Dedicated to Global First Responders

CBRNE NEWSLETTERRORISM

May 2017

www.cbne-terrorism-newsletter.com

North Korean Youth League says 5 million youngsters are "combat ready" and will "annihilate" US with nuclear bombs

Source: http://www.mirror.co.uk/news/world-news/north-korean-youth-league-says-10300504

Apr 27 – **North Korea's Youth League has vowed to use 5million children "equipped with nuclear bombs" to "mercilessly wipe out" the USA.**

A terrifying statement from the communist country's Kimilsungist-Kimjongilist Youth League says its members will "wipe out the enemies" with "invincible nuclear force".

The organisation also vows to "annihilate all aggressors and provokers on the Earth and display fireworks of the final victory".

The Youth League dates back to 1946 when it was founded by Kim Il-Sung, North Korea's supreme leader and grandfather of present-day leader Kim Jong-un.

Kim Jong-un remains chairman of the Youth League and the organisation is tasked with encouraging children over 15 into production, construction and military service.

The Youth League said it is "the will of the Korean youths to resolutely and mercilessly wipe out the US imperialists and south Korean puppet warmongers".

The statement added: "Upon hearing the news that the US imperialists and south Korean puppet group of traitors are making desperate efforts to hurt the dignity of the DPRK (Democratic People's Republic of Korea, the official name for North Korea) and bring down its socialist system while openly talking about 'preemptive attack', 5million youth vanguard of the DPRK are hardening their will to wipe out the enemies with the surging rages at them.

"The large contingents of young people are now waiting for the final order of the headquarters of the revolution, keeping themselves fully combat-ready to mercilessly wipe out with 5million nuclear bombs.

"The US imperialists should know that the Earth will break if invincible nuclear force and the 5million large contingents of young people equipped with nuclear bombs vent their wrath.

"The world will clearly witness how the Paektusan large contingents of young people will annihilate all aggressors and provokers on the earth and display fireworks of the final victory."

The aggressive message from the Youth League comes as tensions rise between North Korea, South Korea, the US and China.

Kim Jong-un's troops yesterday launched hundreds of ballistic weapons to mark the 85th anniversary of the Korean People's Army on Tuesday - and the USA tested a new anti-missile system in South Korea.

It comes amid growing fears about the country's nuclear weapons programme.

Meanwhile, the US Navy's USS Carl Vinson aircraft carrier is reportedly leading an armada of Western warships to carry out military drills off the Korean peninsula.

Kim Jong-un's regime has threatened the US with all-out war while Donald Trump has vowed to "solve" the North Korea problem.

The US has begun installing its Terminal High Altitude Area Defence (THAAD) anti-missile system in South Korea.

America permanently has 38,0000 sailors, marines, soldiers and air-force staff based in South Korea to guard against a North Korea threat.

North and South Korea split after a brutal three-year war in the 1950s, which has never officially ended despite a flimsy peace understanding.

EDITOR'S COMMENT: Scary at first but difficult to implement away from the peninsula area, this new threat is the result of a wird combination: a paranoic leader; a brain washed isolated society and possession of nuclear weapons, all that add realism in any threat announced.

North Korea's army has 'fake weapons', expert says

Source: http://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=11846384

Apr 27 – A military expert says that some of North Korea's military weapons it has put on display are fake, as North Korea's Youth League vowed to use five million children "equipped with nuclear bombs" to "mercilessly wipe out" the USA.

Michael Pregent, a former US Army Intelligence Officer, told Fox News that some of the missiles held by soldiers during Pyongyang's April 15 military parade. 'This was more about sending a message than being combat effective," he said.

Pregent, who is now an adjunct fellow at the Hudson Institute in Washington, DC, looked at several photos of North Korean soldiers from the April 15 parade to make his assessment.

Special operations "commandos" were seen to be carrying what appeared to be AK-47's with grenade-launching capabilities.

But Pregent said what many people believed to be grenade launchers are known as "helical" magazines. This is a piece of equipment that organises rounds in a spiral shape to maximise capacity. It is notorious for jamming.

He said these magazines have a high-failure rate, and he wonders whether any of the rifles were actually loaded, as ammunition manufacturing is a serious issue for the country.

Pregent also claims that the type of sunglasses being worn by the North Korean troops "looks like a flat-face frame, and that's not ballistic. That would wraparound and would also protect your eyes".

Pregent also added that the fingerless gloves worn by some of those soldiers are more for show. "Some of our guys do have them, but most guys go all the way with full gloves based on the heat of the barrel from a round, not to mention they're fire resistant if you need to pick up something," he told Fox News.

He also said that the oversized projectiles added to the end of some of those soldiers' rifles were "laughable."
"If you look, you can see the plastic is over the muzzle," Pregent said.
Despite this, Pregent said that some of the weapons still could be real, but the projectiles themselves would have to be fake "because Kim Jong Un doesn't want them to launch one at the viewing stand".
Pregent also told Fox News the silver-plated rifles held by some of the soldiers also seemed unrealistic.
"Saddam had gold plated handguns, and even he wouldn't give them to his troops, so these are most likely painted," Pregent said.
His claims come as the youth wing of Kim Jong-un's government has vowed to "annihilate all aggressors and provokers on the Earth".
North Korea's Youth League vowed to use five million children "equipped with nuclear bombs" to "mercilessly wipe out" the US.
A statement from the League says its members will "wipe out the enemies" with "invincible nuclear force".
The organisation also vows to "display fireworks of the final victory".
The Youth League dates back to 1946 when it was founded by Kim Il-Sung, North Korea's supreme leader and grandfather of present-day leader Kim Jong-un.
Kim Jong-un remains chairman of the Youth League and the organisation is tasked with encouraging children over 15 into production, construction and military service.

EDITOR'S COMMENT: Fake or not, it is a good idea especially for countries neighboring with aggressive neighbors. And you do not have to introduce new weapons – just multiply existing ones and let spy satelites do the rest. It is a different approach if you have to deal with 10 MLRSs compared to 50 systems strategically located.

NK, currently with 13-30 nukes, is expanding its arsenal by 3-5 weapons per year

Source: http://www.homelandsecuritynewswire.com/dr20170501-nk-currently-with-1330-nukes-is-expanding-its-arsenal-by-35-weapons-per-year

May 01 – David Albright of the Washington, D.C.-based Institute for Science and International Security offers a detailed summary of North Korea's nuclear weapons capabilities and potential. He says that one way to summarize the estimates of plutonium, weapon-grade uranium (WGU), and nuclear weapons is to use ranges of the medians of each case considered. **They are as of the end of 2016:**

- 33 kilograms of separated plutonium (median value of a distribution).
- 175-645 kilograms of weapon-grade uranium, where 175 kilograms corresponds to a median estimate for the case of one centrifuge plant and 645 kilograms corresponds to the median estimate for the case of two centrifuge plants.
- 13 to 30 nuclear weapons, where these values reflect the utilization of 70 percent of the available, estimated stocks of plutonium and weapon-grade uranium. The limits correspond to the median values for the cases of one or two centrifuge plants and each weapon contains either plutonium or weapon-grade uranium.
- Based on this cumulative estimate, North Korea is currently expanding its nuclear weapons at a rate of about 3-5 weapons per year.
- Thirty percent of North Korea's total stocks of plutonium and weapon-grade uranium are assessed as in production pipelines, lost during processing, or held in a reserve.

North Korea keeps secret the number of nuclear weapons that it has built, and there is little, if any, reliable public information about this value. The above range of 13-30 nuclear weapons as of the end of 2016, based on the estimates of North Korea's production and use of plutonium and WGU, is an assessment.
North Korea may have a handful of plutonium-based warheads for its Nodong ballistic missile.

One uncertainty is judging North Korea's dependence on plutonium for its deployed nuclear weapons. It would have incentives to be able to build miniaturized, reliable weapons with only a weapon-grade uranium core, as its declaration after the September 2016 test could suggest it has done.
North Korea would have an incentive to build more advanced nuclear weapons. One type is a composite core nuclear weapon made from both plutonium and weapon-grade uranium. How many it may have built is unknown, as is their size, weight, and reliability. North Korea has enough plutonium for up to 12 nuclear weapons using a composite core of plutonium and weapon-grade uranium, where likewise 70 percent of the fissile material is utilized in the weapons themselves. However, North Korea is unlikely to build only composite core weapons. This estimate would suggest that North Korea could build several of them in addition to other types of nuclear weapons as well.
It is unknown if North Korea could mount a warhead on a Nodong that uses only weapon-grade uranium or has a composite core. In particular, are they too large for the Nodong? However, both possibilities appear increasingly likely.
It is uncertain, and there are reasons to doubt, that North Korea can yet build reliable, survivable warheads for ICBMs.
Continued underground testing will provide North Korea opportunities to improve significantly its weapons in terms of less fissile material (particularly plutonium) per weapon, increased warhead miniaturization, and/or greater explosive yields.
Developing thermonuclear weapons, which can achieve all three above goals, is a declared priority of North Korea.
It appears capable of developing thermonuclear weapons. It is far more likely to be working on one-stage thermonuclear weapons rather than traditional two stage thermonuclear weapons, or "H-Bombs."
The Institute does not assess North Korea as yet capable of building two stage thermonuclear weapons or utilizing gaseous mixtures of deuterium and tritium in a U.S-style boosted fission weapon. However, North Korea is assessed as able to handle solid forms of lithium-6, deuterium, and/or tritium, such as those used in one-stage thermonuclear weapons or other types of boosted fission weapons.
Its existing knowledge should allow it to continue to make progress on a variety of deliverable nuclear weapons, even in the absence of additional underground nuclear tests.

Through 2020
Albright says that through 2020, North Korea is projected to have 25-50 (rounded) nuclear weapons.
A worst case, involving the operation of the Experimental Light Water Reactor (ELWR) at Yongbyon, is that it would have up to 60 nuclear weapons by the end of 2020.
In regards to composite core nuclear weapons, it would have enough plutonium for up to 17-32 nuclear weapons, where the above worst case including the ELWR determines the upper bound.
Significantly higher estimates are possible, such as one that is in an earlier 2015 Institute study on North Korean nuclear explosive materials, if North Korea significantly expands its gas centrifuge program and dramatically boosts its production and separation of plutonium over what is assumed in the current analysis.

— Read more in David Albright, North Korea's Nuclear Capabilities: A Fresh Look (Institute for Science and International Security, 28 April 2017).

Several States on Alert After Dangerous Nuclear Material Stolen in Mexico

Source: https://sputniknews.com/latam/201704251052995691-mexican-states-warned-substance-stolen/

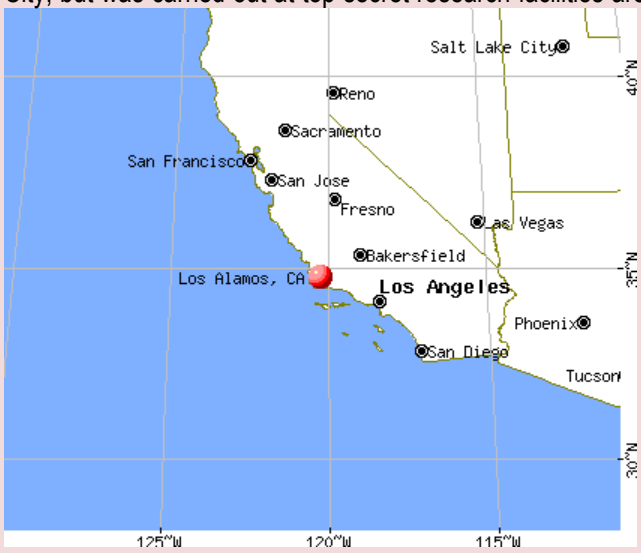
Apr 24 – Mexico's Interior Ministry put nine states on alert Monday when it was discovered that an unknown amount of iridium, a dangerous nuclear substance that's used inside medical equipment, had been stolen in Tlaquepaque, Jalisco state.
Reportedly taken from the back of a white Nissan pickup truck on Sunday, the material was inside of **industrial X-ray equipment**, and the ministry released a statement saying, "This was industrial equipment that included

Iridium-192... which can be dangerous for people if it is taken out of its container."
"This source could cause permanent injuries to the person who handles it or who has been in contact with it for a brief time (minutes or hours) … Being close to this quantity of unprotected radioactive material for hours or days could be fatal," the statement added, according to the Telegraph.
A warning was issued for the states of Zacatecas, Jalisco, Nayarit, Durango Guanajuato, Aguascalientes, Michoacán, San Luis Potosi, and Colima. The theft was reported by Tecnología No Destructiva, SA de CV, the company that handles the equipment.
Nuclear material theft has occurred at least seven times in Mexico since 2013. A truck full of highly radioactive cobalt-60 was stolen in December 2013 by thieves who weren't aware of the vehicle's contents.
After the substance was found several suspects were arrested and hospitalized.
National Nuclear Safety and Safeguards Commission Director Juan Eibenschutz told the Milenio television network at the time that it was "absolutely certain that whoever removed this material by hand is either already dead or about to die … It would probably be fatal to be close to this amount of unshielded radioactive material for a period in the range of a few minutes to an hour," according to RT.
Authorities are telling people to contact local law enforcement if they locate the material, and to stay at least 30 yards away from the substance. Exposure to iridium can can be injurious, but if the left in the container it poses no danger.
Luis Felipe Puente, National Coordinator of the Interior Ministry, tweeted that if people encounter the container, "don't open it."

