts of flooding, drought and heatwaves.

The report concludes that engineered options, such as dams, sea walls, and wells are often the most effective at reducing the impact of a particular hazard, but that they are also expensive, and if they fail they fail cataclysmically. If used in combination with ecosystem-based approaches such as floodplain or mangrove re-establishment and planting vegetation they can be more effective and affordable as well as delivering wider benefits on an on-going basis — not just when the hazard strikes. These ecosystem or "natural" approaches are often more affordable and can have multiple additional benefits to society.

The working group therefore recommends that ecosystem-based approaches are increasingly used in combination with more traditional approaches, although more effort is needed to ensure they are systematically monitored and evaluated. The report uses the Slowing the Flow initiative in Pickering, U.K. as an example of where this is being done.

Professor Georgina Mace, chair of the working group for the report, said: "We are not resilient to the extremes of weather that we experience now and many people are already extremely vulnerable. If we continue on our current trajectory the problem is likely to get much worse as our climate and population change. By acting now, we can reduce the serious risks to our children and grandchildren.

"National governments have a responsibility to do everything in their ability to protect their people from the devastation caused by extreme weather events."

Speaking from the report launch event in Bangalore, India, Professor Paul Bates from the University of Bristol's Cabot

Institute, said: "For the first time this report makes clear that global society is not resilient to the extreme weather that we experience now, and that in the future, with population and climate change, we will be even more threatened."

Professor Bates, a member of the report working group, emphasizes the need for action: "Importantly the report makes a number of practical suggestions, such as encouraging businesses to report exposure to natural hazards in their annual accounts, that will start to address this situation."

The report also calls for changes to global financial accounting and regulation to ensure that extreme weather risk is made explicit. At present, these risks are not systematically factored into investors' valuations or assessed by creditors.

Business surveys, economic forecasts, and country briefings that guide investment decisions and credit ratings are typically based on the availability of skilled labor, access to export markets, political and economic stability, and financial incentives — but there is little or no consideration of actual or potential exposure to disaster risks.

Specifically, the Royal Society suggests that companies report the following:

- 1 in 100 (1 percent) risk per year — a stress test for a company's solvency that evaluates the maximum probable losses expected for events that occur, on average, once in a hundred years or have a 10 percent chance of occurring every decade
- 1 in 20 (5 percent) risk per year — a stress test for a company's annual earnings
- Annual Average Loss — a standardized metric for a company's exposure to extreme events

The full report and interactive versions of global maps showing the change in exposure to floods, droughts, and heatwaves between 2010 and 2090 is available on the Web site.

Also

Reducing the impact of extreme weather

Source: http://www.homelandsecuritynewswire.com/dr20141201-reducing-the-impact-of-extreme-weather

How do we reduce the impact of extreme weather today while preparing ourselves for future changes? What can we do to build our resilience?

A new report, Resilience to extreme weather, investigates these, and other, key questions to help inform important decisions about adaptation and risk reduction that are being made at global, national and local levels.

A Royal Society release reports that the Society has examined people's resilience to weather- and climate-related extreme events, in particular, floods, droughts, and heatwaves. The report looks at how improvements can be made to protect lives and livelihoods by comparing the options available and considering the fundamental building blocks for resilience.

In 2015, important international agreements will be reached on disaster risk reduction, sustainable development, and climate change. Our report will help those negotiating and implementing the new agreements to decide what action to take to most effectively build resilience.

The report's recommendations:

- Governments have a responsibility to develop and resource resilience strategies
- Governments should act together at the international level to build resilience; sharing expertise, co-ordinating policy and pooling resources to confront common risks
- To limit the need for costly disaster responses, more national and international funds will need to be directed to measures that build resilience to extreme weather
- The purpose, design and implementation of policy frameworks covering climate change, disaster risk reduction and development should be aligned and consistent regarding extreme weather
- Those who make and implement policies need to take practical measures to protect people and their assets from extreme weather.

- The risks posed by extreme weather need to be better accounted for in the wider financial system, in order to inform valuations and investment decisions and to incentivize organizations to reduce their exposure
- Information about extreme weather should be suitable for users' needs. Funders should encourage collaborations and ongoing dialogue between producers and users of knowledge
- Research to improve the understanding of risks from current weather and to model accurately future climate change impacts should be increased to provide relevant information for decision-makers, particularly at regional and local levels.

