07\21

HZS CBRNE DIARY

Dedicated to Global First Responders

July 2021

A ALPHA (al-fah)	B BETA (bay-tuh)	Γ GAMMA (gam-uh)	Δ DELTA (del-tuh)
E EPSILON (ep-si-lon)	Z ZETA (zay-tuh)	H ETA (A-tuh)	Θ THETA (thay-tuh)
I IOTA (eye-o-tuh)	K KAPPA (cap-uh)	Λ LAMBDA (lamb-duh)	M MU (muew)
N NU (new)	Ξ XI (zie) or (zee)	O OMICRON (om-i-cron)	Π PI (pie)
P RHO (row)	Σ SIGMA (sig-muh)	T TAU (taw)	Y UPSILON (yoop-si-lon)
Φ PHI (fye)	X CHI (kie)	Ψ PSI (sie)	Ω OMEGA (o-may-guh)

A HOTZONE SOLUTIONS GROUP PUBLICATION

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DIRTY R-NEWS

Iran Says It Foiled "Sabotage Attack" on Nuclear Building

Source: http://www.homelandsecuritynewswire.com/dr20210623-iran-says-it-foiled-sabotage-attack-on-nuclear-building

June 23 – Iran thwarted a planned "sabotage attack" on Wednesday on a building belonging to the country's nuclear energy agency, according to state television.
There were no casualties or damage as it "foiled" the attack before it could cause "any damage to the building," the broadcaster reported.
Nournews, a website believed to have close links to Iran's Supreme National Security Council, said: "On Wednesday morning, a sabotage operation against one of the [Atomic Energy Organization of Iran] buildings was foiled."
"It did not cause any damage in financial or human terms."
The case had been put "under investigation," the report said.
Iran's semi-official ISNA news agency said the building was located near Karaj city, some 40 kilometers (25 miles) west of Tehran.
According to Iran's Atomic Energy Organization, the Karaj facility was founded in 1974 and deals with enhancing the "quality of soil, water, agricultural and livestock production using nuclear technology."

Iran Points Finger at Israel for Previous Attacks

Wednesday's attack comes after several suspected sabotage attacks targeting Iran's atomic program in recent months.
In April, Iran's Natanz nuclear facility suffered a blackout that caused damage to some of its centrifuges, an act Iran described as "nuclear terrorism."
Tehran has accused Israel of several attacks on facilities linked to its nuclear program, as well as blaming Israel for the killing a nuclear scientist last year. Israel has neither denied nor confirmed the allegations.
Last year, Natanz suffered a mysterious explosion at its advanced centrifuge assembly plant that authorities later described as sabotage. Iran now is rebuilding that facility deep inside a nearby mountain. Iran also blamed Israel for the November killing of a scientist who began the country's military nuclear program decades earlier.
All of this coincides with efforts to revive the flagging 2015 nuclear deal between Tehran and world powers.

Reflections on Iran's Production of 60% Enriched Uranium

By David Albright and Sarah Burkhard

Source: http://www.homelandsecuritynewswire.com/dr20210623-reflections-on-iran-s-production-of-60-enriched-uranium

June 23 – As of about June 14, Iran had reportedly produced 6.5 kg 60% enriched uranium (hexafluoride mass) or 4.4 kg uranium mass only. Iran's IR-6 production-scale cascade has produced 60% enriched uranium at an average daily rate of 0.126 kg/day since May 22, using less than 5% LEU as feed, skipping the intermediate step of producing 20% material. Of course, the operation of the IR-6 cascade and the production of 60% is banned by the JCPOA. Returning to the JCPOA requires the destruction of this IR-6 cascade and the removal of the 60%. Failing to do either, such as by mothballing the IR-6's, would represent in effect a renegotiated JCPOA; one that is weaker than the original. Iran's activity must be viewed as practicing breakout to make enriched uranium for use in nuclear weapons. It is learning to make such material more quickly and developing valuable experience in doing so.
This experience also complicates returning to the JCPOA, since that experience cannot be destroyed. As a result, some compensating actions are needed or a number of sanctions should be left in place to compensate for this irreversible gain in violation of the JCPOA.
Often lost in the debate is that 60% enriched uranium can be used directly in a nuclear explosive, although 90% is preferred. Iran now has about 10 percent of what it would need for one nuclear explosive fashioned from 60% enriched uranium. At current rates, Iran would need about 1.3 years to make enough 60% for a nuclear explosive. Two of these IR-6 cascades could make enough in less than 8 months; four could do so in four months.

▶ **See also:** https://isis-online.org/isis-reports/detail/analysis-of-iaea-iran-verification-and-monitoring-report-may-2021 ; https://www.iaea.org/sites/default/files/21/06/gov2021-28.pdf

David Albright *is the founder and president of the Institute for Science and International Security.*
Sarah Burkhard *is a research associate at the Institute.*

Israeli TV: UAVs targeted Iran nuclear facility where centrifuge parts produced

Source: https://www.timesofisrael.com/liveblog_entry/israeli-tv-uavs-targeted-iran-nuclear-facility-where-centrifuge-parts-produced

June 23 – Drones were used in the attempted attack on an Iranian nuclear facility, according to Channel 13.

The targeted facility, a sprawling nuclear center located in **Karaj city**, just some 40 kilometers (25 miles) northwest of Tehran, was manufacturing parts used in centrifuges, according to the network, which cites Iranian sources.

The television report doesn't say who is responsible for the strike or specify on the extent of the damage.

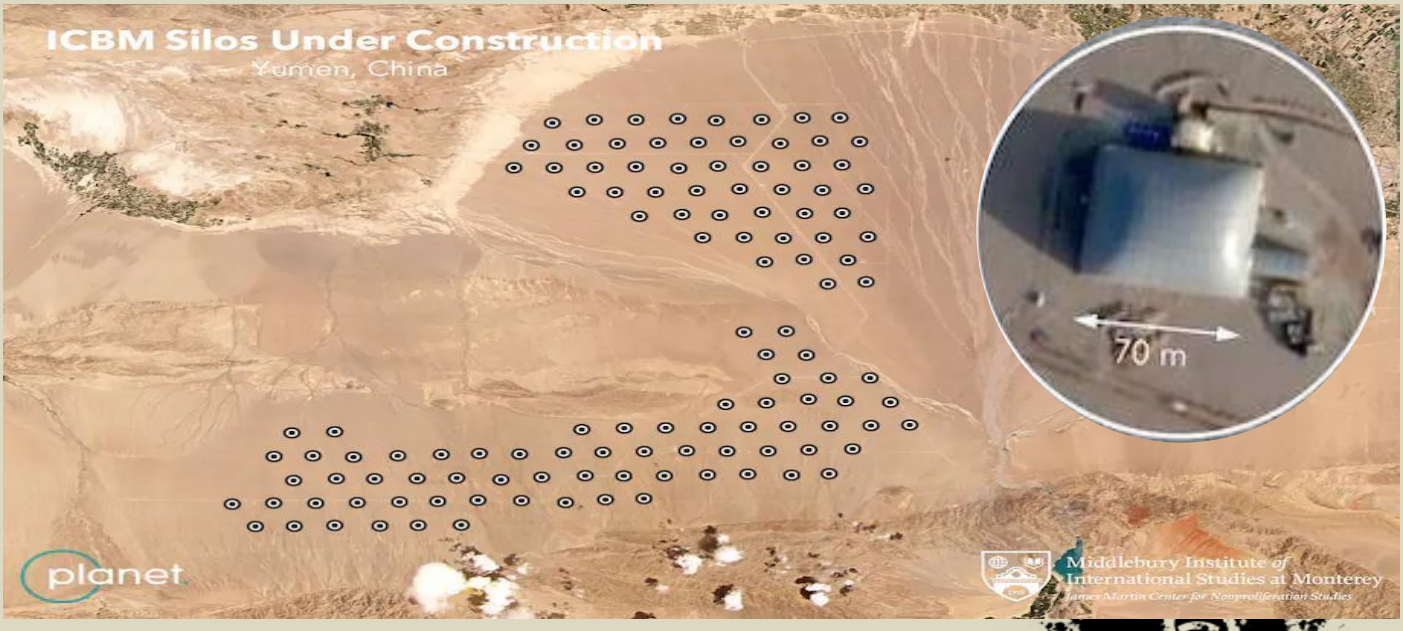
Iran state television earlier said a "sabotage operation against one of the buildings (of the Atomic Energy Organization of Iran) was foiled" without causing any casualties or damage. "The saboteurs failed to carry out their plan," the broadcaster added, without identifying the building or the nature of the attack that had been averted.

Israel, which has vowed to prevent Iran from attaining nuclear weapons, had no official comment on the Iranian reports Wednesday.

China is building more than 100 new missile silos in its western desert, analysts say

Source: https://www.washingtonpost.com/national-security/china-nuclear-missile-silos/2021/06/30/0fa8debc-d9c2-11eb-bb9e-70fda8c37057_story.html?itid=ap_jobywarrick

June 30 – Satellite images point to a construction spree for ICBM launch tubes that could a signal a major expansion of Beijing's nuclear capabilities, though some could be decoys.



▶▶ Read also: U.S. Concerned About Report China is Expanding Missile Silos

A millennial's view: ICBMs are ridiculous

By Noah C. Mayhew

Source: https://thebulletin.org/2021/07/a-millennials-view-icbms-are-ridiculous/

July 08 – The international community is increasingly prioritizing the voices of young experts in nuclear nonproliferation and related issues. This generation—my generation—is facing the simultaneous pressure to pursue higher education to be successful and, at least in the United States, the burden of taking on gargantuan amounts of student debt. As someone who has invested more than $100,000 in educating myself about topics as salient as nuclear nonproliferation, US-Russian arms control, and international diplomacy, I find it absolutely incomprehensible why the United States puts the kind of money it does into military spending ($778 billion in 2020)—and more specifically into the obscene budget for the nuclear modernization project, which will cost taxpayers an estimated $1.2 trillion to $1.7 trillion over 30 years.

These figures lead me, and I suspect many other young American nuclear policy experts, to question why my government is spending this level of money to modernize a leg of the US nuclear triad—namely intercontinental ballistic missiles (ICBMs)—that not only is outrageously expensive but also inherently destabilizing and unnecessary for deterrence.

Former US Defense Secretary William Perry and Ploughshares Fund Policy Director Tom Z. Collina said it in their 2020 book, *The Button*. Arms Control Association Executive Director Daryl Kimball said it in a 2021 edition of *Arms Control Today*. Others have said it and have been saying it for years.

ICBMs are ridiculous.

Let me explain. None of these experts have written these words verbatim, but they have outlined in frightening and depressing fashion why ICBMs should be phased out. There are three main reasons for this: the particular danger ICBMs pose, their redundancy in nuclear deterrence, and their ludicrous cost.

They are the most dangerous leg of the nuclear triad. They are the epitome of use-it-or-lose-it weapons in a crisis. As Perry and Collina point out, Russia knows exactly where all the United States' ICBMs are and could (but certainly wouldn't) attack them at any time in a first-strike scenario. In response to a warning of an incoming attack, true or mistaken, the US could either launch its ICBMs so that they are not destroyed should the attack be genuine, or wait to ensure that the attack is real, thus guaranteeing that a majority of American ICBMs would be destroyed. There is no reason to continue with a US nuclear strategy that creates this much risk, especially given the plethora of false alarms of incoming attacks, which are a matter of public record. Put simply, ICBMs are too dangerous.

Proponents of ICBMs say we need to retain them as a "sponge" that, in a first-strike, full-war scenario, would require an attacker to expend much of its nuclear forces to take out US ICBMs. But the US can respond to a nuclear attack with or without ICBMs. As Kimball and others point out, just one US nuclear-armed submarine, which carries on the order of 160 thermonuclear warheads with yields far greater than the bombs dropped on Hiroshima and Nagasaki, would be enough to devastate an entire country in a second strike. Nuclear-armed submarines are, by design, nearly impossible for other countries to track. If the goal is retaining a second-strike capability to ensure a credible deterrent, ICBMs are redundant.

If one accepts the previous two arguments—that ICBMs are needlessly dangerous and, in fact, redundant—it becomes even harder to understand why the United States spends so much money on them. The 2021 budget for the Ground Based Strategic Deterrent, the planned replacement for today's ICBMs, is $1.5 billion. That is for just one year. The Biden Administration's ask for this program in 2022 is $2.6 billion.