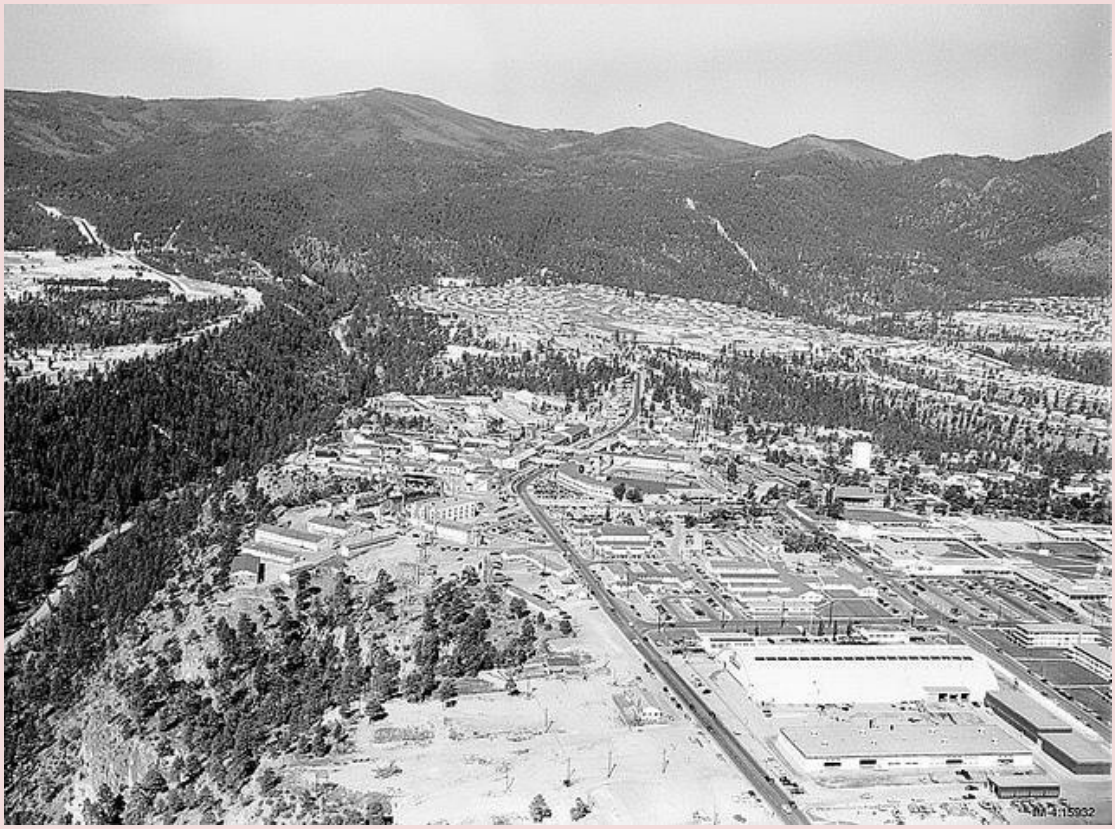
The Totally Normal Town Where Everyone Worked on Weapons of Mass Destruction

By Daniel Oberhaus
Source: https://motherboard.vice.com/en_us/article/the-totally-normal-town-where-everyone-worked-on-weapons-of-mass-destruction

May 13 – In the early 1940s, the United States made its nuclear weapons program a priority with the establishment of the Manhattan Project, a top secret research initiative that would eventually yield the world's first atomic bomb. Despite its moniker, the Manhattan Project wasn't undertaken in New York City, but was carried out at top secret research facilities around the United States. The most famous of these was Los Alamos National Laboratory (nee Los Alamos Scientific Laboratory), a compound tucked away in the Jemez Mountains of northern New Mexico, where Robert Oppenheimer and his handpicked team of top physicists worked in utter secrecy and isolation to develop the most powerful weapon in history.



But as a recently released 1954 memo drafted for PR purposes wants you to know, there's more to Los Alamos than its top secret atomic weapons program. Like the Jeb Bush of travel brochures, this document wants you to know that Los Alamos is completely "normal" and to please stop pretending like it's not. Please.
The site of Los Alamos was recommended by Oppenheimer, in part because it was close to his own New Mexico ranch and also for its isolation. So the US government took over a local school to use as its laboratory and set to work developing a bomb…and a community.



As detailed in the report, "it was considered essential in 1942 to establish a nuclear weapons laboratory [at Los Alamos], and it was of course considered equally essential to provide living quarters and mess halls for the crew and to maintain and supply the project." The US government intended to demolish the lab after the war, so all facilities were considered temporary and generally made from cheap wood. At most, the government reckoned it'd only have to account for 150 scientists, military personnel and their families during Los Alamos' existence, but by the end of its first operational year there were more than 1,500 people inhabiting this shanty town. By the end of the war, Los Alamos boasted a population of over 8,000.

Fortunately for the new emigres to scenic Los Alamos (and unfortunately for the rest of the world), the US government decided it really liked to make nuclear weapons. So rather than tear down the Los Alamos facilities after the war, it began to develop a full-blown community around the lab, replete with "houses, schools, stores, utilities, warehouses" and churches representing 14 different denominations.

Based on the report, it was a rough start for Los Alamos National Laboratory and its community. "At the end of the war, various utility systems, marginal at best, failed completely during the winter, adding to the bleakness of existence in the mud-street and duckboard reservation," the anonymous author of the report notes. But hey, the nearest railhead was only 35-miles away, so if the denizens of Los Alamos closed their eyes and squinted, they could almost imagine they were still connected to civilization.

By the time the report was written in 1953, Los Alamos had just become self-sufficient. For the first time ever, the township managed to generate more revenue than it cost the government to prop up through the Zia Company, which was responsible for all public utilities in the town. In fact, Los Alamos could almost pass as a normal town.

It had multiple barber shops, movie theatres, and jewelers, a photography store, pastry shop and even a florist. There was a police force and fire department, albeit one directly subsidized by the federal Atomic Energy Council that also had to be trained in special firefighting techniques involving radioactive materials. There was a daily flight from Los Alamos to Albuquerque, a library stocked with over 18,000 titles, and living space aplenty, with the smallest one-bedroom apartments going for $22 a month and rents for the largest units capped at $135. Residents of Los Alamos could even listen to the radio, a luxury that wasn't afforded them during wartime. Their local station, KRSN was presided over by a certain Robert Porton, whose "large record collection is the envy of many a disc jockey."

Sure, most of 12,000 citizens were working on developing weapons of mass destruction or the family members of someone who was, but other than that, Los Alamos was a paragon of idyllic 50s American life.

"First-time visitors to Los Alamos often come with a preconceived notion that the will find something awesome and abnormal about the Los Alamos community," the report reads. "They leave, however, with the feeling of having visited an interesting but a perfectly 'normal' American community."

In the 60 years since this report was written, it seems as though little has changed in the town of Los Alamos, New Mexico. The population still hovers around 12,000, the Los Alamos National Laboratory is still in the business of "national security science," and kitschy stores and restaurants with names like Atomic City Quilts or Atomic Eyecare abound.

That's right, it's business as usual in Los Alamos: the totally "normal" town where absolutely nothing strange is going on whatsoever.

Pocket-size biological solution to radioactive threats

Source: http://www.homelandsecuritynewswire.com/dr20170515-pocketsize-biological-solution-to-radioactive-threats

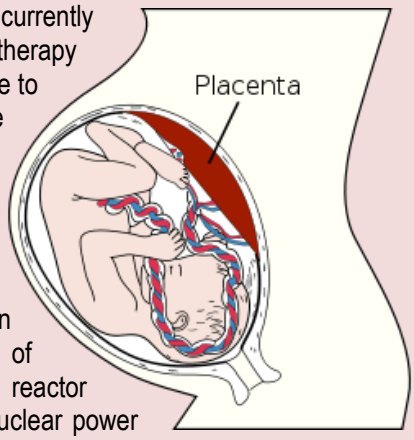
May 15 – Yaky Yanay, co-CEO, **Pluristem Therapeutics**, last week surprised the participants The Jerusalem Post Annual Conferencein New York by saying that a small glass vial he pulled out of his pocket offered a solution to Iran's nuclear threats.

"I have the solution in my pocket," Yanay said.

The controversial nuclear deal with Iran, and the stream of threats from North Korea, have kept the topic of nuclear weapons in the headlines.

The *Jerusalem Post* notes that currently, there is no point-of-care testing to measure the degree of exposure to acute radiation. **First responders do not have detection kits to assess the level of radiation in a patient, and would not be able to separate those affected by radiation poisoning from those who were spared.** Medical personnel must thus provide everyone with anti-radiation therapy, regardless of exposure.

Haifa-based Pluristem Therapeutics has developed an anti-radiation therapy that can be stockpiled for emergencies. **The therapy harnesses the power of the human placenta to contain the cascading effect of radiation exposure in the body and allow for the natural healing of cells.**



The U.S. government is currently evaluating Pluristem's cell-therapy product as a potential candidate to stockpile as a countermeasure (see "U.S. testing radiation therapy developed in Israel," HSNW, 23 February 2016).

Animal trials suggest that the cells could rescue the large majority of a population exposed to high doses of radiation which could follow a reactor meltdown or an attack on a nuclear power plant. Results from a (NHP) pilot study for PLX-R18 showed improved survival compared to cohorts that received placebo. **The two lower dosages, 4 and 10 million cells per kilogram body weight, resulted in an 85 percent survival rate in irradiated NHPs compared to a 50 percent survival rate in the placebo treated control group.** The pilot study also demonstrated a trend toward enhanced neutrophil and lymphocyte recovery.

These data will inform an important study aiming to meet the requirements for a Biologics License Application (BLA) submission under the FDA's Animal Rule regulatory pathway.

The *Post* notes that Pluristem is one of a small number of biotech firms working in this space, including NeoStem,whose core business is the collection and storage

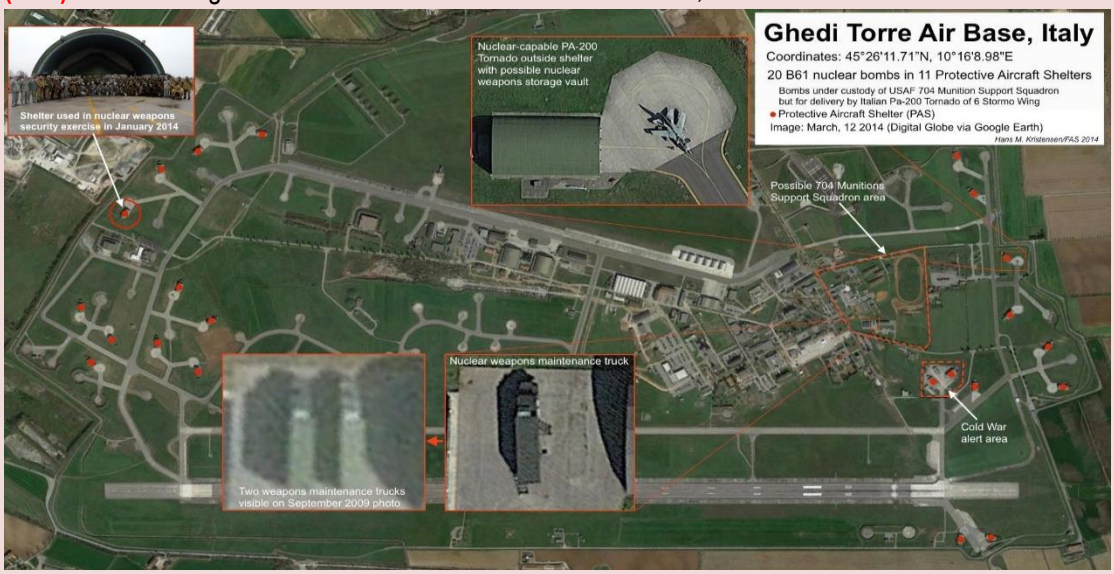
of stem cells for those who want such an insurance plan; or Osirus Therapeutics' Prochymal, currently in FDA Phase III clinical trials for two diseases with clinical manifestations like acute radiation syndrome (ARS); and Cleveland Biolabs, whose Protectan compounds reportedly rescues mammals from lethal doses of radiation by suppressing apoptotic cell death in critical hematopoietic (HP) and/or gastrointestinal (GI) tract cells.