— Read more in Resilience to extreme weather (The Royal Society, 2014); explore the interactive defensive options chart; view detailed trend maps of the estimated effects of extreme weather by 2090

New York wants its own weather detection service

Source: http://www.homelandsecuritynewswire.com/dr20141201-new-york-wants-its-own-weather-detection-service

In the face of recent devastating snowfall in some regions, Governor Andrew Cuomo has announced that the state government will remain committed to its plans for the New York Advanced Weather Detective System, a state-run and focused weather service and alert system.

As the *Buffalo News* reports, lake effect snowfall blanketed much of Erie County with up seven or more feet of snow in a matter of seventy-two hours. Amidst this, the National Weather Service continually ramped up its storm warnings — much to the frustration of some in the area.

Many Erie County officials publicly claimed that the forecasts "failed to project the ferocity and exact locations of the tandem [storms]."

Erie County Executive Mark Polocarz added that "had county officials known there was any chance for 70 or more inches falling across parts of the county, its preparation would have been different."

"It is not that the National Weather Service failed us," Cuomo said, perhaps attempting to leverage a compromise, "It's that the National Weather Service has a certain number of weather stations and they get that information from those weather stations. And, they perform the best they can with the information they have."

The plans for the new state-run weather service began after Hurricane Irene and Tropical Storm Lee hit the state in 2011, followed by the very damaging Superstorm Sandy in 2012. Using roughly 100 weather stations across the state, the aim is for a more accurate picture of the region's weather patterns.

"So, when the wind starts to pick up, when the rain starts to fall,

you can detect it very early in the pattern's development and then you can track its trajectory of that weather pattern, which would obviously give you more data, would give you more information, which would be more reliable," said Cuomo.

The National Weather Service was surprised by the governor's comments and the frustrations of officials in Erie County.

"We were caught by surprise by those comments," said Christopher Vaccaro, a weather service spokesman, "This was a very well-forecasted event. We've been quite forthcoming and quite accurate in terms of what people in the Buffalo area could expect was coming."

The Buffalo branch of the National Weather Service declined to comment.

Regardless, while no timetable has been officially established state officials said that FEMA funding from the aftermath of Superstorm Sandy would pay for the new weather system, and that $15 million was approved in the state budget for 2014-15.

ISIS uses control of water as a tool of war

Source: http://www.homelandsecuritynewswire.com/dr20141212-isis-uses-control-of-water-as-a-tool-of-war

A segment of the Euphrates river after ISIS cut off supply // Source: annahar.com

Global security analysts have warned for some time now that water scarcity due to climate change will be used as a tool of war in regions with poor government. Abhishek Ramaswami, a researcher at New York University's Center for Global Affairs, writes that, in this sense – that is, the use of water and water scarcity as a tool of war — "the impact of climate change isn't going to be felt 20, 30, or 40 years from now. The impacts are being felt today and will only worsen as time goes on."

The on-going wars in Iraq and Syria provide the first examples of the strategic and tactical use of water as a tool of war, as militant groups operating in both countries have been using water against residents of areas they control. In May, Jabhat Al-Nasura cut off water to the Shiite-dominated city of Aleppo in an effort to weaken support there for the regime of Bashar al-Assad.

Ramaswami notes that "ISIS represents the first significant case of the results of climate change being used as a tool of terror." In the spring and summer, ISIS captured the Mosul Dam and the Fallujah Dam, but was repelled by Kurdish and coalition forces before being able to use the two dams for strategic purposes.

In July, the Islamic State (ISIS) tried to gain control of the Euphrates River by seizing the Haditha Dam, the second largest in Iraq. Had ISIS succeeded in doing so, the group could have inflicted a humanitarian disaster on Iraq's thirty-two million people who depend on the Euphrates for water.

ISIS leaders acknowledge that as long as they controlled regional dams and local water sources, seasonal droughts will force Shiite populations to move out of ISIS-controlled territories.