Nuclear policy discourse (correctly) includes increasing input from next-generation or emerging experts—pick your moniker. Here are just a few reasons, from a young expert's perspective, why President Biden should, at the very least, freeze the budget for the Ground Based Strategic Deterrent, as Kimball suggests for a first step, noting that even just freezing

this budget at 2021 levels would save $1 billion. Or better yet, phase out ICBMs altogether, as Perry and Collina suggest. Either of these steps could provide significant cost savings.
Because of the way the federal budget is built, with separate categories for defense and non-defense spending, any immediate cost savings from an ICBM budget freeze would be redirected to other projects within the Defense Department and could not be used for non-military projects. Still, it's a worthwhile thought experiment to consider how future budget requests could phase out ICBMs while increasing funding for other projects by an equivalent amount. The financial strains in student loan debt, healthcare costs, climate change mitigation, and even budgetary issues in nuclear governance demonstrate that there are many better uses for that money.

Student debt
This is the raison d'etre for my rant. Borrowers in the United States already owe nearly $1.6 trillion for educational loans. It is incomprehensible to me and to many other young experts why the country that spends more than any other nation on defense cannot make education affordable for its youth. The federal government, which owns more than 90 percent of US student loan debt, estimates that approximately one third of this debt will never be repaid. What a difference it would make in the lives of so many young experts, both in the nuclear field and elsewhere, if money saved on missiles and missile modernization could be used to bolster the young generation of American leaders, rather than to weigh it down.

Healthcare
A similar argument applies to healthcare. The United States is the only industrialized nation that does not offer universal health insurance. During the COVID-19 pandemic, this fact became much more salient, as hospitals were overwhelmed and the entire healthcare system came under immense pressure. It was a revelation to me, when I moved to Austria, that a trip to the emergency room there wouldn't drown me in bills I couldn't pay. The first time I went to pick up medication and wasn't handed a bill, the pharmacist looked at me and said, "Yes, no bill—in this country we believe healthcare is a human right." Imagine how far the money from the Ground Based Strategic Deterrent program could go toward easing strains on the American healthcare system.

Climate change
It's not just Greta Thunberg who's unhappy with the global response to climate change—it's at least 86 percent of young Americans, and most of us understand that human activities are to blame. To mitigate the effects of climate change, there has to be more money invested in carbon-friendly energy. It doesn't have to be nuclear energy (although Russian colleagues and I argued in 2020 that nuclear is among the safer energy sources). Funds freed up from the ICBM modernization program could go to research and development for advanced reactor designs; and construction of more wind turbines, solar panels, and hydroelectric stations.

Nuclear safeguards
The international community relies on the International Atomic Energy Agency (IAEA) to ensure that nuclear technology remains in peaceful uses. The IAEA applied nuclear safeguards in 183 countries in 2020, and it did so to the tune of 148.7 million euros (approximately $177 million). This budget includes verification activities under the Joint Comprehensive Plan of Action, the Iran nuclear deal. The number of facilities and other locations required to be under safeguards is growing, while the IAEA continues to work with a zero-real-growth budget (increasing only enough to account for inflation). The United States is already the IAEA's largest funder, but the money spent on ICBMs and their modernization would be better spent on support to the IAEA, including Member State Support Programs that augment safeguards activities.
These are just a few items that the United States government could prioritize over ICBMs. Other options include funding verification research, through initiatives like the International Partnership for Nuclear Disarmament Verification, so that when further reductions in nuclear arms become possible, we have the technology to support that. The United States could also contribute more to the implementation of the UN Sustainable Development Goals, including funding to make up for progress lost due to the COVID-19 pandemic.
Young experts in this field are not naïve. We are fully aware that, as long as they exist, nuclear weapons will continue to require spending on maintenance to ensure safety and reliability, regardless of whether these weapons are in silos, on submarines, or in the air. However, it does not make sense, financial or otherwise, to invest enormous sums of money in modernizing the ICBM leg of the nuclear triad when it is not needed for national security.
President Biden has an opportunity here. The hole in arms control left by the US withdrawal from the Intermediate-Range Nuclear Forces Treaty is aching to be filled. The slow rot of the Open Skies Treaty makes this hole even deeper. Why not fill it by unilaterally phasing out an entire class of nuclear weapons? Removing the ICBMs from the US nuclear fleet, even pledging to do so, would provide a sorely needed confidence-building measure in the US-Russia relationship.

My generation is tired of seeing billions directed to dangerous, destabilizing weapons rather than to investments in our future. It's time for ICBMs to go.

Noah C. Mayhew *joined the Vienna Center for Disarmament and Non-Proliferation in July 2018 as a research associate focusing on nuclear nonproliferation, IAEA safeguards and nuclear verification, arms control, US-Russia relations, and the nexus between nuclear security and the peaceful uses of nuclear science and technology. Some of his previous contributions to nuclear discourse have been published by Stiftung Entwicklung und Frieden,* The Nonproliferation Review*, and the Swedish Radiation Safety Authority. Noah is also a Young Deep Cuts Commissioner and currently serves as co-chair for the Emerging Voices Network's NPT Working Group.*

Reactor vessel installed at first Turkish unit

Source: https://www.world-nuclear-news.org/Articles/Reactor-vessel-installed-at-first-Turkish-unit

July 07 – The Reactor Pressure Vessel (RPV) has been installed at unit 1 of the Akkuyu nuclear power plant under construction in Turkey. Russian state nuclear corporation Rosatom, which is constructing four VVER-1200 reactors at the site in Mersin province, described the milestone as "one of the key stages in the main equipment assembly".

identiFINDER® R700

Source: https://www.flir.eu/products/identifinder-r700/

The FLIR identiFINDER R700 Backpack Radiation Detector (BRD) offers new spectroscopic broad-search capabilities. Once dismounted, the identiFINDER R700 provides the capabilities required to successfully perform wide-area searches quickly and efficiently while offering exceptional sensitivity, communication, and trusted spectroscopic algorithms in a lightweight, ergonomic form-factor.

- *Interrogate and Isolate Radiological Threats Quickly*
  Building on the award-winning identiFINDER R440, the identiFINDER R700 offers advanced spectroscopic algorithm and detection techniques scaled to a man-portable backpack for increased sensitivity and speed.
- *Deploy At The Scene Or On The Move, Covertly*
  The identiFINDER R700 can be configured as a nondescript backpack or a stationary screening device, allowing for multiple mission sets from covert wide-area searches to temporary checkpoints.
- *Share Intelligence Broadly, Or Operate Silently*
  Providing critical information to decision-makers quickly is essential, so the identiFINDER R700 provides the capability to do so in real-time and on-demand. Wireless communications and a robust API enable integration with user-deployed networks. Tethered-display options provide a radio silent (air-gapped) option for highly sensitive missions.

Pentagon Sees "Increased Potential" for Nuclear Conflict

By Steven Aftergood

Source: https://fas.org/blogs/secrecy/2021/07/increased-potential/

July 06 – The possibility that nuclear weapons could be used in regional or global conflicts is growing, said a newly disclosed Pentagon doctrinal publication on nuclear war-fighting that was updated last year.

"Despite concerted US efforts to reduce the role of nuclear weapons in international affairs and to negotiate reductions in the number of nuclear weapons, since 2010 no potential

adversary has reduced either the role of nuclear weapons in its national security strategy or the number of nuclear weapons it fields. Rather, they have moved decidedly in the opposite direction," the Department of Defense document said.
"As a result, there is an increased potential for regional conflicts involving nuclear-armed adversaries in several parts of the world and the potential for adversary nuclear escalation in crisis or conflict."
The publication presents an overview of U.S. nuclear strategy, force structure, targeting, and operations. See *Joint Nuclear Operations*, JP 3-72, April 2020.
The document replaces a 2019 edition titled *Nuclear Operations* that was briefly disclosed and then withdrawn from a DoD website. (See "DoD Doctrine on Nuclear Operations Published, Taken Offline," *Secrecy News*, June 19, 2019.)
The current document no longer includes some of the more unfiltered and enthusiastic languages about achieving "decisive results" through nuclear strikes and "prevail[ing] in conflict" that appeared in the 2019 version. The statement that "The President authorizes the use of nuclear weapons" was changed to a more restrained declaration that "Only the President can authorize the use of nuclear weapons."
Meanwhile, new material has been added, including an assessment that the threat from potential adversaries has grown even as the US nuclear posture is said to have been moderated:
"While the United States has continued to reduce the number and salience of nuclear weapons, others, including Russia and China, have moved in the opposite direction. They have added new types of nuclear capabilities to their arsenal, increased the salience of nuclear forces in their strategies and plans, and engaged in increasingly aggressive behavior."
"Russia's strategic nuclear modernization has increased, and will continue to increase, its warhead delivery capability, which provides Russia with the ability to rapidly expand its deployed warhead numbers."
"China continues to increase the number, capabilities, and protection of its nuclear forces."
"North Korea's continued pursuit of nuclear weapons capabilities poses the most immediate and dire proliferation threat to international security and stability."
"Iran's development of increasingly long-range ballistic missile capabilities, and its aggressive strategy and activities to destabilize neighboring governments, raises questions about its long-term commitment to forgoing nuclear weapons capability." Given the mounting threat, DoD said, "Flexible and limited US nuclear response options can play an important role in restoring deterrence following limited adversary nuclear escalation." The updated document gives expanded attention to the role of intelligence in a potential nuclear conflict including "knowledge of an adversary decision maker's perceptions of benefits, costs, and consequences of restraint" and "information about adversary assets, capabilities, and vulnerabilities." Intelligence is also needed for post-strike damage assessments. Strategic messaging is key to deterring conflict, DoD said, though this often seems to involve the threat of force. "The ability to communicate US intent, resolve, and associated military capabilities in ways that are understood by adversary decision-makers is vital. Direct military means include forward presence, force projection, active and passive defense, strategic communications/messaging, and nuclear forces." DoD asserts that its system of nuclear command and control is "ready, reliable, and effective at meeting today's strategic deterrence requirements. There are no gaps or seams that adversaries could exploit." Maybe so. "Possibly the greatest challenge confronting the joint force in a nuclear conflict is how to operate in a post-NUDET [nuclear detonation] radiological environment," DoD said. "By design, nuclear weapons are highly destructive and have harmful effects that conventional weapons do not have. Commanders must plan for and implement protective measures to mitigate these effects and continue operations." *Joint Nuclear Operations* is not available in DoD's online public library of Joint Publications. But a copy of the April 2020 document was released to the Federation of American Scientists last week under the Freedom of Information Act.

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. Mr. Aftergood is an electrical engineer by training.*

China will 'use nuclear bombs' if Japan intervenes with Taiwan

Source [+video]: https://www.express.co.uk/news/world/1464137/china-nuclear-bombs-ccp-threat-japan-taiwan-nukes-interfere-pla-china-xigua-ont

July 18 – The Baoji Municipal Committee, a CCP authority in the province of Shaanxi, shared the five-minute video, originally posted on the Chinese video sharing platform, Xigua. The narrator calls for the use of weapons of mass destruction to be used against Japan to make them surrender "for a second time".

Although the original video was removed (after gaining more than two million views), human rights activist Jennifer Zeng, uploaded the video to Twitter with English subtitles.

The video says: "When we liberate Taiwan, if Japan dares to intervene by force, even if it only deploys one soldier, one plane and one ship, we will not only return reciprocal fire but also start a full-scale war against Japan.

"We will use nuclear bombs first.

"We will use nuclear bombs continuously until Japan declares unconditional surrender for the second time.

"What we want to target is Japan's ability to endure a war. As long as Japan realizes that it cannot afford to pay the price of war it will not dare to rashly send troops to the Taiwan strait."

In 1964, China declared its 'No first use' (NFU) policy - promising not to use nuclear weapons as a means of warfare unless first attacked by another adversary using nuclear weapons.

The NFU policy also prohibits China from dropping weapons of mass destruction on countries not equipped with nuclear weapons.

By contrast, NATO has rejected calls to adopt an NFU policy under the argument that a 'pre-emptive nuclear strike' is a key option.

Japan does not own any nuclear weapons of its own but supports the potential use of US nuclear weapons on its behalf.