US Stores Dozens of Weapons of Mass Destruction in This Non-Nuclear Country

Source: https://sputniknews.com/military/201705161053657854-us-italy-nuclear-weapons/

May 16 – Although Italians have been opposed to Washington's military presence in the country due to major risks that it poses, Rome is unlikely to deal with this issue journalist Fabrizio Di Ernesto told Sputnik Italia.

"**Few people know that Italy stores US nuclear warheads at the Aviano and Ghedi bases despite the fact that the country signed the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). The** Italian government has not confirmed this. However, former US President Bill Clinton said



this in a 2005 interview. The news did not cause a stir. There are approximately 70 nuclear bombs in Italy, a country which voted against nuclear energy at a referendum," the journalist said.

The NPT strives to prevent the spread of nuclear weapons and weapons technology, to promote the peaceful use of nuclear energy and contribute to nuclear disarmament. The treaty has been in force since March 1970.

Italy has stored US nuclear weapons on its territory as part of NATO's nuclear-sharing arrangement, which has seen Washington station its B61 nuclear bombs in non-nuclear countries. **Aviano, a NATO base in the Italian region of Friuli-Venezia Giulia, is home to some 50 B61 bombs, while Ghedi, a base of the Italian Air Force in the region of Lombardy, is estimated to host between 20-40 B61 bombs.**

In addition, US tactical nuclear weapons are stored in Belgium, Germany, the Netherlands and Turkey.

The B61, one of the Pentagon's primary thermonuclear weapons, is in the process of a major upgrade, with its latest version, known as the B61-12, successfully tested in April.

The US military presence in Italy poses other risks to the Mediterranean country.

"The US Navy's Mobile User Objective System (MUOS) was built in the commune of Niscemi, Sicily. It is a communications satellite system which functions thanks to five satellites and four antennas, located in Niscemi, Australia, Virginia and Hawaii. This complex helps all NATO armies to communicate. Since there are only four antennas, one can imagine how powerful they are to be able to transmit and receive signals. Numerous universities have warned that radio waves could cause cancer. Nevertheless, the project was carried out," the journalist said.

Di Ernesto expressed doubt that Italian politicians would force the United States to withdraw its troops, weapons and military installations from the country.

"Sadly, our politicians are fully dependent on Washington," he said. "I don't think that Italian politicians could oppose these bases, taking into account that they are mostly financed by the United States. One could say that the funds that Italy allocates on these bases come from NATO. Some politicians even urge to increase this spending since the more you give to these international organizations, the more you can count on their assistance. This is why no one wants to change anything."

Portable nuclear gauge device lost while in transport between Toronto and Brampton, ON

Source: http://nuclearsafety.gc.ca/eng/acts-and-regulations/event-reports-for-major-nuclear-facilities/event-reporting/transport-intransit-events.cfm

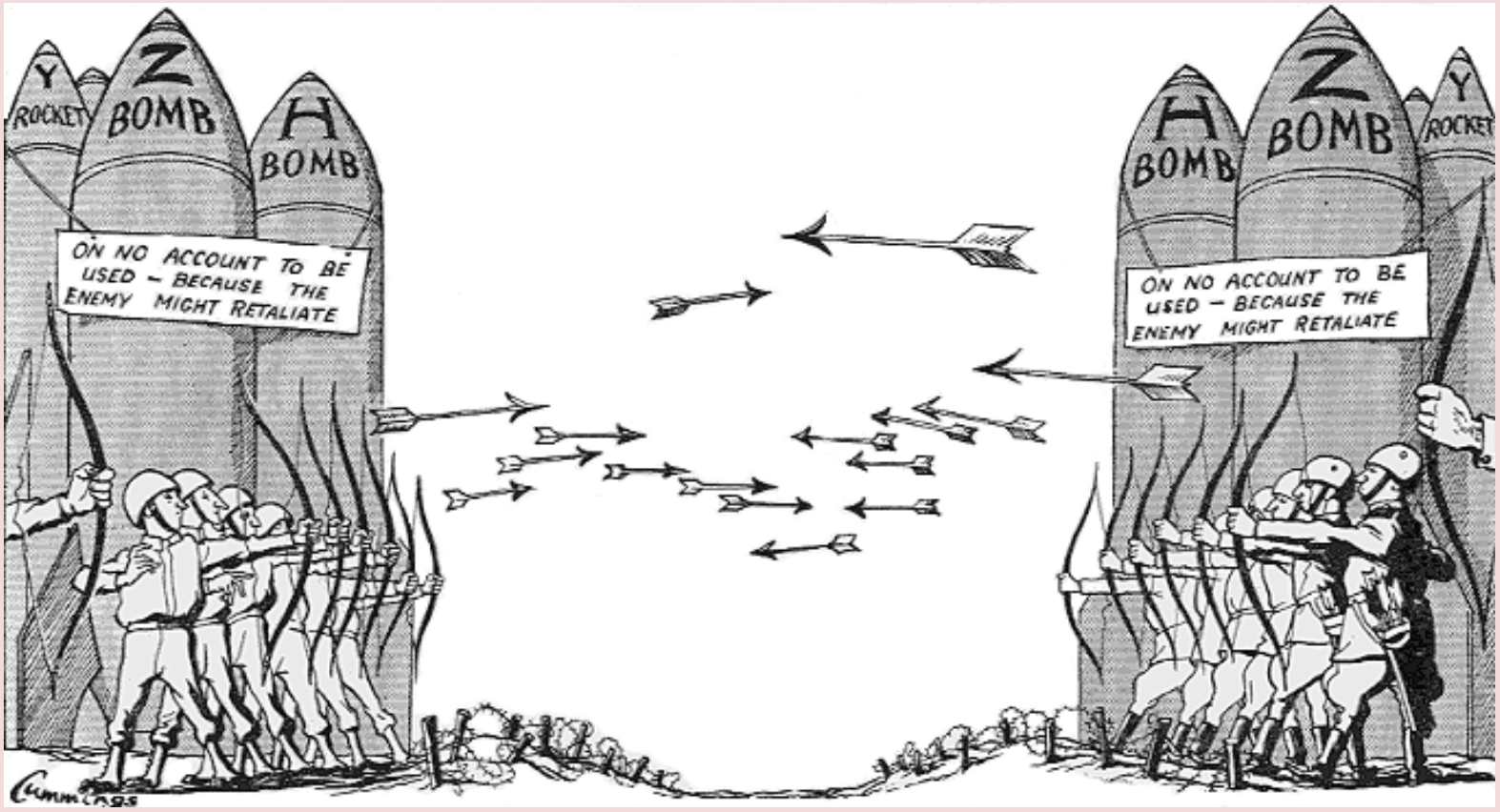
Engtec Consulting Inc. reported to the Canadian Nuclear Safety Commission (CNSC) that it had lost a **Troxler Model 3440 portable nuclear gauge** on the morning of Wednesday, **May 17, 2017**, while it was in transport between Toronto and Brampton, ON.

The device was transported in a yellow box, classified as a Type A package, 81 cm (32") length X 43 cm (17") wide X 46 cm (18") high. The portable gauge is about the size of a shoebox, with

an electronic keypad and a metal handle extending from the top. It contains two radioactive sealed sources: one of cesium-137 and one of americium-241/beryllium.

Radiation device description:
Troxler
Model No. 3440
Serial No. 19621
Cs-137 – 326 MBq (Sealed Source Serial number 50-9346)
Am-241/Be – 1,628 MBq (Sealed Source Serial number 47-15167)

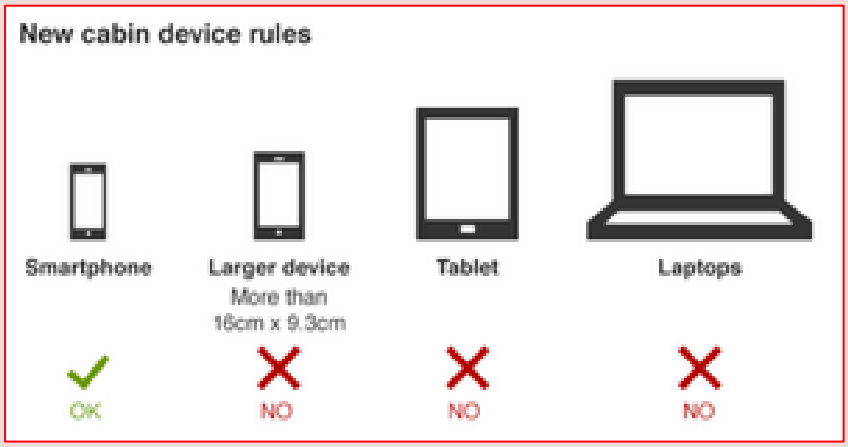
The portable gauge does not pose a hazard as long as it is not tampered with or damaged. If the gauge is found, refrain from moving the gauge and contact the Toronto Police Department at 416-808-2222.



U.S. considering extending electronic-device flight ban to European travelers

Source: http://www.homelandsecuritynewswire.com/dr20170426-u-s-considering-extending-electronicdevice-flight-ban-to-european-travelers

Apr 26 – **Passengers flying from the United Kingdom to the United States may soon be barred from carrying their laptops with them, U.K. government officials said Monday.**



In addition to laptops, tablets and e-readers would also have to be checked-in and stored in the hold with other luggage if the restrictions are implemented.

The *Times* reports that Whitehall is bracing for DHS to extend the security restrictions which were imposed last month on ten airports in eight Muslim-majority countries in the Middle East.

U.K. government sources told the *Times* that they were advised by American security officials that the Trump administration is planning on enforce the electronic device ban on flights from several European countries.

The ban, if implemented, will go into effect before the busy summer travel season begins.

The officials told the *Times* that even if the ban is imposed on several European countries, the United Kingdom may be exempted.

The unnamed official told the *Times*: "As with everything from Trump's America, there are conflicting reports about where, when and what."

A spokesperson for the Department of Homeland Security told the *Times*: "We will continue to evaluate the threat environment and make determinations based on that assessment but we have not made any decisions on expanding the current restrictions against large electronic devices in aircraft cabins from selected airports."

Explosions rock Damascus Airport following cargo flights from Iran

Source: http://www.homelandsecuritynewswire.com/dr20170427-explosions-rock-damascus-airport-following-cargo-flights-from-iran

Apr 27 – Explosions rocked the area near Damascus International Airport early Thursday morning following the arrival of four cargo planes from Iran.

"Hours before the blasts, which took place at 3:25 A.M., two Iranian 747 cargo planes, an Iranian Ilyushin il-76 and a Syrian Ilyushin il-76 landed in Damascus, according to the flight radar tracking site Flightradar24.com," *Haaretz* reported.

Emanuele Ottolenghi, a senior fellow at the Foundation for Defense of Democracies who has tracked air traffic between Iran and Syria for years, said the planes were most likely delivering weapons.

In September of last year, Ottolenghi observed, **"Flight records show that Iran Air's flight 697 — the Tehran-Damascus route — was operated 66 times over the last year, including three times from Abadan, on Sept. 8, June 9 and May 10. There were at least an**

additional 20 Iran Air flights to Damascus between Dec. 14, 2015, and the end of August 2016. Not all originated in Tehran, however."

Syrian state media has attributed the missile strikes to Israel, the BBC reported. While Syrian government sources claim that the strikes targeted a fuel tank and warehouses, rebel groups say that the target was an arms depot operated by the Iran-backed terror group Hezbollah.

Without admitting that Israel attacked the airport, Israeli Intelligence Minister Yisrael Katza said that the **"attack is consistent with our policy to prevent Iran's smuggling of advanced weapons via Syria to Hezbollah by Iran."**

Other Israeli leaders have said that Hezbollah receiving game-changing weapons, such as advanced missiles or chemical weapons, represents a "red line" that Israel will not accept.

Other strikes took place inside Syria earlier this year that were attributed to Israel. In February, a number of Hezbollah targets were struck in Damascus. A January strike in Damascus was assessed by military analyst Ron Ben Yishai to have targeted advanced missiles from Iran that were being transferred to Hezbollah.