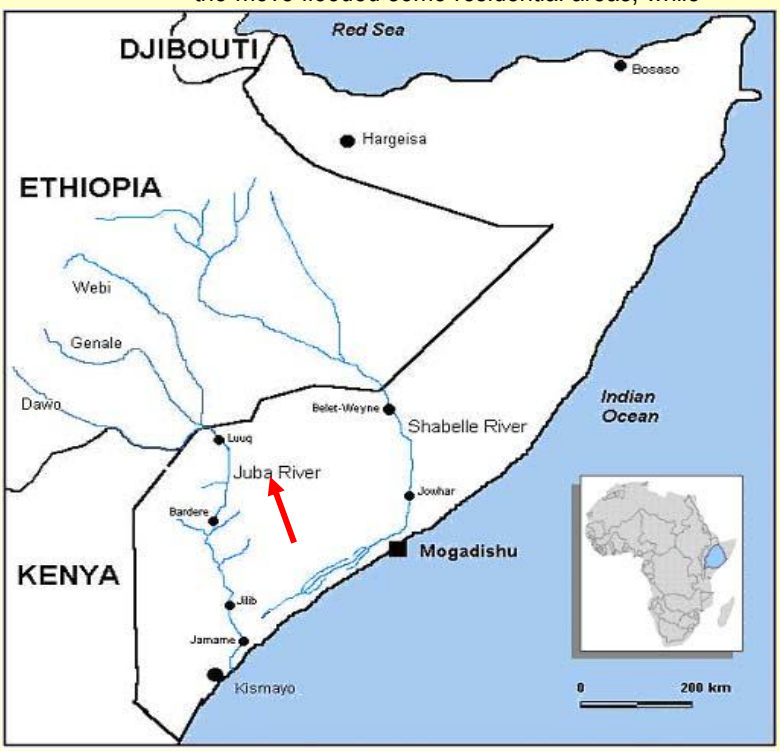
Shortly after ISIS captured Mosul, residents fled as soon as water and electricity were cut off, but many returned after the group reversed its actions in an attempt to gather support among the local population. The U.S. military helped Kurdish forces recapture the Mosul dam, the fourth largest in the Middle East. Had ISIS destroyed the dam, the resulting flood would have displaced and killed millions of Iraqis.

Ramaswami writes that ISIS "has acquired a significant portion of

their power in the region through a troubling phenomenon: water terrorism. ISIS has the power to influence the lives of millions of people through their strategic acquisition of control over water resources…. Unlike other terrorist groups, ISIS emphasizes the seizing of territory and important infrastructure, particularly those involving water and energy resources."

Other scholars agree. Control of regional water sources is critical to ISIS' vision for a Caliphate. "When it comes to creating an Islamic state, it is not just about the control of geographic areas in Syria and Iraq. In order to form a viable state, one must control the state's most vital infrastructure, which in Iraq's case is water and oil," said Matthew Machowski, a research fellow at Queen Mary University.

The Iraqi regime had no qualms about using control of scarce water for its purposes. Earlier this year, for example, Iraqi army soldiers in Anbar province took control of the Haditha Dam and flooded the areas where ISIS insurgents were present. *Al-Monitor* noted that the move flooded some residential areas, while



cutting off water to other areas of the province.

The use of the control of scarce water as a strategic tool in political disputes has been on the rise. With global warming causing Himalayan snow caps – the major source of water for the river systems which feed Pakistan, India, and Bangladesh — to form later and melt sooner, the three countries have been engaged in an escalating tensions over dwindling water resources (see "Former world leaders say global water crisis must be addressed," HSNW, 2 June 2011; "Pakistan charges India with 'water terrorism'," HSNW, 9 June 2011; and "Tensions simmer between India and Bangla Desh over dwindling water sources," HSNW, 26 October 2009).Regional terrorists have noticed: The leader of the Pakistan-based Islamist Lakshar-e-Taiba's Jamaat-ud-Dawah front recently threatened India with "water Jihad."

There are growing water-related tensions in north-east Africa, where Ethiopia is leading a group of countries which claim that colonial-era arrangements have given Egypt rights to a disproportional share of the Nile River water. To remedy the situation, Ethiopia has launched an ambitious project of building a massive dam – calledthe Renaissance Dam – on the Blue Nile River.At 6,000 MW, the dam will be the largest hydroelectric power plant in Africa when completed, as well as the eighth largest in the world.The reservoir at 63 billion cubic meters will be one of the continent's largest. Egypt vehemently opposes the dam construction, which it views as giving Ethiopia the ability to turn off the spigot at will, dooming Egypt and its population (see "Egypt adopts a conciliatory approach toward Ethiopia's massive Nile River dam," HSNW, 27 May 2014; "Egypt warns of disaster if Ethiopia completes Nile River dam," HSNW, 30 May 2013; and "Egypt asks Saudis to mediate in the intensifying Egypt-Ethiopia conflict over Nile River water," HSNW, 10 March 2014).