The video continues to put forward what it calls the "Japan exception theory" which would scrap China's NFU policy and make Japan the 'exception' to the rule.

The video states that since the signing of the NFU, the international situation has changed dramatically.

It states: "Our country is in the midst of a major change that has not been seen in a century and all political policies, tactics and strategies must be adjusted and changed in order to protect the peaceful rise of our country.

"If Japan goes to war with China for a third time, the Chinese people will take revenge on the old and new scores.

"Japan is the only country in the world that has been hit by atomic bombs and has a deep memory of the atomic bombs from the government down to the people.

"It is exactly because Japan has such a unique feeling that nuclear deterrence against Japan will get twice the result with half the effort."

The video concludes by pledging to punish Japan Prime Minister Yoshihide Suga, former Prime Minister Abe Shinzo, and Deputy Prime Minister Aso Taro - and to retake the Diaoyu and Ryukyu islands.

The CCP authority repost comes just weeks after Chinese president Xi Jinping warned foreign nations will "get their heads bashed bloody" if they attempt to interfere with China.

North Korea uranium enrichment continued at Yongbyon with expansion, analyst says

By Elizabeth Shim

Source: https://www.upi.com/Top_News/World-News/2021/07/19/nkorea-North-Korean-uranium-enrichment-Yongbyon/1241626711943/

North Korea began building a "large enrichment hall" at its Yongbyon nuclear facility after 2009, according to former IAEA official Olli Heinonen. File Photo by Siegfried C. Hecker/UPI

July 19 – A former official of the International Atomic Energy Agency said that it is likely North Korea had produced 540 kilograms, or 1,190 pounds, of highly enriched uranium at its Yongbyon nuclear facility by the end of 2020.

Olli Heinonen, former IAEA deputy director general, said in an analysis recently published to 38 North that the production of weapons-grade uranium has become the foundation of North Korea's "ability to produce fissile material for nuclear weapons."

Heinonen said North Korea's Uranium Enrichment Plant at Yongbyon was first made known in 2010, then expanded in 2013 to 2014, "gradually increasing capacity as the installation of necessary infrastructure proceeded."

North Korea began building a "large enrichment hall" after IAEA inspectors were expelled in April 2009 from Yongbyon. Yongbyon's blue-roofed "Hall 1" was built that summer, the analyst said.

Pyongyang continued to expand facilities after 2009. Satellite imagery from June 2013 shows that North Korea built "Hall 2," similar in size to Hall 1.

Members of a U.S. team from Stanford University led by Siegfried Hecker were told in 2010 that Hall 1 could contain 2,000 centrifuges for uranium enrichment, according to Heinonen.

After the expansion, North Korea by the end of 2020 could have in theory produced up to 705 kilograms, or about 1,550 pounds, of highly enriched uranium. But the analyst said the "facility may not have been operating with its estimated full capacity," and actual production may have been closer to 540 kilograms by the end of last year.

"Since the North's 5-megawatt reactor has not run since 2018 and the [Experimental Light Water Reactor] is still unfinished, the Uranium Enrichment Plant appears to now serve as the backbone of the country's fissile material production program," the analyst said.
IAEA chief Rafael Grossi said in June North Korea's nuclear facilities are active, including a facility at Kangson designed to produce Uranium-235.

***Elizabeth Shim**, a native of Seoul, is UPI's chief Asia writer, based in New York. She is an alumnus of the Center for Strategic and International Studies' U.S.-Korea NextGen Scholars Program and a contributor to the upcoming book "Media Technologies for Work and Play in East Asia" (Bristol University Press, 2021).*

Tagged snakes reveal radiation levels in the soil around Fukushima

Source: https://newatlas.com/environment/tagged-snakes-radiation-levels-fukushima/

July 21 – As work continues to clean up the mess left by the meltdown of Fukushima Daiichi Nuclear Power Plant in 2011, scientists are enlisting some local help in their efforts to survey the damage. A study has shown how snakes living in the Exclusion Zone can be serve as living, breathing monitors of radiation levels in the area, with the help of GPS and VHF tags.

The idea of using snakes to track radiation levels around Fukushima came from a group of researchers at the University of Georgia, who were drawn to a certain species for a few key reasons. The rat snake is an abundant species in Japan, typically traveling short distances and tends to accumulate high levels of radionuclides. This limited range of mobility, constant close contact with the soil and tendency to absorb radioactive material make them a useful "bioindicator" of residual contamination in the area.

"Snakes are good indicators of environmental contamination because they spend a lot of time in and on soil," says study author James C. Beasley. "They have small home ranges and are major predators in most ecosystems, and they're often relatively long-lived species."

The team captured nine rat snakes and applied tape around their bodies, using superglue to then attach the GPS and VHF transmitters on top, allowing them to be easily removed afterwards. The animals were tracked as they slithered throughout the Exclusion Zone, though most didn't move far, with each moving an average of just 65 m (213 ft) a day.

The scientists identified 1,718 different locations in total as they tracked the snakes for over a month. Their analysis showed that the **rat snakes** (*Elaphe* spp.) could act as useful bioindicators of contamination, as they found a strong correlation between levels of radio-cesium in the creatures and levels of radiation in the patches of soil that they frequented.

"Our results indicate that animal behavior has a large impact on radiation exposure and contaminant accumulation," says study author Hanna Gerke. "Studying how specific animals use contaminated landscapes helps increase our understanding of the environmental impacts of huge nuclear accidents such as Fukushima and Chernobyl."

▶▶ **The research was published in the journal** *Ichthyology & Herpetology*.

EDITOR'S COMMENT: It would be nice to know the radiation levels measured – or not?

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

EXPLOSIVE NEWS

France: A 500-kilogram bomb from World War II was defused by the authorities

Source: https://www.athina984.gr/en/2021/07/04/gallia-mia-vomva-500-kilon-apo-ton-v-pagkosmio-polemo-exoydeterosan-oi-arches/

July 04 – In a large operation in which 1.800 people were evacuated from their homes, French authorities today defused a 500-kilogram World War II bomb near Saint-Etienne in southeastern France.

The bomb, dropped by the British Air Force in March 1944 during the destruction of factories located in the small town of La Ricamari used by German forces, was discovered in April 2020, during earthworks.

As it was not a danger to the residents, the bomb had been buried under three meters of soil by the Lyon demining service, pending its neutralization today and its transfer to a place in northern France.

Hundreds of people took part in the operation, including 130 police officers who set out to secure the perimeter, with the operation being monitored by cameras and a drone, Thomas Mison, secretary general of the Loire department, told AFP.

Al-Qaeda Urges Acquisition of Ghost Guns in Review of Boulder Mass Shooting

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/al-qaeda-urges-acquisition-of-ghost-guns-in-review-of-boulder-mass-shooting/

July 06 – Al-Qaeda in the Arabian Peninsula said the Boulder supermarket mass shooting underscored the ease with which potential shooters can acquire guns and told would-be jihadists to not start with simpler knife or vehicle attacks "until you search for these weapons and use them in your operation."

The *Inspire* "Praise & Guide: Colorado Attack" follows a previously seen AQAP model of using the name of the longtime how-to English-language magazine geared toward Western jihadists to review recent attacks and assess what was done well by the attacker and what could have been done to inflict more harm. In the Boulder attack, al-Qaeda praised the shooter's choice of weapon and target while saying attackers shouldn't be taken alive and should issue statements before or during attacks to erase ambiguity about motive.

Ahmad Al-Aliwi Al-Issa, 21, used a Ruger AR-556 in the March 22 shooting at King Soopers' grocery store in Boulder, Colo.; authorities have not ascribed a terror motive to the attack. He fatally shot two people in the parking lot, two at the store's entrance, and killed five more people inside the store before shooting his final victim, responding Boulder Police Officer Eric Talley.

Al-Issa appeared in court May 25 on 115 charges including 10 counts of first-degree murder and 47 counts of attempted murder. His next hearing is scheduled for Sept. 7. Al-Issa's defense attorney said in March that time would be needed to evaluate his mental health.

At the time of the shooting, Al-Issa's social media included many photos from his school wrestling competitions, many posts about the Ultimate Fighting Championship, one post declaring he needed a girlfriend and one who was "hopefully not a hoe," and a few anti-LGBT and anti-abortion posts. The Inspire issue seized on "several Islamic posts" within his social media history including one stating "Muslims may not be perfect, but Islam is," and a post "in which he was criticizing the authorities for not doing anything to prevent the spread of the gatherings of the homosexuals."

AQAP said the mass shooting served to increase "the division between the American people, between the right and the left" due to the white victims at the supermarket and due to how it "raised the matter of the spread of weapons in America." After including some stats about gun violence in America, the issue adds that "just as Allah Almighty has afflicted them with Corona He has also afflicted them with these conflicts amongst them."

The terror group praised Al-Issa for picking an easy-to-use and accurate firearm, for choosing "a place where people gather, which can bring about the largest number of deaths" during a "time in which people gather to take the Corona vaccination," and for not drawing enough suspicion to himself before the attack in a way that derailed his plot.

Al-Qaeda urged attackers to pick targets where crowds would have difficultly hiding or escaping, and to "take your precautions in terms of ammunition" to fight until death with police — unlike the Boulder shooting, which ended with Al-Issa's arrest. Would-be attackers were also urged to make their attacks more explosive by using IED recipes from past *Inspire* issues, Molotov cocktails, "or by taking matches, a lighter and an inflammable material at the very least to burn the place, as this greatly intensifies and multiplies the impact of the operation on the enemy, whether from an economic, psychological or media point of view."

"Take advantage of the presence of weapons and their spread in America to be able to possess them and to carry out Jihadi operation using them," the magazine continues, next to a collage of images from gun stores including a storefront in Fuquay-Varina, N.C. "The possibility to place restrictions on the possession of weapons in America or to reduce their spread is extremely far and difficult. And all that you need is to search the internet and in arms shops for what is legally required of you to possess a weapon and how to buy it. And let the weapon be a machine gun, and if you find an obstacle for this, all you must do is look for ways to obtain stealth weapons by purchasing ready-made weapon parts and then assembling and installing them manually by yourself, and this method has two advantages: The first advantage: The control over it is less and the ways to obtain it are easier. The second advantage: The weapon will be without a serial number."

The magazine includes an image of parts on a table, labeled "ghost gun."

If still hampered by trying to buy or make a gun, al-Qaeda encourages lone attackers to "try to buy weapons through the black market, as well as through offers in free sales and advertisements on the internet and elsewhere, because this market is beyond the reach of the regime." The magazine shows a Black Friday ad from a gun shop in Auxvasse, Mo., adding that "what needs to be understood is that weapons are very widely spread in America and there are more than 390 million weapons."

"There is nothing easier in America than obtaining weapons, and therefore do not begin carrying out operations involving stabbing with knives and running over with cars until you search for these weapons and use them in your operation," the terror group added.

Complaining that a lack of explicit credit for attacks has led to assigned motives "such as psychological illness or being discontent with the status they are in," al-Qaeda includes a lengthy section on how lone jihadists should "give out a media message" before or during the attack — such as livestreaming the attack, contacting media directly, posting on social media using one's real name, or shouting "at the time of carrying out the operation in a loud voice that everyone can hear" — in order to inspire others, "as it multiplies the results."

AQAP has previously used attacks in the United States as teaching tools, releasing a special edition of *Inspire* after the June 2016 mass shooting in which 49 people were killed at the Pulse nightclub in Orlando, Fla. Gunman Omar Mateen pledged allegiance to ISIS in a 911 call, but al-Qaeda stressed that the act was more important than who took credit for it. Mateen "capitalized on the means available at his reach" and inspired "every new lone mujahid [to] try to do his best to realize and attain similar or more fatalities in his operation…especially when they see how easy it is to execute an operation," the issue said, classifying the shooting as "targeting general gatherings" and "sending a message to the public that elects, supports and pays taxes to their criminal governments."