In December, Israeli Defense Minister Avigdor Liberman suggested that an attack on the Mazzeh military airport near Damascus targeted chemical weapons headed to Hezbollah.

Bomb suspect Zahid Hussain 'made fairy light detonator'

Source: http://www.bbc.com/news/uk-england-birmingham-39736373

Apr 27 – A would-be terrorist attempted to fashion a bomb using a pressure cooker and fairy lights, a court has heard.

Zahid Hussain, 29, filled the appliance with shrapnel and made "improvised igniters" from the festive decorations, jurors were told.

Birmingham Crown Court heard he had researched railway lines as a potential target for the "non-viable" bomb, which he wrongly thought capable of causing devastation.

He denies several charges.

'Bedroom radicalised'

Prosecution QC Annabel Darlow said Mr Hussain was found in possession of a number of books which contained instructions on sabotage and guerrilla warfare tactics.

Zahid Hussain attempted to make a pressure-cooker bomb and improvised detonator parts from fairy lights

She said: "After his computer was recovered, material showed that Mr Hussain held a pronounced interest in Islamic State and events in Syria.

"In his own words he had become bedroom radicalised - turned into a radical by material he had accessed in his own bedroom."

Miss Darlow said the defendant had tried to build "a number of explosive devices", including a pressure cooker bomb and fairy light igniters.

Mr Hussain also attempted to

create a remote-control "initiator" for a device by modifying a wireless doorbell, she said.
Jurors were told Mr Hussain, formerly of Naseby Road, Alum Rock, Birmingham, was arrested on 9 August after reports of a man carrying a hammer and behaving suspiciously near his home.
He was taken to a police station where officers found handwritten recipes for explosives, a modified fairy light and a hand-drawn map showing a drainage chamber in Alum Rock.
Officers then went to his home where they found an "improvised laboratory" and four allegedly viable igniters fashioned from fairy lights, the court heard.
Mr Hussain, who was flanked in the dock by two psychiatric nurses, has pleaded not guilty to preparation of terrorist acts, two counts of making explosives and one of attempting to make explosives.
The trial continues.

AQAP sticky and rock camouflaged IEDs recovered in Hadhramaut

Source: https://www.linkedin.com/pulse/learn-top-terrorist-trends-future-threats-first-ever-monthly-perez

On February 24, 2017, the Engineering Unit of the Yemen Army neutralized two IEDs planted near a police station in Ghayl Ba Wazir village in Hadhramaut, Yemen's southern province. According to reports, at least one IED was concealed in rock shell camouflage and both IEDs were fitted with mobile phone-based RC initiation systems. Rock camouflage shells have thus far been documented in use by the Houthis in Yemen, who produce massive quantities of this camouflage item. It seems that the Houthis' widespread use of this TTP has lately been noted and adopted by al-Qaeda in Yemen.

Eco-extremist instructional video on the production of a parel IED

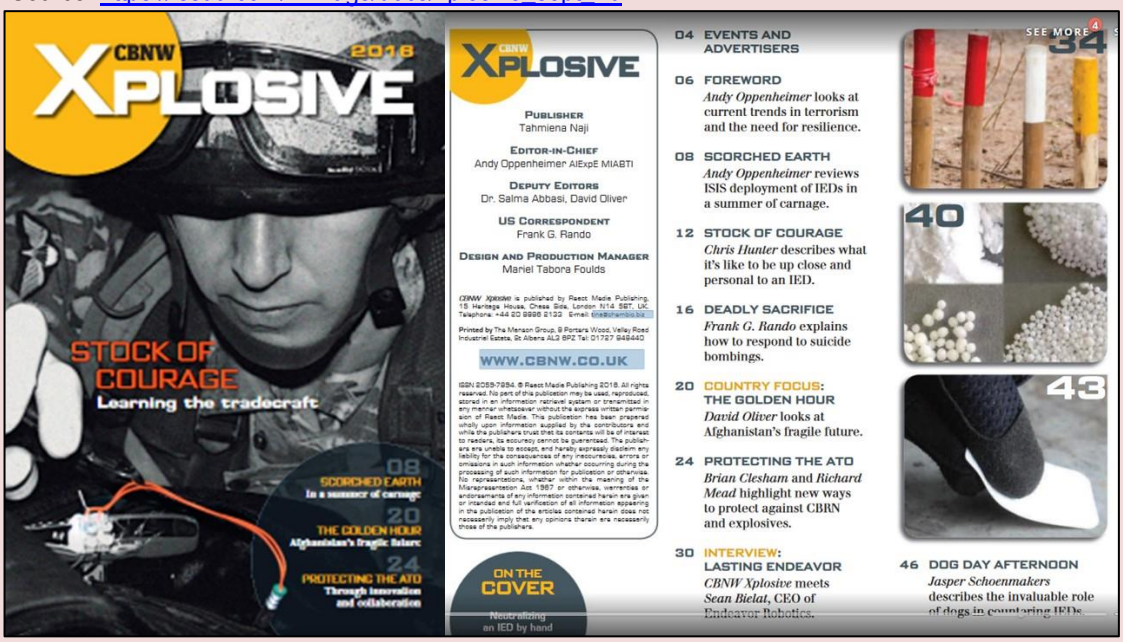
Source: https://www.linkedin.com/pulse/learn-top-terrorist-trends-future-threats-first-ever-monthly-perez

On February 23, 2017, the eco-terrorist group Individualists Tending toward the Wild (Individualidades Tendiendo a lo Salvaje: ITS) that operates mainly in South America posted a video that contains a detailed illustration of the preparation of a booby-trapped parcel IED rigged to initiate when opened, and includes Spanish subtitles. ITS recently claimed responsibility for several terror attacks involving the same parcel IED configuration that appears in the instructional video.

CBNW Xplosive Sept 16

A publication of CBNW Magazine

Source: https://issuu.com/immags/docs/xplosive_sept_16



NY Public Schools Promote Course Justifying Suicide Bombings

Source: https://clarionproject.org/ny-public-schools-promote-course-justifying-suicide-bombings/

May 10 – A lesson plan developed in New York State and promoted by the New York State Education Department called "Dying to be a Martyr," features video interviews with Islamic terrorists who explain why their attacks on Israelis are justified, according to an investigation by *The Blaze*.

For the last decade, the plan has been offered to teachers through the taxpayer-funded Public Broadcasting Service's "LearningMedia" website. The PBS website offers "a media-on-demand service offering educators access to the best of public media and delivers research-based, classroom-ready digital learning experiences."

The lesson plan is geared for high school-age students. As *The Blaze* reports, "There are no instructions in the lesson plan for teachers to denounce these views and no videos are featured showing the Israeli response.

"Among the other biased aspects of the lesson plan are instructions for teachers to 'Check for understanding by asking students to respond to the focus question. (Mohanned, feels he would rather die and by a martyr than live his life, sees his life as hollow—in contrast he sees Israelis as happy, going out, having fun, traveling.) Ask your students why Mohanned may feel that way (Answers may include: Palestinians have less land, fewer privileges, cannot come and go as they please.)'"

A further investigation by the news outlet showed that until the expose on the lesson plan was published, it was being promoted by the New York State Education Department (NYSED). After a request was made for comment by state officials, NYSED's website was changed and the lesson plan was dropped.

However, the plan was still listed on another NYSED website as well the promotion of a video titled "Story of Islam: A History of the World's Most Misunderstood Faith."

***The Blaze* reports that out of 40 items included on the website, "Dying to be a Martyr" was the only complete lesson plan listed.**

The author of the plan is a long-standing public teacher in upstate New York. Requests for comments by *The Blaze* from the author as well as the NYSED were ignored.

423 casualties of anti-vehicle mines incidents reported in 2016

Source: http://counteriedreport.com/news/423-casualties-of-anti-vehicle-mines-incidents-reported-in-2016

May 08 – In 2016, there were 181 incidents related, or suspected to be related, to anti-vehicle mines (AVMs) in 22 states and territories. These incidents caused 423 casualties (195 dead and 228 injured) of which 46 per cent were civilians. While in post-conflict societies, the humanitarian and developmental impact of AVMs is sustained, almost nine out of ten casualties occurred in conflicts settings. Ukraine alone accounted for 24 per cent of global casualties, followed by Mali, Pakistan and Syria.

These were among the findings released by the GICHD and the Stockholm International Peace Research Institute (SIPRI) on Wednesday, 5 May during the 2017 Stockholm Forum on Peace and Development.

The report analyses disaggregated AVM incident data collected in 2016, which are also displayed oninteractive online maps. It compares findings with the 2015 global AVM incident report and follows up on a comprehensive study on the humanitarian and developmental impact of AVMs carried out in 2014. This latest report is a further step in strengthening evidence on the impact of AVMs.

Dismantle bombs — or die trying.

The life of a bomb defuser in Iraq

By Molly Hennessy-Fiske

Source: http://www.latimes.com/world/middleeast/la-fg-iraq-bomb-defuser-2017-htmlstory.html

Bomb defuser Wissam Daoud treads carefully through salvaged Islamic State explosives at the abandoned house. (Marcus Yam / Los Angeles Times)

May 05 – It is only days before he is due to return home on leave, and commanders have sent him behind enemy lines for one last mission: take some of the explosives the Iraqi

army has salvaged from Islamic State and resow them like deadly seeds in the no man's land they call *ard al haram* — the forbidden zone.

Islamic State infiltrators have been stealthily crossing through the deserted stretch of abandoned homes and barricaded businesses to mount attacks against Iraqi troops; the explosives are meant to stop them.

Like many young soldiers, Wissam Daoud, a bomb technician with the Iraqi Ministry of Interior's Emergency Response Division, has been fighting alongside his army colleagues for three years to drive the militants out. He has tracked the evolution of their explosives through a half dozen offensives, and can identify them at a glance: the *Iemsawi*, modified mortar rockets; *kamala*, which can be triggered remotely or by applying pressure; bottle bombs attached to doors; plasma bombs camouflaged as household items or debris.

His job is to render them harmless, or turn them back against the enemy, or die trying.

Daoud's army is no longer the one that turned and fled when fast-moving jihadi militants seized Mosul in 2014. Just as the Iraqi military has hardened through training and combat, so has he.

Dying in an explosion is no longer the 25-year-old Daoud's worst fear. That, he's come to realize, would be painless — he carries an Iraqi flag in his pants pocket, to be draped over his body should the need arise.

What Daoud has learned to fear is a sniper's bullet. Bombs you can see. Snipers are elusive. Their bullets leave soldiers bedridden, permanently disabled.

"Better to die than to be injured," Daoud says. "No one cares about you in Iraq when you are injured."

More than a dozen of his friends have been shot by snipers, and he knows how it goes. Bomb defusers are paid about $1,000 a month, the same as other soldiers, and when they're injured and off duty, the pay gets reduced. Daoud has helped cover injured comrades' hospital bills, and has still seen them languish at home, unable to afford surgeries, medicine and other care the government would not provide.

Daoud's father was also a bomb defuser; he lost three fingers during the bloody war with Iran in the 1980s. He told Daoud not to come home injured. They laughed, but neither considered it a joke.

Iraqi commanders have refused to release military casualty figures since the Mosul offensive started Oct. 17, saying they're bad for morale. But Daoud knows they are high: 200 of his friends have died, many of them young defusers with families.

Daoud prepares his 10-man team for the possibility of a bad outcome each time they set out. "Either I will hold you," he tells them, "or you will hold me."

His longtime mentor will be shot by a sniper on an upcoming mission. His assistant will die before his eyes. And Daoud, a devout Shiite Muslim who joined the military out of religious duty, will have to decide the price he is willing to pay to defeat the elusive, black-flagged Sunni extremists who have declared his country their caliphate.

Since the offensive to retake Mosul started last fall, Daoud has defused hundreds of incendiary devices. He kept them around the abandoned home where his unit was billeted at the edge of West Mosul.

Before setting off for the forbidden zone, Daoud dumped a salvaged suicide belt next to his bed, set a sausage-shaped IED in the living room and stacked mortar rounds by the front door. He paused to demonstrate Islamic State bomb triggers fashioned from syringes and clear plastic fishing line. This is why he cautions children he sees in freed areas of west Mosul not to play with junk they find in abandoned storefronts.

"One small mistake," said the shaggy haired, chain-smoking, veteran bomb technician, "and you're dead."

Daoud's two brothers are also bomb defusers. He grew up tinkering with electronics in Baghdad, later volunteering to defuse bombs militants planted in his blue-collar Shaab neighborhood.