Somali-based al-Shabaab is also aware of the importance of water control. The group has seized control of multiple water sources in its fight against the Somali government. In 2011, the Somali government retook control of major cities and ports from al-Shabaab, but earlier this year, the terrorist group buried the main borehole that supplied the city of Garbaharey in water. "Al Shabaab has changed tactics and started to cut off liberated cities from their water source so that they can demonstrate some kind of power and presence," says Abdilatif Muse Noor, a member of the Somali parliament. Access to the closest water source, the **Juba River**, is controlled by al-Shabaab, and the group has banned residents in government-controled areas from fetching

water in al-Shabaab controlled areas. Today, a significant number of residents in Somali-government controlled areas rely on humanitarian air drops for water.
Ramaswami says al-Shabaab's tactic of cutting water to specific populations as a lesson from the ISIS playbook. "ISIS has established a blueprint that can be used by other entities to take advantage of drought and water scarcity — especially in nations with poor governance — a common theme throughout the developing world," he writes, and concludes: "For all the conversation about ISIS taking control of oil refineries, one could argue that their control of water is even more significant, as it deprives the population of a resource necessary for daily sustenance and gives the militant group significant leverage over local governments and populations."

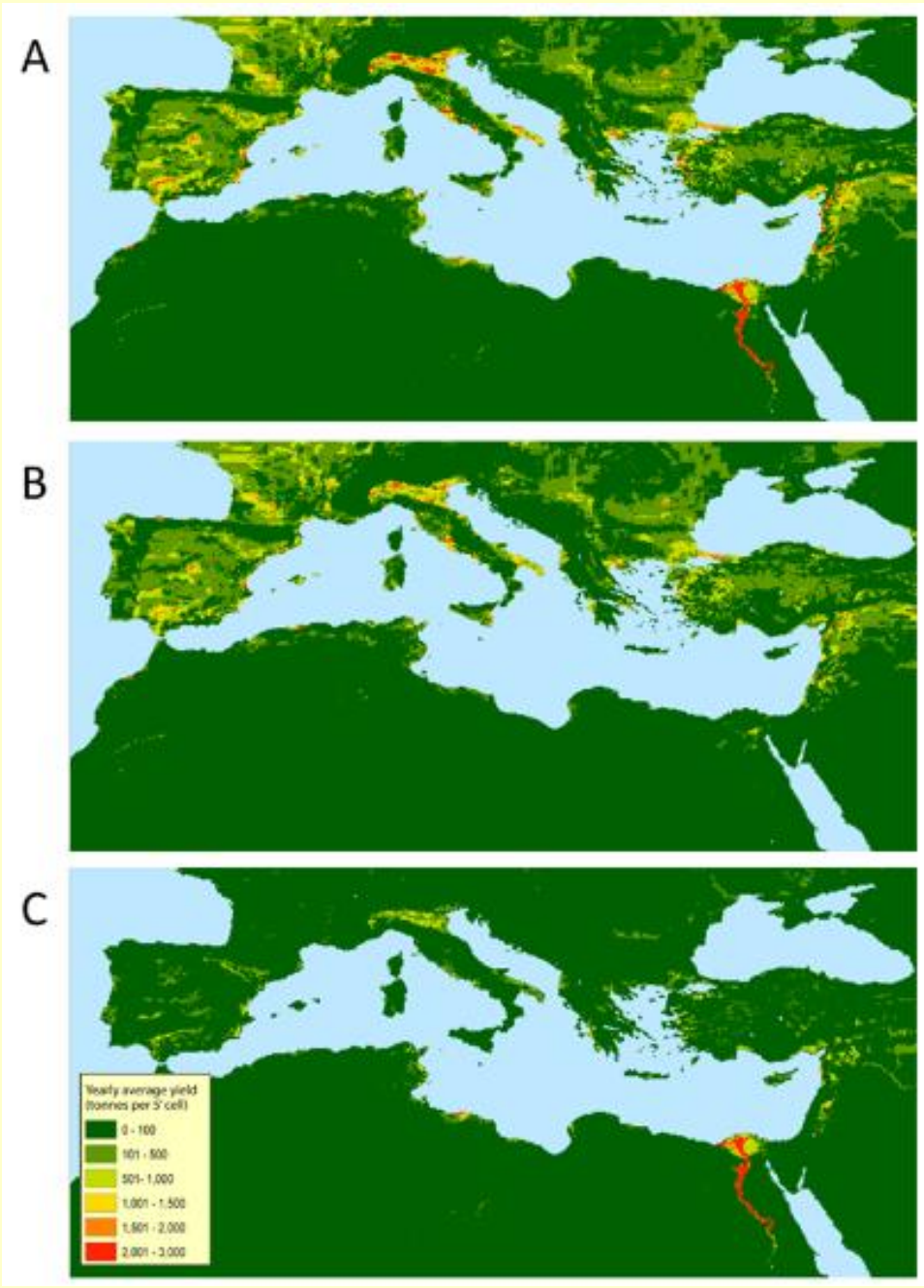
Water's role in the rise and fall of the Roman Empire