After the September 2016 bombings targeting locations in New Jersey and New York's Chelsea neighborhood, along with a stabbing attack at a St. Cloud, Minn., mall, AQAP released a special *Inspire* edition titled "The 9/17 Operations" that praised the attacks as an "exceptional success" for achieving a goal of "reviving fear and terror at a time when

successive American administrations lie to their people, convincing them that they have crushed 'terrorist' groups and disrupted their capabilities and therefore the American citizens live in a peace, safe and stable life."
However, the terror group criticized some tactical details such as the use of a timer on the bomb targeting a Seaside Park, N.J., race that ultimately was delayed — thus the pipe bomb in the trash can didn't cause any injuries when it detonated. "In this case, we prefer the use of a remote control detonator as used by the Tsarnaev brothers in the Boston Marathon," al-Qaeda said, also criticizing the pressure-cooker bomb that exploded in a Chelsea dumpster — 31 people were injured in the blast, but the terror group noted that "people pass by quickly besides garbage containers and they don't normally stand beside them" so it would have been "better to put the bomb in a place where people are gathering and standing around it, such as a shopping center."

Bridget Johnson *is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill.*

Landmine-sniffing rat continues legacy of fallen hero

Source: https://www.bbc.com/news/uk-england-somerset-57866990

Howes, the mine-sniffing rat works in Cambodia for the British landmine charity the Mines Advisory Group (MAG)

July 18 – A rat named in memory of a landmine clearance expert and former British soldier is continuing his work 25 years after his murder.
The landmine-sniffing rat Howes has just started her new job clearing the deadly legacy of conflict in Cambodia.
Christopher Howes from Backwell, North Somerset and his colleague Houn Hourth were killed by the Khmer Rouge in 1996.
The idea to name the rat came from two of Howes' old school friends after they visited Cambodia to honour his work.
Christopher, 36, and his interpreter Houn were working in Cambodia with the Nobel Peace Prize-winning British landmine charity the Mines Advisory Group (MAG).
They were kidnapped along with their team on 26 March 1996.
Christopher and Houn successfully urged the release of the team offering to stay with their captors to secure their colleagues' freedom.
Both men were murdered days later by Khmer Rouge guerrillas.

Christopher had previously served with the Royal Engineers for seven years and was posthumously awarded the Queen's Gallantry Medal in 2001.

His sister Pat Phillips said: "He was passionate about the landmine cause.

"He always assured us he was careful at his job and wouldn't be hurt, but murder was another thing."

The African giant pouched rats are trained to detect a chemical compound within the explosives, meaning they ignore scrap metal and can search for mines more quickly.

Once they find an explosive they scratch the top to alert their human co-workers.

MAG's Cambodia country director Alexey Kruk said: "Chris and Houn were killed while carrying out their life-saving work freeing communities from the fear of landmines."

"They were selfless and brave, we remember them as heroes."

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

CYBER NEWS

C2BRNE DIARY

How to protect critical infrastructure from ransomware attacks

By Sejal Jhawer and Gregory Falco

Source: https://thebulletin.org/2021/06/how-to-protect-critical-infrastructure-from-ransomware-attacks/

June 25 – Whether the targets are local governments, hospital systems, or gas pipelines, ransomware attacks in which hackers lock down a computer network and demand money are a growing threat to critical infrastructure. The attack on Colonial Pipeline, a major supplier of fuel on the East Coast of the United States, is just one of the latest examples—there will likely be many more. Yet the federal government has so far failed to protect these organizations from the cyberattacks, and even its actions since May, when Colonial Pipeline was attacked, fall short of what's necessary.

A screenshot of the Petya ransomware that began spreading in 2016. In recent years, ransomware attacks have wrought havoc on important digital infrastructure, like gas pipelines and city governments. Typically, affected users are asked to pay their attackers to regain access to their systems. Image via Wikimedia Commons.

The pipeline attack crystalized how cyber threats can affect the physical world. Not knowing how deep the ransomware had infiltrated its computer network last month, Colonial Pipeline halted its operational pipelines for five days before paying a Russian group called DarkSide a ransom of $4.4 million. Meanwhile, East Coasters raced to gas stations in panic as fuel hoarders drained the stations of their supplies. The news was full of alarming scenes of long lines at the pump and even of fuel-laden vehicles catching fire.

In the aftermath of Colonial Pipeline, President Joe Biden issued an executive order that requires federal information technology contractors to provide information about breaches, improved standards on federal networks, and more. While the order deals with federal networks, the hope is that new practices affect the private sector, as well. Most important, the order outlines the federal government's intent to move towards a so-called "zero trust" network architecture—a setup where all users are continuously authenticated and validated before receiving access to any application on the network. But rather than merely recommending zero-trust systems, the government needs to actually require it.

The zero-trust model

A zero-trust network assumes that all data and all users are suspect and could compromise the security of the network—even after they are already inside it. User identities are continuously authenticated (confirmed) and validated. Zero-trust security often employs a number of strategies, most commonly including frequent multi-factor authentication (such as two-factor authentication) and micro-segmentation of the network and data (in which users can only access certain security zones and must authenticate their identity at multiple steps). This represents a departure from the previous model of network security known as "castle-and-moat," in which users are verified once, but granted unrestricted access to resources once inside the network. Though difficult to initially penetrate, such castle-and-moat paradigms—most traditionally, remote data access through corporate virtual private networks (VPNs)—allow an attacker who has breached the network's security to wreak full havoc once inside with minimal to no further identity verifications. In this sense, a zero-trust model is a step in the right direction towards defensible security.

However, the federal government says no more than the following on the subject of zero trust: "To facilitate this approach, the migration to cloud technology shall adopt zero-trust architecture, as practicable." The statement is vague and non-prescriptive. Since zero trust is fundamentally a security principle, it could be developed in a number of ways through a number of different strategies; the phrase "zero trust" does not actually define how such a system is implemented. The federal government must formulate how such networks should be built.

The software-defined network

One method of defining zero-trust implementations is to specify how data should be treated in the network, an approach directly aligned with what's known as software-defined networks. These networks enable administrators to define policies—or rules—through software that control the network and data flow to enhance security. As opposed to traditional, hardware-based networking paradigms, software-defined networks allow network administrators greater control and visibility into the network. Data is sent over networks in small segments called "packets."

Like an envelope containing a letter, network packets also possess labels called "metadata" that convey information about the packet's content, such as the network protocol used or the originating IP address of the data. Software-defined networks can read a packet's metadata. This ultimately allows the network administrators to create policies and make decisions based on incoming packets' metadata about how different packets should be routed —or whether one should be removed from the network.
Software-defined networks and their ability to create security policies at the fine-grained, software level can serve as the means to define and enforce zero-trust security policies. Such a zero-trust approach can ensure all users are authenticated and authorized in their requests, and if Colonial Pipeline had implemented a software-defined network, it could have prevented the ransomware from propagating throughout their systems, as the network would not have properly authenticated the software. No such measures were in place.
As with any technology, there are, of course, risks associated with software-defined networks. One need look no further than Russia to see how software policies that actively engage with data on a network could enable authoritarian regimes to control users' access to content information. A national-scale network with draconian policies about what can pass through the network and what cannot would enable the interception of user data. Because software-defined networks can provide heightened, fine-grained control over what different users can access, national-scale software-defined networks in the hands of authoritarian governments enable censorship, which is why we propose that these systems should only be implemented on US critical infrastructure system networks that have one purpose only—to make sure the critical infrastructure operates as intended.

What the government should (and should not) do now
The US government should require critical infrastructure organizations to enforce zero-trust policies by using a software-defined network. It is only with such a prescriptive measure that we can substantially move the needle on improving critical infrastructure cybersecurity.
The Colonial Pipeline incident revealed how the cybersecurity for critical infrastructure organizations is largely managed by companies themselves. Pipelines could turn down federal reviews. They weren't obligated to fix known issues. That needs to change. Requiring the implementation of software-defined networks in accordance with zero-trust security paradigms would be an important step in that direction.
We do not see (or recommend) that the United States set up a software-defined network enforcing zero trust at the national level anytime soon. (This would require an amazing amount of coordination—at a minimum it would necessitate private sector companies transferring partial operations to federally operated infrastructure.) Such a shift towards national control over all networks would likely upend the public's trust in private companies as all companies would become dependent on federally controlled assets. Some companies see their network security as a competitive advantage and should the government take over networks, their investment would be wiped out. Critical infrastructure, however, certainly would benefit from software-defined networks, even if the government doesn't mandate them.
DarkSide eventually returned access of Colonial Pipeline's network to the company, which re-started its operations just days before the hack might have caused serious problems. But the company wasn't able to entirely restore its data. Though the Justice Department recently seized $2.3 million of the ransom payment from DarkSide, the attack will likely cost the company tens of millions of dollars over the next few months as it repairs its networks. The Colonial Pipeline attack wasn't as bad as it could have been. Will the same be true next time?

Sejal Jhawer *is a senior at Stanford University from Long Island, NY. She majored in computer science, with a minor in Ethics & Technology, and studied under Professor Gregory Falco.*
Dr. Gregory Falco *is a security researcher at Stanford University's Freeman Spogli Institute, an incoming Assistant Professor at Johns Hopkins University's Department of Civil & Systems Engineering and the Institute for Assured Autonomy and an NSF-Fulbright Scholar in Critical Infrastructure Cybersecurity in Iceland. His research is on space system and critical infrastructure cybersecurity and resilience.*

The Internet of Things and The Internet of Everything: What's the Difference?

Source: https://www.salesforce.com/eu/blog/2020/01/evolution-of-the-internet-of-things-and-internet-of-everything.html

The evolution of the global internet has resulted in virtual connections that affect real-world objects and activities. Everything is connected to everything else, creating a distributed ecosystem that reaches far beyond the interconnectivity of things. This is known as the Internet of Everything.

Though the Internet of Everything arose from the Internet of Things, it has become a dynamically evolving phenomenon that is poised to disrupt the business world.

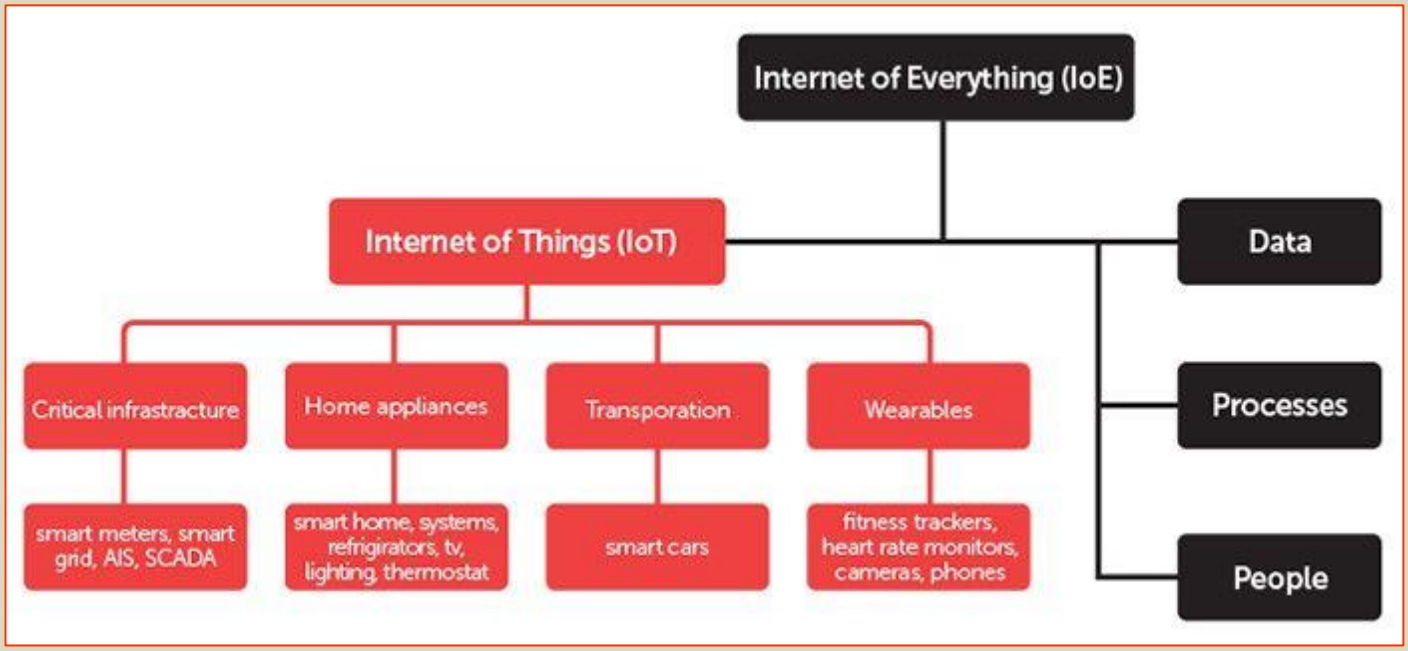
What is the Internet of Things?