West Mosul's bombs have been the toughest and most plentiful of any offensive so far, he said.

"Many bombs here are hard to see," he said, picking up bomb triggers his team salvaged from booby-trapped homes. "Soldiers can't find them. We call them 'stupid traps.' Clear plastic wire is attached to a door. You won't see it until you pull it with your hand or your head."

Daoud recommends handling a bomb like a baby ("Don't wake it!") or a dog ("Don't frighten it!").

He has seen plenty of civilians killed by Islamic State explosives. In January, his team was pinned down by snipers while trying to rescue a family fleeing east Mosul, who then set off a booby trap. He found their bodies in the street, including a newborn.

Daoud has been injured twice. Two years ago, he stepped on a bomb while fleeing an Islamic State sniper south of Mosul in Baiji, breaking bones in his chest. He still has trouble sleeping because of the injury. More recently, he cut his right leg while destroying a bomb he found at west Mosul airport.

Before Daoud ventured into the forbidden zone, his mother called him, distraught. She'd just seen the bodies of several soldiers killed in Mosul returned to neighbors.

"I'm worried about you," she sobbed. "I saw on the TV the troops reached Ashur Hotel."

Daoud had been at the hotel the day before, defusing bombs. That morning, his team had removed a half dozen mortar rounds and homemade bombs from a Mosul house, and he had joked, "If I keep doing this, I won't ever have any babies!" He was still single, having postponed marriage until after Iraqi forces recapture Mosul.

But he didn't want his mother to worry. So he smiled, and reassured her in a soft voice that he was not on the front lines.

On the day things fell apart in the forbidden zone, Daoud was defusing bombs in a hotel in what was once Mosul's city center.

Later, smoking in his bedroom, he would recall how it started.

By 4 p.m., he was itching to leave, afraid militants were lurking nearby.

"I think it's time to go back," he told his commander.

But Maj. Hussam Hashash, 38, chubby and balding with a thick mustache, wanted to stay another half hour to check a house.

Daoud's fresh-faced mentor, Emir Abdel Mehdi, 24, suggested they avoid approaching the house from the street. So they slipped in through a hole in the wall. Soldiers stood guard outside.

The defusing team advanced in a line, wary of militants to their right.

Then came the shots — from the left.

Mehdi was hit in the left hand and leg. Before Daoud could reach him, sniper fire dislodged a cinder block, pinning Mehdi to the ground. As Daoud watched, his mentor was shot again, in the belly.

Daoud, the major and his slender young assistant, Ali Motar, 36, ran to the wounded soldier. They freed, then carried Mehdi through another hole in a wall to safety while calling for help on their radios.

The assistant was shot in the head as he stood next to Daoud in the house. He died almost immediately.

"Ali was slow," Daoud later recalled. "That's when the sniper shot him."

Mehdi was bleeding heavily. Daoud had to slap his mentor's face to keep him from losing consciousness.

He called an American officer he knew at the joint U.S.-Iraqi military base in nearby Qayyarah. Daoud often helped U.S. forces defuse bombs in his spare time, and had gotten to know the U.S. soldiers. If anything ever happens to a member of your team, the officer had said, call me.

Mehdi was more than just a battle buddy: He had taught Daoud the job, then named his 4-year-old son after him.

Now Daoud was asking the American officer if he could bring Mehdi to the base's clinic. The officer agreed. Mehdi was still alive when they arrived.

He survived. Daoud and his teammates told the medics to notify Motar's young wife that he had not.

"We didn't have the courage," Daoud said later, feeling guilty for having brought the assistant with him.

Mehdi was sent home to Baghdad for surgery.

Days later, Daoud headed home, too. He carried with him the backpacks of his injured and fallen colleagues, to deliver to their families.

Bomb blast at Rome post office

Source: http://www.wantedinrome.com/news/bomb-blast-at-rome-post-office/

May 12 – An explosion occurred outside the post office on Rome's Via Marmorata, where the Aventino and Testaccio districts meet, just before 10.00 on 12 May.

No injuries have been reported after the blast, which police believe may have been caused by two "rudimentary bombs." Police are suggesting that it may be the work of anarchists although they are investigating all possibilities.

The explosive devices were placed in a plastic box between two cars in the car park beside the post office and did not cause structural damage.

Police investigating a separate bomb alert in the Circo Massimo area have said that it was a false alarm

Protesters in Venezuela are deploying "poo-poo-tov cocktails" made of human feces in response to tear gas attacks by police.

Source: http://www.breitbart.com/national-security/2017/05/09/venezuelan-protesters-deploy-poo-poo-tov-cocktails-made-human-feces-riot-police/

May 09 – The home-made weapons, which are glass bottles filled with a mixture of human feces and water, have been used in several cities throughout Venezuela by demonstrators against the National Guard and the Bolivarian National Police as Venezuelans protest Nicolas Maduro's socialist government, *El Pais* reported.

The "fecal" bombs made their first appearance last weekend during a demonstration in Los Teques, a city located a few miles from Caracas.

Demonstrators have already scheduled a protest for Wednesday called "La Marcha de la Mierda," known in English as "the March of Shit."

A dozen National Guard officers in Los Teques hit by the excrement were allegedly grossed out by the bombs and began vomiting, according to *El Pais*.

The demonstration in Los Teques has sparked interest in these "poo-poo-tov cocktails" on social media, with many users posting "recipes" on how to make the bombs on Twitter.

Teenage hacker, 16, who made £400,000 by developing a virus used in 1.7MILLION Xbox live and Minecraft online attacks faces jail

Source: http://www.dailymail.co.uk/news/article-4432646/Teenage-hacker-16-makes-400-000-faces-jail.html

Apr 21 – A teenage computer hacker who pocketed nearly £400,000 by selling a virus which was used in 1.7 million hacking attacks is facing jail.

Adam Mudd, now 20, sold access to the Titanium Stresser tool which let users crash websites and computers by flooding them with data.

He developed the distributed denial of service, or DDoS, software from his bedroom, and started selling it to criminals when he was at school aged 16.

Mudd raked in nearly £400,000 by the time he was 18 by selling the programme to cyber criminals between September 2013 and March 2015.

He received a total of £240,153.66 and 249.81 bitcoins - worth an overall £386,079.

Using the username themuddfamily, he also carried out nearly 600 attacks himself against 181 victims.

One attack on his college was so large it may have hit the University of Cambridge, the Old Bailey heard.

Mudd admitted computer hacking and money laundering last October.

At his sentencing hearing today, the court heard the Titanium Stresser programme had 112,298 registered users.

The 1.7million attacks were carried out against more than 650,000 victims - of which just over 52,000 were in the UK.

Victims included Xbox Live users, and players of the computer games Runescape and Minecraft.

Runescape was targeted 25,000 times - 1.4 per cent of the total attacks.

In the last four years, the company that owns the game has spent nearly £6million attempting mitigate from DDoS attacks, the court heard.

Jonathan Polnay, prosecuting, said: 'I am not trying to suggest those are all from the defendant.'

But he added: 'Every attack that took place in January 2015 came from Titanium Stressor.

'The specific cost of the loss in revenue from the January attacks was £184,000.'

Mudd carried out 594 attacks by himself, including four on his college in 2014 - and the loss was 'incalculable', the court heard.

Mr Polnay said: 'On each occasion, the attack caused the entire college network to go down, on one occasion for half of the day.

'The cost in man hours to investigate and resolve the issue is around £2,000.

'The loss in terms of work and productivity is incalculable, because no one can work in the whole college while the network had been taken down.

'The 16th of September attack was so large it is likely to have affected a further 70 schools

and higher education establishments, including the Universities of Cambridge, Essex and East Anglia as well as local and district councils.'

The attacks were carried out across the world, including the US, Brazil, Australia and Europe.

Mr Polnay said: 'Where there are computers, there have been attacks.

The attacks were carried out across the world, including the US, Brazil, Australia and Europe

'Almost every major city in the world.'

Turning to the money laundering, Mr Polnay said: 'This is a young man who lived at home. This is not a lavish lifestyle case.

'This is about status. The money making is almost by the by. It, to some extent, provides a measure of the seriousness of it. The money is an indicator of how much has been carried out.'

PayPal blocked people from using it for TitaniumStresser payments, but to get around this, 328 separate PayPal accounts were created using fake details.

Mr Polnay said: 'The defendant also used sophisticated techniques to disguise the source of the funds he was receiving, including peer blocking and the use of other websites as payment gateways.

'On one occasion, the defendant falsely arranged for a legitimate website to be linked to the TitaniumStresser so PayPal would wrongly refuse to accept payments from them.'

Investigators looked at Mudd's Skype chats, which showed he knew his programme was being used for the attacks, the prosecutor said.

After one user complained someone was using it for attacks, he replied 'I don't care', Mr Polnay said.

Mudd was arrested on March 3 2015 while he was in his bedroom on his computer.

He was taken to Stevenage Police Station, and made a prepared statement in which he admitted creating the tool but denied being involved in crime.

In a later interview in September 2015, Mudd said the tool started as 'Titanium Booter' and was meant as a 'legitimate stressing tool' for people to stress test their own servers.

The prosecutor said: 'He stated that he renamed it to Titanium Stresser as an attempt to relegitimise it after it had become a DDoS service.

'He stated that it very quickly became a for hire DDoS service that became out of his control but that by mid-2013 he accepts that he was willingly running the Titanium Stresser as a DDoS service.

'He did give explanations to everything and admitted that he was effectively money laundering.'

Mudd admitted doing unauthorised acts with intent to impair the operation of a computer, a charge of making, supplying or offering to supply the Titanium Stresser programme, and concealing criminal property.

Prosecutor Mr Polnay highlighted psychiatric and psychological reports on Mudd which revealed he had Asperger's Syndrome.

He said it was a mitigating feature in terms of the impact of prison and his culpability for the crime.

But he asserted that evidence from Skype chat suggested Mudd was 'well aware what he was doing was illegal and wrong'.

Mudd was supported by his mother and father, who sat in the well of the court.

PayPal blocked people from using it for TitaniumStresser payments, but to get around this, 328 separate PayPal accounts were created using fake details (stock image)

The court heard the defendant lacked social interaction outside his family and suffered from anxiety.

Mitigating, Mr Cooper said Mudd had been 'sucked into' the cyber world of online gaming and become 'lost in an alternate reality' after withdrawing from school due to bullying.

He said Mudd, who was expelled from college, had been offline for two years, which was a form of punishment for any computer-obsessed teenager.

Mudd, who was described as 'bright and high functioning', now understood what he did was wrong but at the time he lacked empathy due to his autistic condition, the court heard.

Mr Cooper said: 'This was an unhappy period for Mr Mudd during which he suffered greatly.

'This is someone seeking friendship and status within the gaming community.'

Among his online peers there was an 'element of bravado and showmanship', he added.

Judge Topolski asked defence barrister Ben Cooper for more information about what the money transfer to Mudd's father's bank account was about.

But he added: 'Overall, I am prepared to sentence your client on the basis this was not the purpose of his criminality.

'It is not acquisitive in a financial sense. What he was seeking to acquire was his position in his world - status.'

The judge said he would adjourn sentencing until Tuesday, April 25.

The typical age of British criminals behind some of the world's most high-profile cyber attacks is just 17, according to new research.

Experts at the National Crime Agency (NCA) said they were shocked at the age of many of those wreaking havoc online.

The crime fighting agency, often touted as Britain's answer to the FBI, is desperate to find ways to divert young minds away from the darker corners of the internet.

Officials have started making 'cease and desist' visits to the homes of those suspected of being on the fringes of internet crime. In the past four years, more than 80 people have been warned that if they continued their activities they faced arrest and prosecution. The figures were contained in an analysis of who is responsible for the rising tide of online attacks against the Government, companies and individuals. Mobile phone companies including Talk Talk, the NHS, Sony, Nintendo, 20th Century Fox and even the NCA itself have all been targeted.

Investigators went back to those who had been prosecuted, arrested or cautioned for computer misuses offences and asked them why they did it.

They discovered that many youngsters began exploring the dark side of the internet after using web-connected games consoles such as the Xbox and PlayStation.

Some were as young as eight when they developed a passion for computers, with many spending every possible moment playing games. By the age of 13 or 14, they had started to adapt the software so they could cheat before moving on to more shadowy activities, including looking for website vulnerabilities, blackmailing companies, creating hacking toolkits to sell and breaking into online accounts.

Richard Jones, of the National Cyber Crime Unit, said: 'There is great value in reaching young people before they ever become involved in cyber crime, when their skills can still be a force for good.