Source: http://www.homelandsecuritynewswire.com/dr20141212-water-s-role-in-the-rise-and-fall-of-the-roman-empire

The Roman Empire, stretching over three continents and persisting for many centuries, was home to an estimated seventy million people. In such a vast area ensuring a stable food supply was no easy task, particularly given the variable and arid climate of the Mediterranean region. Smart agricultural practices and an extensive grain-trade network enabled the Romans to thrive in the water-limited environment of the Mediterranean, a new study shows. The stable food supply brought about by these measures, however, promoted population growth and urbanization, pushing the Empire closer to the limits of its food resources.
Smart agricultural practices and an extensive grain-trade network enabled the Romans to thrive in the water-limited environment of the Mediterranean, a new study shows. The stable food supply brought about by these measures, however, promoted population growth and urbanization, pushing the Empire closer to the limits of its food resources. The research, by an international team of hydrologists and Roman historians, is published today in *Hydrology and Earth System Sciences*, an open access journal of the European Geosciences Union (EGU).
An EGU release reports that the Roman Empire, stretching over three continents and persisting for many centuries, was home to an estimated seventy million people. In such a vast area ensuring a stable food supply was no easy task, particularly given the variable and arid climate of the Mediterranean region. So how did the Romans maintain reliable food supplies to their cities for centuries under such challenging conditions?

To find out, Brian Dermody, an environmental scientist from Utrecht University, teamed up with hydrologists from the Netherlands and classicists at Stanford University. The researchers wanted to know how the way Romans managed water for agriculture and traded crops contributed to the longevity of their civilization. They were also curious to find out if these practices played a role in the eventual fall of the Empire.
"We can learn much from investigating how past societies dealt with changes in their environment," says Dermody. He draws parallels between the Roman civilization and our own. "For example, the Romans were confronted with managing their water resources in the face of population growth and urbanization. To ensure the continued growth and stability of their civilization, they had to guarantee a stable food supply to their cities, many located in water-poor regions."
In the *Hydrology and Earth System Sciences* paper, the team focused on determining the water resources required to grow grain, the staple crop of the Roman civilization, and how these resources were distributed within the Empire. It takes between 1,000 and 2,000 liters of water to grow one kilo of grain. As Romans traded this crop, they also traded the water needed to produce it — they exchanged virtual water.
The researchers created a virtual water network of the Roman world. "We simulated virtual water trade based on virtual-water-poor regions (urban centers, such as Rome) demanding grain from the nearest virtual-water-rich region (agricultural regions, such as the

Nile basin) in the network," explains Dermody.



The team used a hydrological model to calculate grain yields, which vary depending on factors such as climate and soil type. The authors used reconstructed maps of the Roman landscape and population to estimate where agricultural production and food demand were greatest. They also simulated the trade in grain based on an interactive reconstruction of the Roman transport network, which takes into account the cost of transport depending on factors such as distance and means of transportation.