Although the term was coined back in 1999, the Internet of Things has undergone a dramatic transformation in the past 20 years. Just a few decades ago, people were connected to each other and the world through landline telephones, televisions and radios, which offer a limited and one-way experience. You could listen and watch, but no interaction with a television or radio.

Home computers ushered in changes that connected people through dial-up internet and a now-antiquated infrastructure. Eventually, DSL replaced dial-up, landlines gave way to mobile phones, and then smartphones, and desktops were replaced by laptops and tablets.

Now, nearly everyone in the developed world is connected to the internet through one or more devices. Eventually, internet connectivity moved beyond devices designed for the internet, such as mobile phones, to objects like vehicles, watches, washing machines and healthcare monitors.

Known as the Internet of Things, the interconnectivity of all these internet-enabled devices opened up a world of possibilities. With embedded technology, the devices can communicate with each other or the internet, and connected devices in automated systems can gather information and analyse it to help organisations gain insights for actionable results.



What is the Internet of Everything?

The Internet of Everything is based on the idea of all-around connectivity, intelligence and cognition. Unlike computerised devices that rely on intelligent internet connections, any object can be fitted with digital features and connected to a network of other objects, people and processes, with the goal of converting information into actions for new capabilities and experiences.

The Internet of Everything's pillars are:

- **Decentralisation**: Data is processed in numerous distributed nodes, and not within a central system.
- **Data input and output**: External data can be stored on devices and returned to other components within the network.
- **Connection to every technology in digital transformation**: The Internet of Everything connects to cloud computing, artificial intelligence, big data, the Internet of Things, machine learning and other vital future technologies.

The constituent elements of the Internet of Everything are:

- **People**: People offer personal insights through connected devices, such as healthcare sensors and social media, and artificial intelligence, and other technologies analyse the data to discover insights about human concerns and deliver personalised content that's relevant to their needs.
- **Things**: Things encompass the Internet of Things or the physical objects with sensors that generate data and transfer it through the network.

- **Data**: Data from devices is raw, but once aggregated and analysed it can be used for actionable decisions and intelligent solutions.
- **Processes**: Processes are based on other current technology, such as social networking, machine learning and artificial intelligence to provide relevant information to a particular person. In this way, the Internet of Everything maximises the potential of big data.

The primary components of the Internet of Everything are hardware, software and services.

Internet of Things vs Internet of Everything

Though they're often intertwined and some aspects of their evolution occurred together, it's important to understand the differences between the Internet of Things and the Internet of Everything.

The primary difference between the Internet of Things and the Internet of Everything are the pillars for the concepts:

- *The Internet of Things* focuses on physical objects.
- *The Internet of Everything* focuses on four constituents: people, things, data and processes.

Simply put, the Internet of Things involves the interconnectivity of physical objects and data input and output, while the Internet of Everything is a comprehensive term that refers to the interconnectivity of various technologies, processes and people.

Despite these differences, they share some similarities:

- **Decentralisation**: Both are distributed and don't operate within a centralised system, giving them independence.
- **Security**: Distributed systems are vulnerable to cyberattacks and breaches, though decentralisation ensures that the entire system and its connected devices aren't compromised if problems occur in specific areas.

Examples of the Internet of Things and the Internet of Everything

Marketing Cloud is integrated with Honeycomb, Centrica Connected Home's custom IoT platform, which provides a range of insights into customer journeys and behaviours

The Internet of Things has become a part of our daily lives. It includes connected and 'smart' devices, such as:

- Vehicle telematics
- Voice-controlled home assistants
- Fitness trackers
- Air-quality monitors

The Internet of Everything expands on these common uses and offers applications for every industry. Here are some examples:

- Manufacturing can use sensors for predictive maintenance and equipment monitoring to reduce downtime and costs from inefficiencies.
- Municipalities can use smart meters for electricity and water monitoring in residential and commercial buildings to monitor usage and look for ways to reduce costs.
- Logistics companies can use sensors and devices on delivery trucks to optimise delivery schedules and routes for cost reduction and customer satisfaction.

Looking to the future

The capabilities and applications for both the Internet of Things and the Internet of Everything are growing, with both moving toward full interconnectivity. As we move toward this new future and its dramatic changes to business processes, we can expect improved products and services that better serve the interests of both stakeholders and consumers.

When Does a 'Cyber Attack' Demand Retaliation? NATO Broadens Its View

By Stefan Soesanto

Source: https://www.defenseone.com/ideas/2021/06/when-does-cyber-attack-demand-retaliation-nato-broadens-its-view/175028/

June 30 – In the 14 years since NATO first declared that a "cyber attack" could amount to an assault requiring collective action, alliance members have never made it quite clear what would constitute such an attack. But now they appear to be broadening the still-hazy definition.

Since the Wales Summit of 2014, analysts have largely worked under the assumption that a cyberattack would have to be as destructive as a kinetic attack to reach the legal threshold that would trigger defensive actions. This view was reinforced throughout the years by

NATO's use of the grammatical singular, i.e., "a cyberattack," and the equivalency drawn between a kinetic attack and the effects and scale of a cyberattack.

At the Cyber Defense Pledge Conference in 2018, for example, NATO Secretary General Stoltenberg said, "NATO leaders agreed that a cyber-attack could trigger Article 5 of our founding treaty. Where an attack on one Ally is treated as an attack on all Allies." As recently as June 7, Stoltenberg told the Atlantic Council: "In a way it sends a message that a kinetic attack can of course cause a lot of damage, and so can of course a cyberattack. It does not matter whether it is a kinetic attack or a cyberattack. We will assess as allies when it meets the threshold for triggering Article 5."

With the publication of the NATO Brussels Summit Communique on June 14, the alliance fundamentally re-conceptualized how and what kind of adversarial activities can lead to crossing the threshold of an armed attack. The most important change: the insertion of the word "cumulative."

According to paragraph 32 of the Communique, allies now recognize that "the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack." Asked to clarify the insertion of the term 'cumulative,' the NATO press office responded that (a) the term was indeed used deliberately, and (b) the reason for using it is because the alliance has recognized that the cyber threat landscape is evolving, and that several low impact cyber incidents by the same threat actor can have the same impact as a single destructive cyberattack. The Estonian Ministry of Defense added via email that "it is paramount that we would also take into account long-term cyber operations and attacks that might cause cumulative damage equal to what a single cyber-attack could cause."

The Communique itself still battles with the grammatical singular of "a cyberattack," saying, "We reaffirm that a decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis." But gone is the sole equivalence to a kinetic attack. In addition, the alliance now also recognizes the impacts of "ransomware incidents and other malicious cyber activity targeting our critical infrastructure and democratic institutions, which might have systemic effects and cause significant harm."

This means that NATO is finally inching away from cyberattacks as the metric of choice, and will hopefully move toward the more relevant unit of cumulative cyber activities – or in other words adversarial cyber campaigns. It is also positive to see that the threat of ransomware is receiving recognition as a security threat within the alliance. And it is good that NATO starts considering systemic effects resulting from malicious cyber activities – of which some might occur outside the alliance's geographic area of responsibility. The 2012 attack against Saudi Aramco for example, could have posed a systemic threat to the majority of alliance members if oil and gas shipments were severely disrupted over a longer period of time.

But it remains unclear how NATO's "cumulative" approach will work. What falls into this accumulation? Non-state ransomware campaigns? Non-destructive state-sponsored cyber espionage activity? And do these adversarial cyber activities have to occur in parallel, within a limited time, or are they continuously accumulated?

NATO's press office has said the move toward "cumulative cyber activities" should not be seen as lowering the threshold for triggering Article 5, because (a) there is no clearly defined threshold to begin with due to NATO's strategic ambiguity, and (b) triggering Article 5 will be discussed by the alliance members on a case-by-case basis – meaning ultimately it is a political decision. This argumentation is of course debatable and hinges upon how member states will calculate cumulative cyber activities and which member state will push for a precedent.

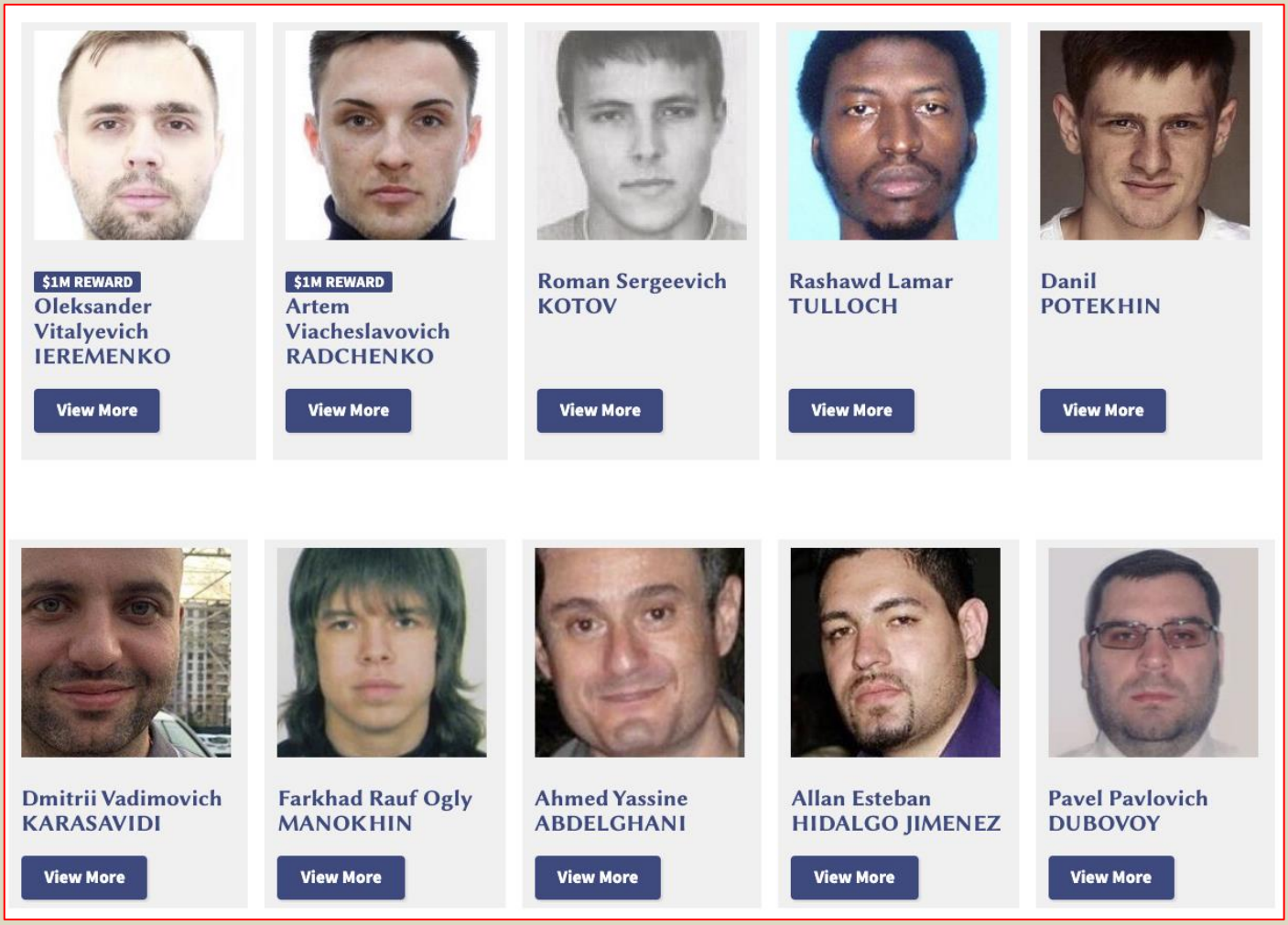
Notably, the French Ministry of Defense and the UK government support the "accumulation of events" theory in their respective statements on international law applicable to cyberspace. The UK government states that adversarial cyber activities that "cease almost instantaneously or within a short timeframe" may nevertheless be part of "a wider pattern of cyber activities [that] might collectively constitute an internationally wrongful act justifying a response." The French Ministry of Defense interprets international law similarly by arguing that cyberattacks which in isolation do not reach the threshold for an armed attack could qualify as such if the accumulation of their effects reaches a threshold of sufficient severity, or if they are carried out concurrently to operations in the physical domain that constitute an armed attack by the same entity or different entities acting in concert. It remains unclear why the other 28 NATO members agreed to include the accumulation of events theory into the Brussels Communique, and what their individual interpretation of the word 'cumulative' actually is.