'The aim of this assessment has been to understand the pathways offenders take and identify the most effective intervention points. That can be as simple as highlighting opportunities in coding and programming, or jobs in the gaming and cyber industries.'

Cyber attacks ten years on: from disruption to disinformation

By Tom Sear

Source: http://www.homelandsecuritynewswire.com/dr20170427-cyber-attacks-ten-years-on-from-disruption-to-disinformation

Apr 27 – Today is the tenth anniversary of the world's first major coordinated "cyberattack" on a nation's internet infrastructure. This little-known event set the scene for the onrush of cyber espionage, fake news, and information wars we know today.

In 2007, operators took advantage of political unrest to unleash a series of cyber measures on Estonia, as a possible form of retribution for symbolically rejecting a Soviet version of history. It was a new, coordinated approach that had never been seen before.

Today, shaping contemporary views of historical events is a relatively common focus of coordinated digital activity, such as China's use of social media to create war commemoration and *Russia Today*'s live-tweeting the Russian Revolution as its centenary approaches.

In 2017 and into the future, it will be essential to combine insights from the humanities, particularly from history, with analysis from information operations experts in order to maintain cybersecurity.

Estonia ground to a halt

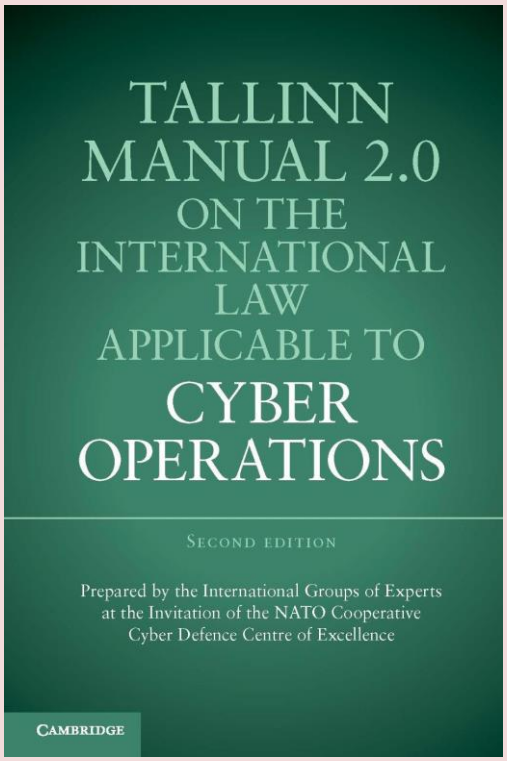
A dispute over a past war triggered what might be called the first major "cyber attack."

On 27 April 2007 the government of Estonia moved the "Soldier of Tallinn" – a bronze statue that commemorated the Soviet Army of the Second World War – from the center of the city to a military cemetery on Tallinn's outskirts. The action followed an extensive debate over the interpretation of Estonia's past. A "history war" concerning the role of the Soviet Union in Estonia during and after the Second World War had split Estonian society.

Several days of violent confrontation followed the statue's removal. The Russian-speaking population rioted. The protests led to 1,300 arrests, 100 injuries, and one death. The disturbance became known as "Bronze Night."

A more serious disruption followed, and the weapons were not Molotov cocktails, but thousands of computers. For almost three weeks, a series of massive cyber operations targeted Estonia.

The disruption – which peaked on 9 May when Moscow celebrates Victory Day – brought down banks, the media, police, government networks and emergency services. Bots, distributed denial-of-service (DDoS) and spam were marshalled with a sophistication not seen before. Their combined effects brought one of the most digital-reliant societies in the world to a grinding halt.



The Tallinn Manual

In the aftermath, NATO responded by developing the NATO Cooperative Cyber Defense Center of Excellence in Estonia. A major contribution of the center was the publication of the Tallinn Manual in 2013 – a comprehensive study of how international law applied to cyber conflict. The initial manual focused on disabling, state-based attacks that amount to acts of war.

Tallinn 2.0 was released in February 2017. In the foreword, Estonian politician Toomas Hendrik Ives argues: "In retrospect, these were fairly mild and simple DDoS attacks, far less damaging than what has followed. Yet it was the first time one could apply the Clausewitzean dictum: War is the continuation of policy by other means."

The focus of the new manual reveals just how much the world of cyber operations has changed in the ten years since Bronze Night. It heralds a concerning future where all aspects of society, not just military and governmental infrastructure, are subject to active cyber operations.

Now the scope for digital incursions by one nation on another is much wider, and more widespread. Everything from the personal data of citizens held in government servers to digitized cultural heritage collections have become issues of concern to international cyber law experts.

A decade of cyber operations

In the ten years since 2007 we have lived in an era where persistent cyber operations are coincident with international armed combat. The conflict between Georgia (2008) and Russia, and ongoing conflict in the Ukraine (since 2014) are consistent with this.

These operations have extended beyond conventional conflict zones via intrusion of civic and governmental structures.

There are claims of nation-state actors active measures and DDoS incidents (similar to those that may have disabled last year's Australian census) on Kyrgyzstan and Kazakhstan in 2009.

German investigators found a penetration of the Bundestag in May 2015.

The Dutch found penetration in government computers relating to MH17 reports.

Now, famously, we know there were infiltrations between 2015-16 into U.S. Democratic party computers. Revealed in the last few days, researchers have identified phishing domains targeting French political campaigns.

There are even concerns that, as Professor Greg Austin has explained, cyber espionage might be a threat to Australian democracy.

Recently, the digital forensics of a computer hacked in 1998 as part of an operation tagged Moonlight Maze revealed that it is possible that the same code and threat actor have been involved in operations since

at least that time. Perhaps a 20-year continuous cyber espionage campaign has been active.
Thomas Rid, Professor in Security Studies at King's College London, recently addressed the U.S. Select Committee on Intelligence regarding Russian active measures and influence campaigns. He expressed his opinion that understanding cyber operations in the twenty-first century is impossible without first understanding intelligence operations in the twentieth century. Rid said: "This is a field that's not understanding its own history. It goes without saying that if you want to understand the present or the future, you have to understand the past."

Targeting information and opinion
Understanding the history of cyber operations will be critical for developing strategies to combat them. But narrowly applying models from military history and tactics will offer only specific gains in an emerging ecosystem of "information age strategies."
The international response to the "attack" on Estonia was to replicate war models of defense and offence. But analysis of the last ten years shows that is not the only way in which cyber conflict has evolved. Even the popular media adopted term "cyberattack" is not now less encouraged for incidents smaller than Estonia as it masks the vulnerability and risk of the cyber security spectrum.
Since Estonia 2007, internet-based incursions and interference have escalated massively, but their targets have become more diffuse. Direct attacks on a nation's defense forces, while more threatening, may in the future be less common than those that target information and opinion.
At the time, the attack on national infrastructure in Estonia seemed key, but looking back it was merely driving a wedge into an existing polarization in society, which seems to be a pivotal tactic.
Nations like Australia are more vulnerable than ever to cyber threats, but their public focus is becoming more distributed, and their goal will be to change attitudes, opinions and beliefs.
A decade ago in Estonia, a cyber war erupted from a history war. The connection between commemoration and information war is stronger than ever, and if nations wish to defend themselves, they will need to understand culture as much as coding.

__Tom Sear__ is Ph.D. Candidate, Australian Centre for Australian Centre for Cyber Security, Australian Defence Force Academy, UNSW.

EDITOR'S COMMENT: In Greece we have "fake interviews" as well. A well known reporter asks "calculated" questions and the politician interviewd answers in a way that is consistent with his/her party propaganda misleading the watching audience – mainly because they both think that we are idiots! But despite the fact that we have the governance we deserve, we continue not to be idiots.

Are Terrorists Using Cryptocurrencies?

By David Manheim, Patrick B. Johnston, Joshua Baron and Cynthia Dion-Schwarz
Source: https://www.rand.org/blog/2017/04/are-terrorists-using-cryptocurrencies.html

Apr 21 – Over the past few years, several experts have voiced concerns that the Islamic State (also known as ISIS) and other terrorist groups could use cryptocurrencies such as Bitcoin as a new funding stream to further their operations. But in spite of these fears, the use of digital currencies among terrorists is not widespread—yet. Neither terrorist financing methods nor cryptocurrency technology is static, however, and the world could soon see the worst-case scenario unfolding. Greater pressure on existing terrorist finance methods coupled with easier-to-use cryptocurrencies that give users greater anonymity may well lead to a large-scale adoption of the technology by extremists.
At present, cryptocurrencies are hardly a go-to solution for terrorist financiers. Most types afford only limited anonymity, and it is difficult to quickly transfer large amounts of money through these systems. Moreover, there is limited acceptance of digital cash in regions such as the Middle East and North Africa, where many terrorist groups are most active.

Yet as the U.S. Treasury Department and its partners have increasingly denied terrorists access to other parts of the international financial system, new cryptocurrency technologies could provide an attractive alternative. To be sure, gauging whether these new technologies will be adopted, and if so, how quickly, is difficult. The answer depends on a host of unknowns, such as what other technologies are around the corner, how the public uses the new cryptocurrencies, and how useful or safe they prove to be. Digital currencies could be used for general funding; for money laundering; or to pay the personnel, associates, and vendors that keep the terrorist machine running. But there can be barriers to use as well, depending on the type of group and how its operations are financed.

The Current Landscape

ISIS receives most of its funding from sources that require control of territory, including the sale of oil, extortion rackets, and the confiscation of private property. Exact numbers are hard to estimate, but taxation of various sorts is said to account for $360 million in revenue per year. It is likely to continue to rely on these funding sources even as its territorial base in Iraq and Syria shrinks.

The territory-based revenue model restricts the group's ability to use cryptocurrency, partly because the latter is difficult to convert into a form that could be readily used in ISIS-controlled areas. Even if this challenge was solved, the large amounts of money a group such as ISIS would need would also severely limit its ability to traffic in cryptocurrency markets. Even as ISIS leadership seeks more diverse funding sources, it is unlikely to become an early adopter as long as it continues to rely on control of territory for funding.

Or consider al Qaeda. The group's fundraising apparatus relied heavily on foreign support until after 9/11, when the U.S. Treasury Department and international banking regulators cracked down on such sources (PDF). If foreign support is still viable, and al Qaeda supporters feel safe doing so, donations of funds via cryptocurrency could undermine the success of this crackdown. Yet most cryptocurrency offers neither sufficient anonymity nor ease of use for would-be donors, and until that changes, it remains unlikely to become a significant source of funds.

Unlike ISIS and al Qaeda, Hezbollah relies heavily on state sponsorship for financing, eliminating much of the need for access to cryptocurrency. In addition, some traditional banks' accommodation of the group currently makes legally moving money a viable option. At the same time, the group's illegal activities abroad—including its large network of associates in drug and other illicit markets in Latin America's tri-border area—are likely to push it to become an early adopter of the virtual currency. If Hezbollah turns to cryptocurrency, given its role in technology transfer in other domains, it may portend the transfer of the relevant technical expertise to other terrorist groups in the near future.

Finally, "lone wolf" attackers—citizens of Western countries inspired by or remotely directed by international terrorist groups—and smaller regional terrorist organizations are mostly self-financed and do not heavily fundraise. However, some lone wolves and individuals traveling to join ISIS have raised funds via Kickstarter-like campaigns. Although cryptocurrency is not yet a viable method for such funding, current efforts by terrorist groups indicate this may already be changing as technical barriers to its use diminish.

The Cryptocurrency Evolution

De-anonymization is currently the largest issue preventing terrorists from using cryptocurrency.

De-anonymization is currently the largest issue preventing terrorists from using cryptocurrency.

Bitcoin and similar currencies allow users the ability to transact without identification, affording partial anonymity, but without user privacy, Western governments can identify and target the funds of these groups. If the terrorists fail to install careful safeguards, preserving this anonymity is unlikely. Just as in other areas of cryptography, the security of transactions can decrease over time as newer attack techniques are developed.

Efforts have also begun to integrate many important cryptocurrency services, such as exchanges where cryptocurrency is bought and sold, into various anti-money-laundering programs in the United States, Europe, and around the world. These regulations require verification of identity and reporting of suspicious transactions and allow law enforcement to investigate users more easily. The more successful a currency becomes, the greater the pressure from users and other stakeholders to work within the traditional financial system and abide by these laws. Greater scrutiny by authorities will inevitably follow.

Additionally, the nations leading counterterrorism finance efforts are among the most sophisticated in terms of cybertechnology, with a wide variety of tools at their disposal. They could attack terrorist groups through vulnerabilities not known to the public. Furthermore, even if the cryptocurrency itself is secure, the computers used for the transactions are vulnerable to the same types of attacks any computer system is, including social engineering, hacking, and physical destruction. Even without these challenges, some terrorist organizations distrust systems funded by Western governments or researchers. This distrust may extend to cryptocurrencies.