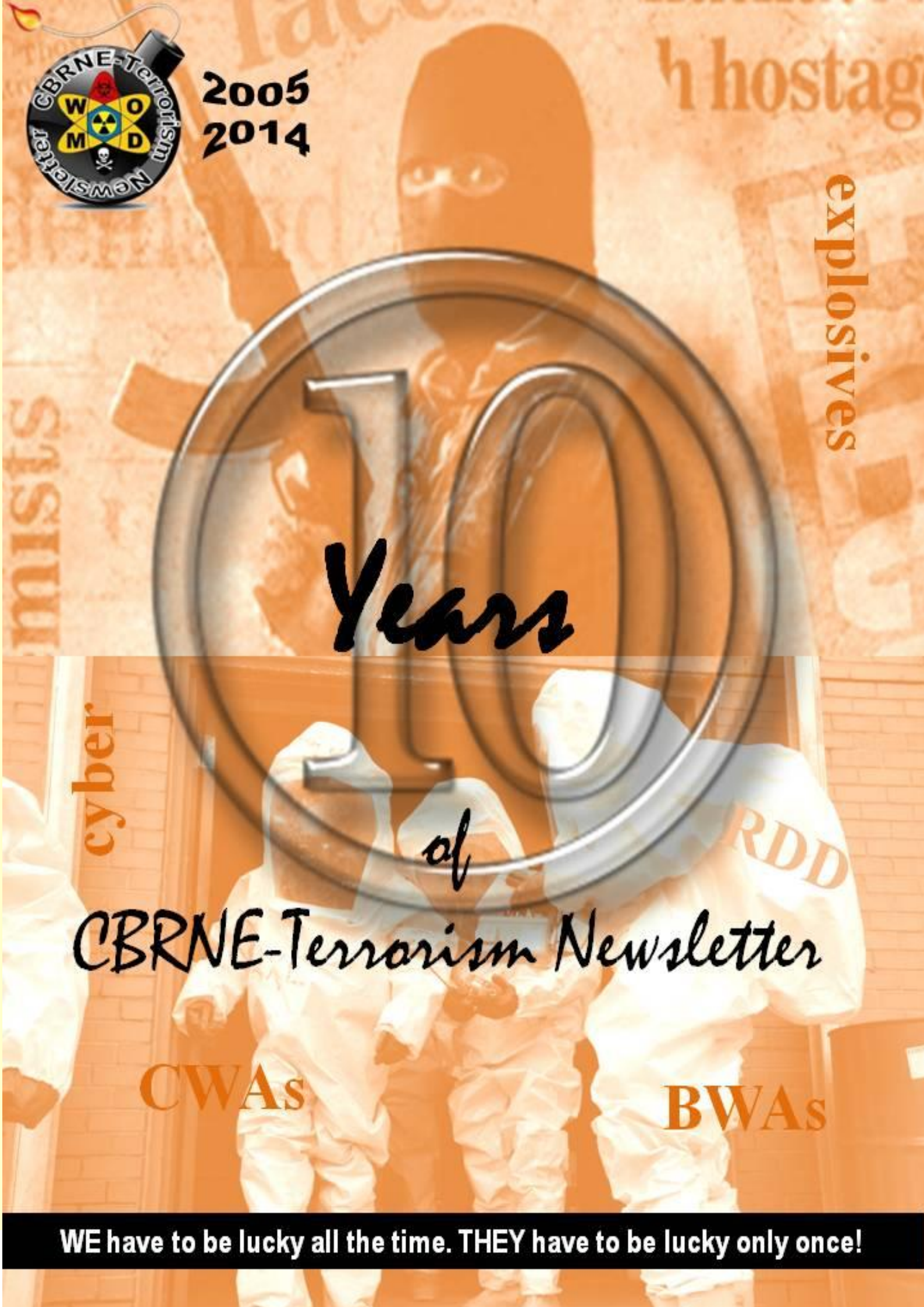
Their virtual water network indicates that the Romans' ability to link the different environments of the Mediterranean through trade allowed their civilization to thrive. "If grain yields were low in a certain region, they could import grain from a different part of the Mediterranean that experienced a surplus. That made them highly resilient to short-term climate variability," says Dermody.

(a) Average cereal yield in tonnes per 5' cell, calculated in PCR-GLOBWB and based on 52 years of climate forcing. The yields from rainfed (b) and irrigated (c) agriculture are shown separately

The Romans' innovative water-management practices, however, may also have contributed to their downfall. With trade and irrigation ensuring a stable food supply to cities, populations grew and urbanization intensified. With more mouths to feed in urban centers, the Romans became even more dependent on trade whilst at the same time the Empire was pushed closer to the limits of their easily accessible food resources. In the long term, these factors eroded their resilience to poor grain yields arising from climate variability.

"We're confronted with a very similar scenario today. Virtual water trade has enabled rapid population growth and urbanization since the beginning of the industrial revolution. However, as we move closer to the limits of the planet's resources, our vulnerability to poor yields arising from climate change increases," concludes Dermody.

— Read more in B. J. Dermody et al., "A virtual water network of the Roman world," Hydrology and Earth System Science *18 (2014): 5025-40*
▶ http://www.hydrol-earth-syst-sci.net/18/5025/2014/hess-18-5025-2014.pdf


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