Time will tell how the alliance members will posture themselves in practice. Some members might be seizing the opportunity to drive the discussion deeper by bringing up preemptive or preventative self-defense in and through cyberspace. Others might entirely ignore the word "cumulative" due to their very different interpretations of international law applicable to cyberspace. And finally, it is inherently unclear whether adversaries understand this change in the alliance's posture, whether they care enough, and whether they should take it seriously. NATO leaders should recognize the need for clearer statements on the matter.

***Stefan Soesanto** is a Senior Researcher in the Cyber Defense Team at the Center for Security Studies (CSS) at the ETH Zurich.*

Secret Service Launches Most Wanted Cyber Fugitives Page

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/secret-service-launches-most-wanted-cyber-fugitives-page/



July 06 – The U.S. Secret Service relaunched its Most Wanted Fugitives page on the agency's website. Featuring the latest available information on these wanted fugitives, the website encourages the public to submit any relevant information they may have to mostwanted@usss.dhs.gov.

The Secret Service has a long and storied history of safeguarding America's financial and payment systems from criminal exploitation. The agency was created in 1865 to combat the rise of counterfeit currency following the Civil War. As the U.S. financial system has evolved – from paper currency to plastic credit cards to digital information – so too have the Secret Service's investigative responsibilities.

Cybercrime remains an enduring threat to the security of the nation's financial infrastructure. Cybercriminals quickly shift their activity based on emerging opportunities to steal and launder funds using any tactics, techniques and procedures available to them.

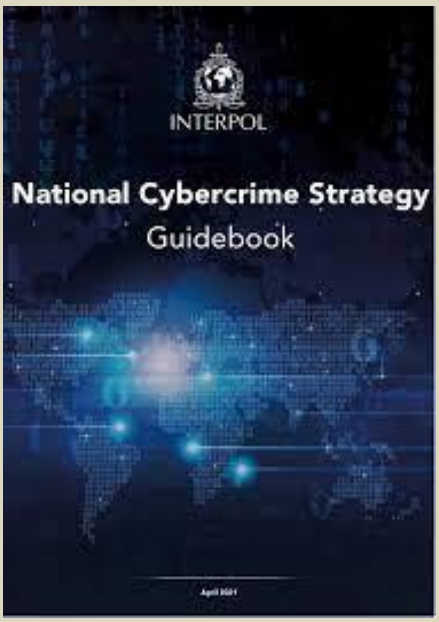
To address this continued shift in criminality, the Secret Service operates a network of Cyber Fraud Task Forces (CFTF), a public-private partnership with law enforcement agencies at every level, prosecutors, the private sector and academia. The mission of the Secret Service CFTFs is to prevent, detect and mitigate complex cyber-enabled financial crimes, with the ultimate goal of arresting and convicting the most harmful perpetrators.

INTERPOL Offers National Cybercrime Strategy Guidebook

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/interpol-offers-national-cybercrime-strategy-guidebook/

July 06 – INTERPOL's National Cybercrime Strategy Guidebook has been produced as part of phase two of the ASEAN Cyber Capacity Development Project (ACCDP II). The ACCDP is a project that is funded by the Japan-ASEAN Integration Fund (JAIF) 2.0 via the ASEAN

Secretariat and with the Singapore Ministry of Home Affairs as the project proponent. INTERPOL is the implementing agency.
This project aims to strengthen the ability of countries to combat cybercrime and work together as a region and internationally. The ACCDP specifically addresses the need for criminal justice authorities to develop their cyberskills, knowledge and regional partnerships through tailored activities and products. The ACCDP forms part of INTERPOL's global cybercrime response and supports the implementation of its global cybercrime strategy. INTERPOL supports national efforts to combat cybercrime and considers it a global focus area alongside terrorism and organized crime.

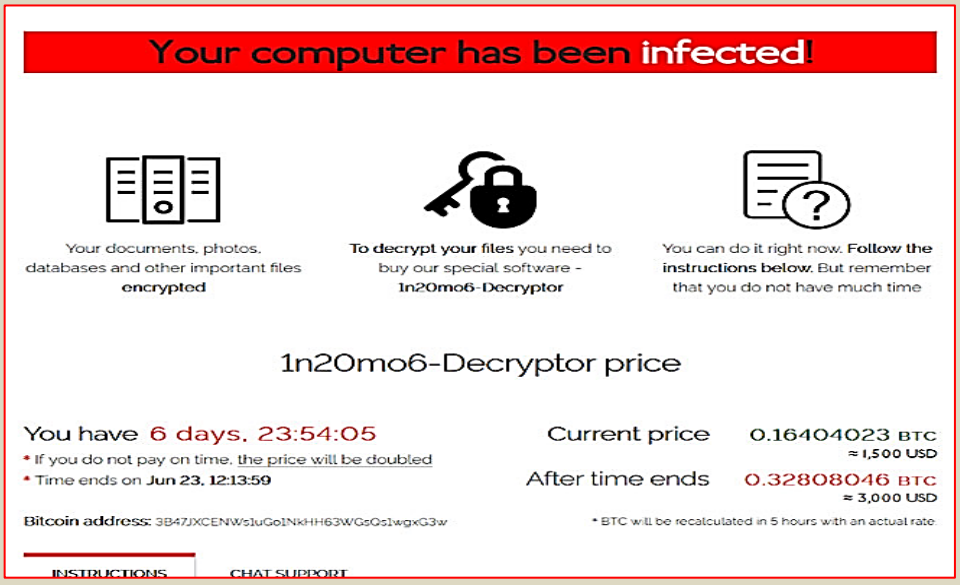


The consolidated findings of in-country assessments (National Cyber Reviews) conducted in the first phase of the ACCDP revealed that there was a clear need in many ASEAN member states (AMS) for a cybercrime strategy. Thus in phase two of ACCDP this Guidebook was developed.
The development of the Guidebook started with a one-week workshop attended by representatives from law enforcement, national cyber agencies and external advisors and continued with the input of various experts from INTERPOL and its member countries.
The information contained in this Guidebook is not tailored to any specific region but instead details identified good practices which are in use internationally.
The Guidebook is designed to be used by any country looking to develop, review or enhance its national cybercrime strategy.
The project observed a significant disparity between the anti-cybercrime initiatives, laws and processes in force in INTERPOL member countries and underlined the importance of more closely aligning them with international good practices.
This Guidebook was created to provide a methodological approach to the potentially challenging task of creating or updating a cybercrime strategy.

▶▶ Download the Guidebook here

The Kaseya Ransomware Attack Is a Really Big Deal

Source: http://www.homelandsecuritynewswire.com/dr20210707-the-kaseya-ransomware-attack-is-a-really-big-deal



July 07 – If you're not already paying attention to the Kaseya ransomware incident, you should be. Matt Tait writes in *Lawfare* that it is likely the most important cybersecurity event of the year. Bigger than the Exchange hacks by China in January. Bigger than the Colonial Pipeline ransomware incident. And, yes, more important than the SolarWinds intrusions last year.
Kaseya is a managed service provider; its customers use Kaseya to manage their company information technology (IT) infrastructure. As part of this task, Kaseya can deploy software to the systems under management – Tait says that, in a way, that is broadly equivalent to a software provider deploying an automatic update to those machines.

Under normal circumstances, automatic software deployment, especially in the context of software updates, is a good thing. But here this feature was turned on its head. Russian-based criminal gang REvil hacked into Kaseya's management system and pushed REvil software to all of the systems under Kaseya's

management. From there, the ransomware promptly disabled those computers and demanded a cryptocurrency payment of about $45,000 per system to set the machines free. As of writing, REvil claims that about a million total computers were affected and is offering a "bulk discount" of $70 million to unlock all affected systems in a single payment.

The direct impact is already enormous, but, Tait writes, "to me, the direct impact is, in some sense, far less important than the issue of how the incident occurred, namely by subverting software delivery mechanisms as a means to install ransomware."

Tait says that there are three more reasons why we should worry about Kaseya-like attacks:

- ✓ First, supply chain compromises, such as these, are very often *indiscriminate*; everyone who installs a malicious update gets the malware.
- ✓ Second, and perhaps scariest, observation is that the software vendors used in malicious update compromises thus far have, in the grand scheme of things, been relatively small.
- ✓ Third, defensive remediation of ransomware deployed through automatic updates is pathological to the cybersecurity industry itself in a way that is qualitatively different from other categories of cybersecurity incidents.

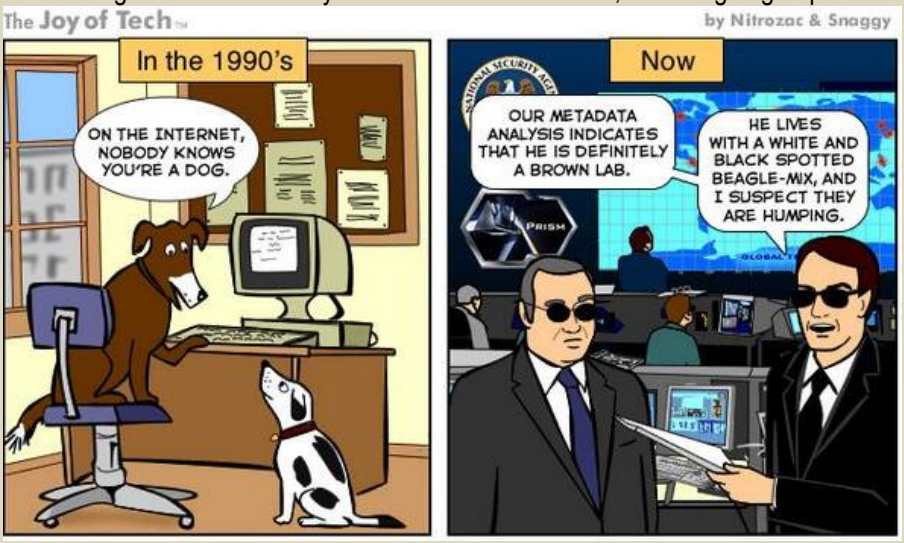
In short, software supply chain security breaches don't look like other categories of breaches. Tackling this problem is no small task, But before researchers and policymakers can start to look for solutions, the first step is recognizing why supply chain compromise is fundamentally different from most other problems encountered day-to-day in cybersecurity, and one with a failure mode that can be unusually fast and large scale. Only then will the information security community be able to start tackling the problem with the scale and seriousness that it deserves.

Holding the World to Ransom: The Top 5 Most Dangerous Criminal Organizations Online Right Now

By Roberto Musotto

Source: http://www.homelandsecuritynewswire.com/dr20210707-holding-the-world-to-ransom-the-top-5-most-dangerous-criminal-organizations-online-right-now

July 07 – Ransomware attacks are growing exponentially in size and ransom demand — changing the way we operate online. Understanding who these groups are and what they want is critical to taking them down. Here, we list the top five most dangerous criminal organizations currently online. As far as we know, these rogue groups aren't backed or sponsored by any state.



On the internet, nobody knows you're a dog!

These words from Peter Steiner's famous cartoon could easily be applied to the recent ransomware attack on Florida-based software supplier Kaseya.

Kaseya provides software services to thousands of clients around the world. It's estimated between 800 and 1,500 medium to small businesses may be impacted by the attack, with the hackers demanding US$50 million (lower than the previously reported US$70 million) in exchange for restoring access to data being held for ransom.

The global ransomware attack has been labelled the biggest on record. Russian cybercriminal organization REvil is the alleged culprit.

Despite its notoriety, nobody really knows what REvil is, what it's capable of or why it does what they does — apart from the immediate benefit of huge sums of money. Also, ransomware attacks often involve vast distributed networks, so it's not even certain the individuals involved would know each other.

Ransomware attacks are growing exponentially in size and ransom demand — changing the way we operate online. Understanding who these groups are and what they want is critical to taking them down.