Despite these limitations, technological progress promises advances that could accelerate the adoption of cryptocurrency for both lawful and illicit uses, including terrorist financing. Many of the steps currently required to secure anonymous use of cryptocurrencies are not user-friendly, requiring a moderate degree of sophistication and the cumbersome manual transfer of data from secure offline systems. But these usability challenges are likely to fade. Best practices for security will become more widespread as they become easier to use and better known, which has been the case with other technologies, including secure instant-messaging software such as Signal and WhatsApp, which have replaced older and more difficult-to-use programs that were only partially secure.

Some newer cryptocurrencies provide far more robust anonymity, which could harm counterterrorism efforts by undermining a key tool used to track terrorist organizations. Next-generation anonymous currencies such as Zcash and Monero can reduce traceability of transactions that were fixtures in earlier generations of cryptocurrency. Monero greatly increases privacy via cryptographic anonymization, and the ability to hide IP addresses and other advances may be forthcoming. (Recent work (PDF), however, shows that their success is limited.) Zcash, launched late last year, allows secure transactions using a different method that may be extended in the future to allow offline transactions, enabling unrecorded and potentially untraceable transfers that don't rely on clumsy methods like the physical transfer of a cryptocurrency wallet. This would make the use of these currencies viable in parts of the world without reliable Internet access. If these technologies live up to their promise, a major impediment for terrorists and other financial criminals will be removed—at least until even newer ways to attack anonymity and privacy are devised.

For now, cryptocurrencies are unlikely to be stable enough or trusted enough for widespread use—and funding is only one small but critical part of terrorist operations. Although cryptocurrency technologies

continue to have significant limitations for terrorist use, those barriers should decline over time and cause the use of digital currency to spread to other groups. Terrorists' embrace of cryptocurrencies is not yet apparent, but it is not likely far off on the horizon.

David Manheim *is an policy researcher, assistant at the nonprofit, nonpartisan RAND Corporation and a Ph.D. candidate at the Pardee RAND Graduate School.*
Patrick Johnston *is a political scientist at RAND and specializes in counterinsurgency and counterterrorism, with a particular focus on Afghanistan, Iraq, and the Philippines.*
Joshua Baron *is an information scientist specializing in cyberspace operations and cryptography at RAND. Cynthia Dion-Schwarz is a senior analyst at RAND.*

Australian militants funded by gift cards

Source: http://www.skynews.com.au/news/top-stories/2017/05/02/australian-militants-funded-by-gift-cards.html

May 02 – **Terrorists are using pre-paid gift and travel cards to shuffle money throughout Australia, travel to Middle East conflict zones and bankroll international attacks.**

More than 10 million 'stored value cards' are active in Australia - worth upwards of $1.5 billion - and are highly vulnerable to criminal exploitation, a report has found.

Justice Minister Michael Keenan said given the convenience of the readily available cards, it was no surprise criminals and terrorists were exploiting the seemingly innocent technology for ill-gotten gains.

'Any way you can move money around they're going to look to exploit, whether it be

credit cards, whether it be any other instrument within our financial system and that includes pre-paid cards,' he told reporters in Melbourne on Tuesday.

A report released by intelligence agency AUSTRAC has identified 12 instances within two years where the cards were highly likely to have been used to finance terrorism.

They involve more than $170,000 loaded onto travel cards in Australia and redeemed in countries bordering Syria including Turkey, Jordan and Lebanon.

AUSTRAC traced another 66 suspicious transactions including stored value cards redeemed in jurisdictions considered high risk for terrorism financing or transit hubs for terrorism.

'Certainly these cards have been used for terrorists who have left Australia to access that money overseas, and that's one of the vulnerabilities highlighted by the report,' Mr Keenan said.

'Internationally, we have seen SVCs used to fund terrorist attacks, including the horrific terrorism attacks in Paris in November 2015.'

The most prevalent offences identified through the report were money laundering, cyber-enabled fraud, other frauds (including topping SVCs up with lost, stolen or fake credit cards) as well as tax evasion.

Other suspicious activities linked to the cards include scams (primarily suspected romance schemes) and the offshore loading and redemption of SVCs by unknown third parties.

'The most significant potential consequence (of the cards) is the threat to national and international security if used to facilitate terrorism financing,' the AUSTRAC report said.

'Particularly in sustaining and enabling the activities of Australian foreign terrorist fighters.'

AUSTRAC chief executive Paul Jevtovic said stored value cards which could be loaded, reloaded and redeemed in cash domestically carried a higher level of risk than those which could not.
So too did cards which could be redeemed overseas, such as pre-paid travel cards, as opposed to those which could only be used in Australia.
Mr Jevtovic urged Australian businesses offering the cards to protect themselves and the community from criminal misuse.
'I encourage all Australian businesses that issue SVCs to familiarise themselves with this risk assessment to ensure their anti-money laundering and counter- terrorism financing systems and processes are effective,' he said.

Is "Cyberwar" War?

By Steven Aftergood
Source: https://fas.org/blogs/secrecy/2017/05/cyberwar-war/

May 01 – **Are offensive cyber operations an act of war?**
"I would say specifically to your question what defines an act of war [in the cyber domain]– that has not been defined. We are still working towards that definition across the interagency," said Thomas Atkin of the Office of Secretary of Defense at a congressional hearing last year.
He elaborated in newly published responses to questions for the record:
"When determining whether a cyber incident constitutes an armed attack, the U.S. Government considers a number of factors including the nature and extent of injury or death to persons and the destruction of, or damage to, property. Besides effects, other factors may also be relevant to a determination, including the context of the event, the identity of the actor perpetrating the action, the target and its location, and the intent of the actor, among other factors." See *Military Cyber Operations*, hearing of the House Armed Services Committee, June 22, 2016.
If cyberwar is in fact war, would civilians who support military cyber operations be lawful combatants? They might not be, Mr. Atkin said.
"During armed conflict, some civilians who support the U.S. armed forces may sit at the keyboard and participate, under the direction of a military commander, in cyberspace operations. The law of war does not prohibit civilians from directly participating in hostilities, such as offensive or defensive cyberspace operations, even when that activity would be a use of force or would involve direct participation in hostilities; however, in such cases, a civilian is not a 'lawful combatant' and does not enjoy the right of combatant immunity, is subject to direct attack for such time as he or she directly participates in hostilities, and if captured by enemy government forces may be prosecuted for acts prohibited under the captor's domestic law."
But any such danger to unlawful civilian cyber-combatants is probably not an imminent hazard, he added. "Most, if not the great majority, of our civilian cyber workforce involved in providing support to cyberspace operations during armed conflict will not be serving on the battlefield where they may be the object of attack or risk being detained by the enemy. Instead, most will be providing their support remotely from areas outside the area of hostilities, are not easily identifiable as an individual, and are likely serving in the United States."

Steven Aftergood *directs the FAS Project on Government Secrecy. The Project works to reduce the scope of national security secrecy and to promote public access to government information. He writes Secrecy News, which reports on new developments in secrecy policy and provides direct access to significant official records that are otherwise unavailable or hard to find. In 1997, Mr. Aftergood was the plaintiff in a Freedom of Information Act lawsuit against the Central Intelligence Agency which led to the declassification and publication of the total intelligence budget for the first time in fifty years ($26.6 billion in FY 1997). In 2006, he won a FOIA lawsuit against the National Reconnaissance Office for release of unclassified budget records. Mr. Aftergood is an electrical engineer by training (B.Sc., UCLA, 1977). He joined the FAS staff in 1989. From 1992-1998, he served on the Aeronautics and Space Engineering Board of the National Research Council. His work on challenging government secrecy has been recognized with the Pioneer*

Award from the Electronic Frontier Foundation (2010), the James Madison Award from the American Library Association (2006), the Public Access to Government Information Award from the American Association of Law Libraries (2006), and the Hugh M. Hefner First Amendment Award from the Playboy Foundation (2004).

NHS England hit by 'cyber-attack'

Source: http://www.bbc.co.uk/news/health-39899646

May 10 – Trusts and hospitals in London, Blackburn, Nottingham, Cumbria and Hertfordshire have been affected.

Some GP surgeries have had to shut down phone and IT systems while A&Es have told people not to attend unless it's a real emergency. NHS England says it is aware of the issue and is looking into it. Software called ransomware is thought to be behind the cyber-attack. Among those affected is the East and North Hertfordshire NHS Trust which says it is experiencing problems with computers and phone systems. It has postponed all non-urgent activity and is asking people not to come to A&E at the Lister Hospital in Stevenage.

IT specialists are working to resolve the problem as quickly as possible, a statement from the trust says. Also affected is Derbyshire Community Health Services NHS Trust which says it has shut down all of its IT systems following a "secure system attack".

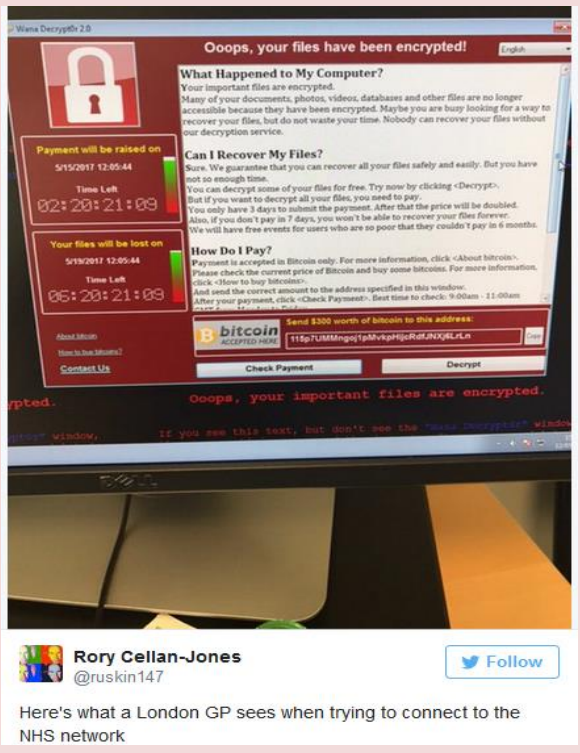
A GP from a surgery in York said: "We received a call from York CCG [Clinical Commissioning Group] around an hour ago telling us to switch off all of our computers immediately.

"We have since remained open, and are dealing with things that can be dealt with in the meanwhile." Meanwhile, Blackpool Hospitals NHS Trust has asked people not to attend A&E unless it was an emergency because of computer issues.

An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak

By Thomas Fox-Brewster (Forbes Staff)

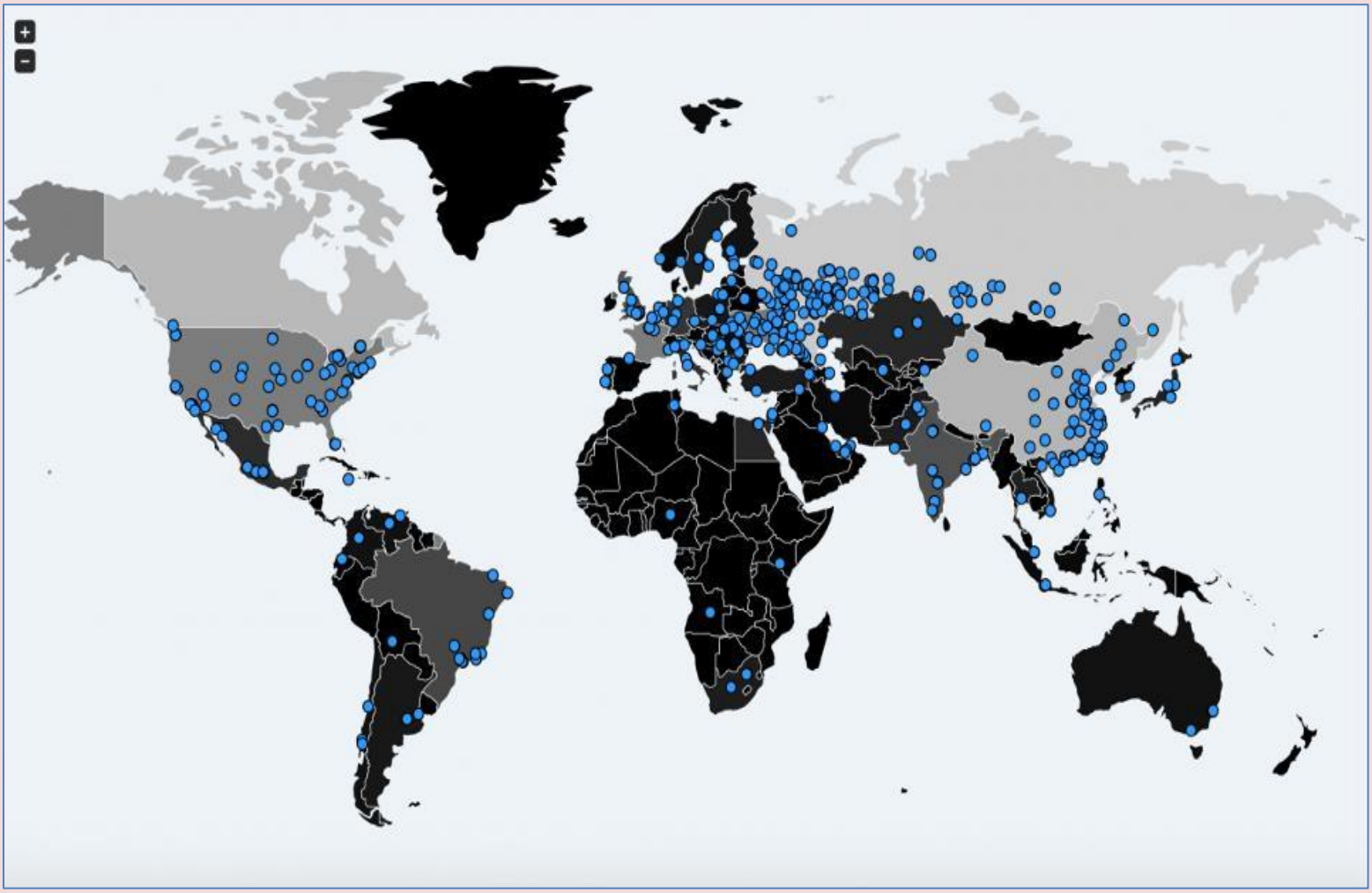
Source: https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#7a45da0ae599



May 12 – It's been a matter of weeks since a shady hacker crew called Shadow Brokers dumped a load of tools believed to belong to the National Security Agency (NSA). It now appears one leaked NSA tool, an exploit of Microsoft Windows called EternalBlue, is being used as one method for rapidly spreading a ransomware variant called WannaCry across the world.

The ransomware has hit UK hospitals hard, with multiple sources reporting closures of entire wards, patients being turned away and some National Health Service (NHS) staff being sent home. Barts Health, a central London NHS trust, advised patients to look for assistance elsewhere and said ambulances were being diverted elsewhere, while another NHS organization said it had to turn away outpatients and limit its radiology services. In the Essex town of Colchester, the hospital decided to close much of its A&E department to accept only

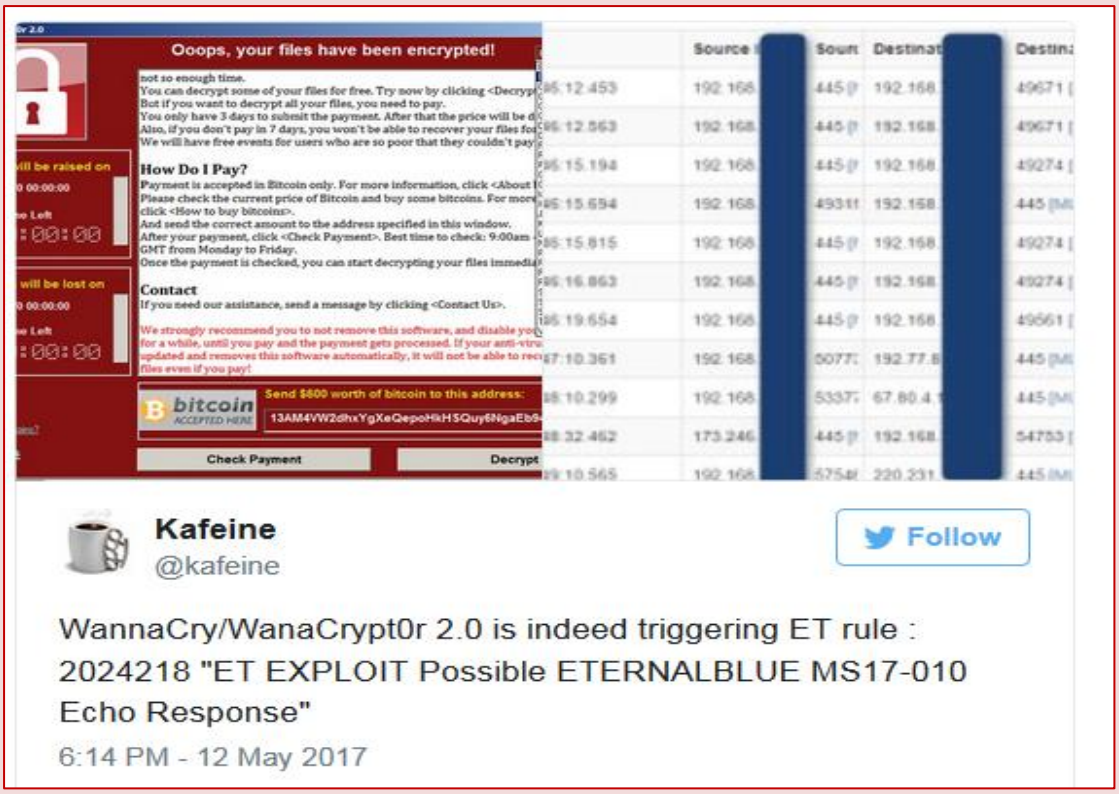
those in "critical or life-threatening situations."
The NHS confirmed 16 NHS organizations had reported that they were hit by the WannaCry ransomware.
But the WannaCry outbreak has hit systems in at least 11 other nations. A security researcher with AVG Avast, Jakub Kroustek, said he'd recorded 36,000 detections of the malware variant today. Russian security firm Kaspersky later said it'd seen as many as 45,000 in 74 countries. According to the MalwareHunterTeam, which said WannaCry was "spreading like hell," Russia has been the hardest hit, but Spain also seems to be under severe attack too, with telecoms giant Telefonica reportedly affected.
As shown on a map from another independent security researcher, MalwareTech, a large number of U.S. organizations have been hit. According to the researcher, at least 1,600 have been infected with WannaCry in America, compared to 11,200 in Russia and 6,500 in China.



The outbreak of WannaCry has hit tens of thousands of systems across the world, including PCs in America.
Victims have been asked to pay up to $300 to remove the infection from PCs, otherwise their files remain locked and their computers rendered unusable.
FedEx confirmed to *Forbes* it was one of the America organizations attacked: "Like many other companies, FedEx is experiencing interference with some of our Windows-based systems caused by malware. We are implementing remediation steps as quickly as possible. We regret any inconvenience to our customers."

Eternal Blue danger
The use of the NSA EternalBlue exploit was confirmed by an independent malware researcher known as Kafeine:

Kafeine told *Forbes* that it was unsure if the exploit was being used as the ransomware's primary



method of infection, but was certain it was used in some capacity. Separately, UK-based researcher Kevin Beaumont tweeted that WannaCry was using the NSA attack, which exploited a now-patched Microsoft Windows vulnerability, also known as MS17-010. And a Spanish Computer Emergency Response Team (CERT) said the vulnerability was used by the ransomware crooks.

As *Forbes* had previously reported, Russian cybercriminals have been discussing ways in which to make use of the Shadow Brokers leak. That included the possible use of EternalBlue, which abused the Server Message Block (SMB), a network file sharing protocol.

"MS17-010 is the best candidate for this ransomware attack," said Matthew Hickey, co-founder of British cybersecurity training hub Hacker House. He compared it to another massive malware outbreak of yore, called Conficker, which used worm-like features to spread rapidly across the world.

What's disconcerting is that if MS17-010 was used in these fresh cybercriminal attacks, it would indicate many hadn't patched despite the widespread reporting of the issue, which was fixed in March. "Is it unsurprising that people don't apply fixes? Not really," added Hickey. "MS17-010 will be widely used for these kind of purposes. If anything I am only surprised it hasn't happened sooner.

"It does indeed highlight dangers of NSA exploits being released to the public. I have made the point repeatedly that people should not downplay the significance of the recently released tools and exploits. They are weapons-grade and available for easy use. Attacks like the one hitting the NHS are an easy way for criminals to capitalize on these exploits."

'WMD of ransomware'

According to CrowdStrike's vice president of intelligence Adam Meyers, the initial spread of WannaCry is coming through spam, in which fake invoices, job offers and other lures are being sent out to random email addresses. Within the emails is a .zip file, and once clicked that initiates the WannaCry infection.

But the most concerning aspect of WannaCry is its use of the worm-like EternalBlue exploit. "This is a weapon of mass destruction, a WMD of ransomware. Once it gets into an unpatched PC it spreads like wildfire," he told *Forbes*. "It's going through financials, energy companies, healthcare. It's widespread."

Given the malware is scanning the entire internet for vulnerable machines, and as many as 150,000 were deemed open to the Windows vulnerability as of earlier this month, WannaCry ransomware explosion is only expected to get worse over the weekend.

British blogger 'accidentally stops international ransomware attack' by spending £8 registering a domain name

Source: http://www.mirror.co.uk/news/uk-news/british-blogger-accidentally-stops-international-10413643

May 13 – A British blogger reportedly stopped the worldwide spread of the cyber attack that hit the NHS - by spending £8 registering a domain name.

The WannaCry ransomware has affected tens of thousands of computers in more than 70 countries around the world by using a flaw in an old version of Microsoft Windows .

But cyber security blogger **@MalwareTechBlog** managed to find a 'kill switch' that halts the spread of the bug, the Guardian reports , at least temporarily.

Within the code of the bug there was an unregistered website name, and when Malware Tech realised it was up for grabs he registered it for $10.69.

"I saw it wasn't registered and thought 'I think I'll have that'," the Daily Beast reports him as saying .

He redirected the site to a 'sinkhole' server, which gives out false information so computers can't access the real website. In effect, this blocks the spread of the ransomware attack.

But the misery won't necessarily stop warns Malware Tech, who posts about issues like ransomware on his blog .

"If we did stop it, there's like a hundred percent chance they're going to fire up a new sample and start that one again," he said. "As long as people don't patch it's just going to keep going."

► **UPDATE:** Could it be a N. Korean cyber attack?

New tool for first responders: An ice bag to the face

Source: http://www.homelandsecuritynewswire.com/dr20170427-new-tool-for-first-responders-an-ice-bag-to-the-face

Apr 27 – **A new study suggests a simple bag of ice water applied to the face could help maintain adequate blood pressure in people who have suffered significant blood loss**. Blair Johnson, assistant professor at the University at Buffalo, yesterday presented his team's work at the American Physiological Society's annual meeting during the Experimental Biology 2017 meeting, held in Chicago.

APS says that the researchers' aim is to help prevent cardiovascular decompensation, a sudden precipitous drop in blood pressure that limits oxygen delivery to the heart, brain, and other vital organs. Decompensation is a significant risk after blood loss, even once the person is no longer actively bleeding.

"We believe that cooling the face could potentially be used as a quick and temporary method to prevent cardiovascular decompensation after blood loss once active bleeding has stopped," said Johnson. "We think that this technique could be used by first responders or combat medics on the battlefield to give additional time for transportation or evacuation."

As a preliminary test of the technique, the researchers recruited ten healthy volunteers, who were put into a special chamber that mimics what happens to blood circulation when a person has lost about one-half to one liter of blood and had a tourniquet applied to stop further blood loss. The researchers applied bags of either ice water or room-temperature water to the volunteers' faces for fifteen minutes while continuously measuring indicators of cardiovascular function.

Participants treated with the ice bag showed significant increases in blood pressure, suggesting that cooling the face could help bolster cardiovascular functioning after blood loss and prevent a dangerous fall in blood pressure.

Johnson cautioned that the technique is intended only for preventing cardiovascular decompensation after active bleeding has stopped, for example, by using a tourniquet. Increasing blood pressure during active bleeding could exacerbate blood loss.

After conducting more laboratory research to determine the environments and types of situations in which face cooling is most likely to be effective, the researchers hope to test the technique in a clinical trial.

— Read more in Bair Johnson et al., "Face Cooling Increases Blood Pressure during Simulated Blood Loss" (paper presented at the Experimental Biology 2017 meeting, 26 April 2017).

International CBRNE Institute

join us

CBRN Knowledge Center

Explosives Knowledge Center

ici-belgium.be/en/