Here, we list the top five most dangerous criminal organizations currently online. As far as we know, these rogue groups aren't backed or sponsored by any state.

DarkSide

DarkSide is the group behind the Colonial Pipeline ransom attack in May, which shut down the US Colonial Pipeline's fuel distribution network, triggering gasoline shortage concerns.

The group seemingly first emerged in August last year. It targets large companies that will suffer from any disruption to their services — a key factor, as they're then more likely to pay ransom. Such companies are also more likely to have cyber insurance which, for criminals, means easy moneymaking.
DarkSide's business model is to offer a ransomware service. In other words, it carries out ransomware attacks on behalf of other, hidden perpetrator/s so they can lessen their liability. The executor and perpetrator then share profits.
Groups that offer cybercrime-as-a-service also provide online forum communications to support others who may want to improve their cybercrime skills.
This might involve teaching someone how to combine distributed denial-of-service (DDoS) and ransomware attacks, to put extra pressure on negotiations. The ransomware would prevent a business from working on past and current orders, while a DDoS attack would block any new orders.

Revil

The ransomware-as-a-service group REvil is currently making headlines due to the ongoing Kaseya incident, as well as another recent attack on global meat processing company JBS. This group has been particularly active in 2020-2021.
In April, REvil stole technical data on unreleased Apple products from Quanta Computer, a Taiwanese company that assembles Apple laptops. A ransom of US$50 million was demanded to prevent public release of the stolen data. It hasn't been revealed whether or not this money was paid.

Clop

The ransomware Clop was created in 2019 by a financially-motivated group responsible for yielding half a billion US dollars.
The Clop group's specialty is "double-extortion". This involves targeting organizations with ransom money in exchange for a decryption key that will restore the organization's access to stolen data. However, targets will then have to pay extra ransom to not have the data released publicly.
Historical examples reveal that organizations which pay a ransom once are more likely to pay again in the future. So hackers will tend to target the same organizations again and again, asking for more money each time.

Syrian Electronic Army

Far from a typical cybercrime gang, the Syrian Electronic Army has been launching online attacks since 2011 to promote political propaganda. With this motive, they have been dubbed a hactivist group.
While the group has links with Bashar al-Assad's regime, it's more likely made up of online vigilantes trying to be media auxiliary for the Syrian army.
Their technique is to distribute fake news through reputable sources. In 2013, a single tweet sent by them from the official account of the Associated Press, the world's leading news agency, had the effect of wiping billions from the stock market.
The Syrian Electronic Army exploits the fact that most people online have a tendency to interpret and react to content with an implicit sense of trust. And they're a prime example of how the boundaries between crime and terror groups online are less distinct than in the physical world.

FIN7

If this list could contain a "super villain", it would be FIN7. Another Russian-based group, FIN7 is arguably the most successful online criminal organization of all time. Operating since 2012, it mainly works as a business.
Many of its operations have been undetected for years. Its data breaches have exploited cross-attack scenarios, wherein the data breach serves multiple purposes. For example, it may enable extortion through ransom while also allowing the attacker to use data against victims, such as by reselling it to a third party.
In early 2017, FIN7 was alleged to be behind an attack targeting companies providing filings to the US Security and Exchange Commission. This confidential information was exploited and used to obtain ransom which was then invested on the stock exchange. As such, the groups made huge sums of money by trading on confidential information. The insider trading scheme facilitated by hacking went on for many years — which is why it's not possible to quantify the exact amount of economic damage. But it's estimated to be well over US$1 billion.

Organized Crime vs Organized Criminals

When it comes to complex criminal organizations, techniques evolve and motives vary.
The way they organize themselves and commit crimes online is very different from your local offline gang. Ransomware can be launched from anywhere in the world, so it's very difficult

to prosecute these criminals. Matters are made even more complicated when several parties coordinate across borders.
It's no wonder the challenge for law enforcement agencies is significant. It's crucial that authorities investigating an attack are sure it was indeed perpetrated by who they suspect. But to know this, they need all the help they can get.

Roberto Musotto *is Research fellow, Edith Cowan University.*

Journalists, Activists among 50,000 Targets of Israeli Spyware: Reports

Source: http://www.homelandsecuritynewswire.com/dr20210719-journalists-activists-among-50-000-targets-of-israeli-spyware-reports

July 19 – Israeli cyber firm NSO Group claims that its Pegasus surveillance malware is sold to governments so they can better track terrorists and criminals, but many of the 45 governments deploying the surveillance software use it to track journalists, opposition politicians, and civil society activists. Some of these governments are authoritarian (for example, Azerbaijan, Bahrain, Kazakhstan, UAE, Saudi Arabia). Other are democracies (for example, India, Mexico, South Africa). The only EU member country to deploy the surveillance malware is Hungary, which places it in violation of the EU's strict privacy and surveillance regulations.

Macron's Secure Mobile Phone Compromised by Pegasus Spyware

The secure smartphone of French president Emmanuel Macron was compromised by the Pegasus surveillance malware. It was surreptitiously installed by Moroccan intelligence operatives, who introduced the virus into the phones of former Prime Minister Edouard Philippe and fourteen other current and former French cabinet ministers. **Read more**

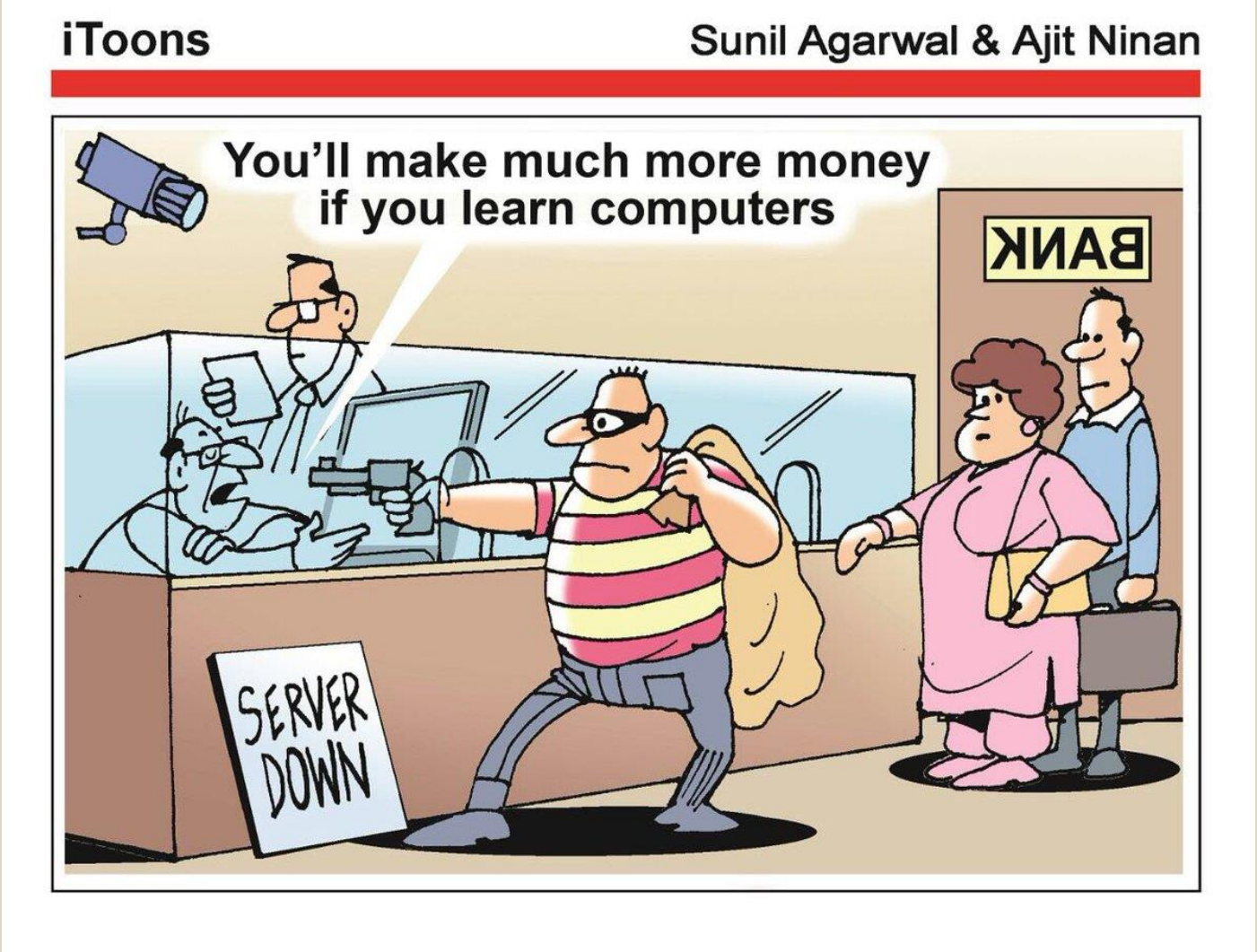
Total Economic Impact of Cybercrime on Australia in 2019 Was $3.5 Billion

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/total-economic-impact-of-cybercrime-on-australia-in-2019-was-3-5-billion/

July 19 – This report estimates the cost of pure cybercrime to individuals in Australia in 2019. A survey was administered to a sample of 11,840 adults drawn from two online panels—one using probability sampling and the other non-probability sampling—with the resulting data weighted to better reflect the distribution of the wider Australian population.

Thirty-four percent of respondents had experienced some form of pure cybercrime, with 14 percent being victimised in the last 12 months. This is equivalent to nearly 6.7 million Australian adults having ever been the victim of pure cybercrime, and 2.8 million Australians being victimised in the past year.
Drawing on these population estimates, the total economic impact of pure cybercrime in 2019 was approximately $3.5b. This encompasses $1.9b in money directly lost by victims, $597m spent dealing with the consequences of victimisation, and $1.4b spent on prevention costs. Victims recovered $389m.

▶▶ Read the report at the Australian Institute of Criminology



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

Developing Drones to Address Pandemic-Related Challenges in Scandinavia

Source: http://www.homelandsecuritynewswire.com/dr20210623-developing-drones-to-address-pandemicrelated-challenges-in-scandinavia

June 23 – The onset of the Covid-19 pandemic spurred an immediate need to develop new, innovative systems in supply chains and infrastructure. And for three Norwegian graduate students enrolled in the MIT Professional Education Advanced Study Program (ASP), spring 2020 was the moment when technology, innovation, and preparation met opportunity.

Lars Erik Matsson Fagernæs, Bernhard Paus Græsdal, and Herman Øie Kolden were all students at the Norwegian University of Science and Technology (NTNU) but only met after they arrived on the MIT campus for their ASP in 2019. Fagernæs came to MIT to study computer science, Græsdal focused on robotics, and Kolden came to study plasma physics, though he had prior experience with drones through a job at a defense contractor.

When the pandemic began in early 2020, Fagernæs, Græsdal, and Kolden were all still in Cambridge, Massachusetts. NTNU would eventually recall them home, but not for a few months. To pass the time, they read news from Norway and identified a problem that they thought they could solve.

Norway is not an easy country to traverse, with roads laid out circuitously around mountains and fjords. Small regional hospitals do not have easy access to the labs and testing facilities at larger university hospitals. "Some local governments don't even test for Covid during weekends because they have issues with transportation," says Fagernæs. "In some parts in the north, you have to drive for 10 or 15 hours just to transport tests to the hospital for analysis."

The friends had already been working on a drone-related project and pivoted to the idea of making a drone to transport biological samples. They chose a fixed-wing quadcopter design that combines vertical takeoff and landing with efficient long-distance travel.

Long-Duration Drones for Medical Delivery

Their prototype drones were built at MIT and tested in the Johnson Athletic Center around its running track. They found inspiration in the work of MIT professors like Russ Tedrake, director of the Center for Robotics at the Computer Science and Artificial Intelligence Laboratory (CSAIL) and a professor of electrical engineering and computer science.

"Bernhard and Lars took my graduate robotics class," Tedrake says. "They were extremely engaged and regularly asked questions that made it clear they were not just listening to the lectures, but were actively experimenting with the ideas. My role was to introduce them to topics in dynamics, control, and optimization, and talk them through the projects, but the innovation and hard work was all theirs!"

In building their drone, Fagernæs, Græsdal, and Kolden had to overcome a number of technical issues, including icing, vibrations, and variable temperatures. Evolving EU drone regulations necessitated building redundant systems and a parachute in case of malfunction. However, the biggest challenge was the distance they needed to fly, 120 kilometers from start to end. **An autonomous flight of that length had never been completed in Scandinavia before**.

"People thought we were crazy," Fagernæs recalls. "But we were lucky enough to speak to the right people at the hospital who were desperate for a solution, and they decided to give us a chance. So, we have been working ever since, day and night."

This past March, the students achieved a proof-of-concept flight, making a 120-kilometer flight in just 80 minutes, cutting hours off ground transport times — all with minimal piloting. They believe this is the longest autonomous drone flight in Scandinavia, strong evidence to support the viability of a much-needed service that will extend far beyond the Covid era.

"The drone has both internal and external sensors, which give you information about the world. Then based on that information, it's able to navigate and fly autonomously," says Græsdal.

Given the number of sensors and automation built into the aircraft, a single pilot could conceivably back up 10 or more drones.

"Because of the current state of regulations, nobody in the world operates fully autonomous drones. It's definitely coming, though," Kolden adds. "We have what's called a 'back-backseat pilot' so if there's a warning then you can take control."

Crediting MIT

In order to develop their technology further, Fagernæs, Græsdal, and Kolden have also launched a startup, Aviant. Publicity from their test flight has already led to interest from their Scandinavian neighbors. "We are now expanding into Sweden," reports Fagernæs. "We are doing two projects in Sweden, helping with all sorts of logistics with drones, because [transportation infrastructure] is a huge problem in Sweden as well."

The trio is effusive about their MIT experience. "We're starting a company, changing Norwegian infrastructure — this never would have happened without MIT," Græsdal says.

"As ASP students, everything at MIT was open to us. We had offices to work in and networking events sponsored by ASP, where we met other students, as well as people from industry," adds Fagernæs.
Fagernæs, Græsdal, and Kolden count Bianca Sinausky, program administrator of ASP, as a personal friend for the guidance she provided throughout their time on the MIT campus, and for her assistance navigating pandemic-related disruption as they returned home and completed their program requirements from Norway.
According to Sinausky, the students were ideal candidates for the program. "The Advanced Study Program offers those with a bachelor degree the opportunity to enroll in MIT classes as a non-degree student, and provides maximum flexibility for working professionals and exceptional graduate students who want to enhance their knowledge and further their careers with an MIT education," she says. "It's gratifying when ASP students like Bernhard, Herman, and Lars Erik meet at MIT through their passion for engineering, technology, and science, and are able to quickly make a positive impact in their home country, and potentially around the world."
Adds Bhaskar Pant, executive director of MIT Professional Education, "the success of these Norwegian students underscores the reason why we consider the Advanced Study Program the 'jewel in the crown' at MIT Professional Education. It is a very special boutique program that allows enrollees to access the full resources of MIT while networking with each other to realize their high aspirations, including building a startup to help meet human challenges during and after a pandemic!"

Anti-Drone Weapons Defending Baiden's Visit to Belgium

Source: https://i-hls.com/archives/109059

June 17 – Anti-drone weapons were carried by security teams during U.S. President Joe Biden's visit to Belgium this week. Images shared to social media show Belgian security forces wielding a combination of handheld anti-drone weapons to protect a meeting between Biden and King Philippe of Belgium. Their deployment is a reminder of how serious the threat of drone attacks on high-value targets is worldwide.
Two different types of anti-drone systems were carried by members of the Belgian Federal Police, one which fires a net projectile at drones, and another that uses radiofrequency (RF) jamming to disrupt links between drones and their operators.
One of the weapons appears to be the **DroneGun Tactical** (right photo) made by the Australian firm DroneShield. According to the company, the system can cause drones to "respond via vertical on the spot landing or return to its remote controller or starting point"

when successfully disrupted by its multi-band radiofrequency (RF) jamming attack. These types of anti-drone weapons work by severing the command and control links between drones and their operators, and can instantly cease video transmission between them. These types of jammers don't work against autonomous systems which do not rely upon RF links with human controllers, although those systems are far less flexible and are usually only capable of targeting fixed points, not fluid targets that are often in motion,
The other weapon seen carried by the Belgian Federal Police appears to be a **Skywall Patrol** (left photo) made by UK-based OpenWorks Engineering. The gun is described by its manufacturers as a "handheld drone capture system" that uses compressed air to fire nets or a combination net-and-parachute round at hostile drones. It is effective in

bringing down drones because "Conventional weapons often fail to incapacitate a drone and do not offer a proportionate response to the drone threat." Further, the company writes, conventional weapons "can also escalate a situation when used in the vicinity of large crowds", according to thedrive.com.

Indian police say bomb-laden drones hit air base in Kashmir

Source: https://apnews.com/article/kashmir-india-religion-5aa73efb693b3a6bda7739dbdba027a3

June 27 — Indian officials said Sunday they suspect explosives-laden drones were used to attack an air base in the disputed region of Kashmir, calling it the first such incident of its kind in India.

Dilbagh Singh, the region's police director-general, told the private news channel New Delhi Television that "drones with payload were used in both the blasts." Singh called the attack an act of terrorism.

Two soldiers were lightly wounded in the explosions, according to a military officer who spoke on condition of anonymity in keeping with military regulations.

India's air force tweeted that the attack caused minor damage to a building on the base, located in the southern city of Jammu in the Indian-controlled portion of Kashmir, while the second blast hit an open area. It said no military equipment was damaged.

The incident, if proven to have been carried out by anti-India rebels, would mark a major shift in strategy against New Delhi. Rebels have primarily used classic guerrilla tactics such as ambushes, hit-and-run attacks, remote-controlled explosions and car bombings.

Lt. Gen. D.S. Hooda, who was head of the Indian military's Northern Command from 2014 to 2016 which covers Kashmir, said Sunday's potential drone strike poses a "huge and serious challenge" for the security apparatus. He said commercial drones are easily available on the market and don't need advanced technology to be used in attacks.

"Drones have a small visual signature and traditional radars hardly pick them up," Hooda said. "It will require a whole range of new modifications for the military to intercept and defuse these kinds of attacks."
Muslim-majority Kashmir is divided between India and Pakistan, and the Himalayan region is claimed by both in its entirety. Rebels have been fighting against Indian rule since 1989. Most Muslim Kashmiris support the rebel goal that the territory be united either under Pakistani rule or as an independent country.
New Delhi deems Kashmir militancy to be Pakistan-sponsored terrorism. Pakistan denies the charge, and most Kashmiris call it a legitimate freedom struggle.
Both countries claim to have shot down spy drones in the parts of Kashmir under their respective control.
The air base in Jammu is also used as a civilian airport, and the Press Trust of India news agency quoted the airport's director, Pravat Ranjan Beuria, as saying there was no disruption to civilian flights.
Indian authorities said forensic investigators were surveying the area, and were later joined by the country's premier anti-terrorism agency, the National Investigating Agency.
Last week, India's Prime Minister Narendra Modi held a crucial meeting with pro-India politicians from Kashmir for the first time since New Delhi stripped the region's semi-autonomy and imposed a slew of administrative changes, which many likened to the beginning of settler colonialism.
Indian authorities in recent years have raised the possibility of drone attacks by rebels in the region, especially after repeatedly accusing Pakistan of using China-made drones along the frontier to drop weapons packages for militant groups since last year.
Tens of thousands of civilians, rebels and government forces have been killed in the conflict.

EDITOR'S COMMENT: The unexpected always happens especially in countries with bad neighbors. This the new face of war and one might make a reasonable hypothesis based on the relationships between certain countries. Always upon solid proofs that a drone (or more) is involved.

How drones became a tool of terror?

Source: https://www.indiatoday.in/india/story/decoded-use-of-drones-for-terrorism-1820245-2021-06-28

The Association of the United States Army (AUSA) in February 2021 published a report titled, The Role of Drones in Future Terrorist Attacks. Here, the AUSA said the Islamic State made the first successful use of drones for terrorism.

It cited a Washington Post article that said, "In August 2014, the terrorist group [Islamic State] began using drones to gather battlefield intelligence and to document the effects of suicide bombings, often broadcasting the videos online to bolster morale, according to the report by MEMRI [Middle East Media Research Institute, a non-profit press monitoring and analysis organisation]."
"Occasionally the group would strap an explosive onto a small drone and try to land it near a military outpost, as it happened in October when a booby-trapped toy aircraft exploded as Kurdish fighters were examining it near the northern Iraqi city of Irbil."
Earlier in 2013, Al-Qaeda attempted a terror attack using multiple drones in Pakistan without success. From 2016 on, the Islamic State made drone attacks a regular feature in its operations in Iraq and Syria.
The threat was so serious that in 2019, European Union Security Commissioner Julian King warned that European cities could be targeted by terror groups using drones.
Besides the Islamic State, the Hezbollah — active in Palestine and Lebanon, the Houthi rebels, the Taliban and several terror outfits in Pakistan are known to employ drones for terrorism.

How serious is the threat of drone attacks from Pakistan?

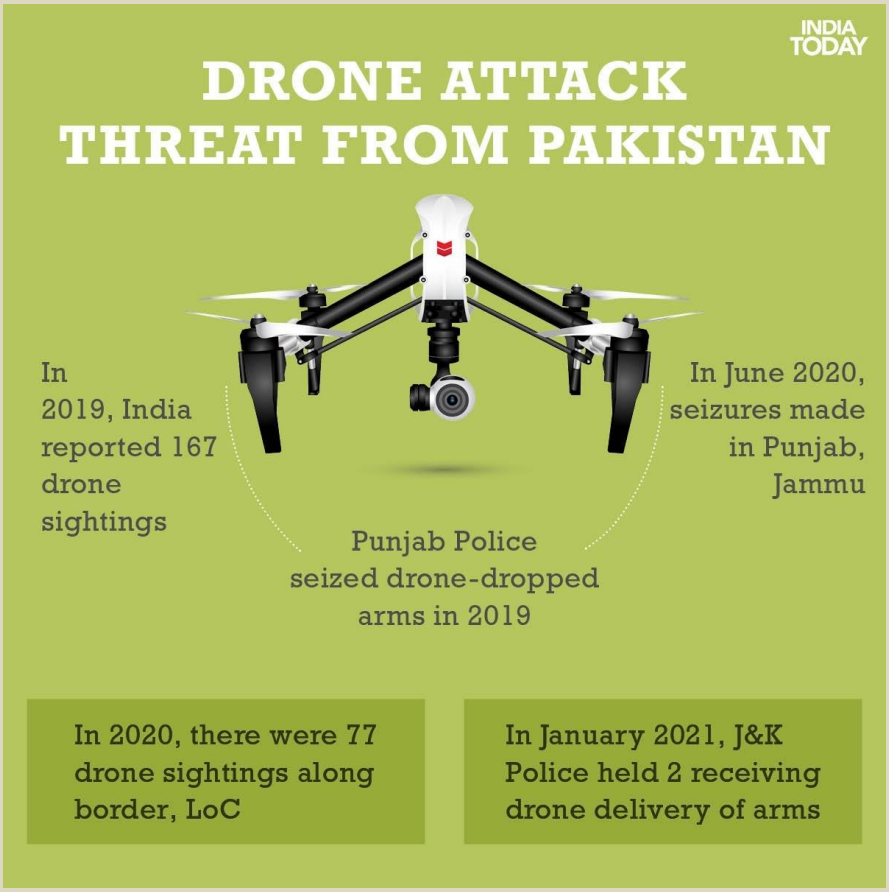
The threat of drone attacks from the Pakistani side is very real. Sighting of drones near India-Pakistan border and the Line of Control (LoC) has been frequent. Some of them have carried weapons to the Indian side.

In 2019, security personnel reported 167 sighting of drones from Pakistan, according to the official figures. In the pandemic hit 2020, there were 77 sightings.

In September 2019, the Punjab Police had seized a drone-dropped arms consignment to bust a terror module, which was receiving supplies from Pakistan. The seizure included AK-47 rifles and China-made pistols.

Another drone-dropped arms consignment was seized in Punjab's Gurdaspur in June 2020. The same month, the Border Security Force (BSF) shot down a drone in the Hira Nagar sector of Jammu. The recoveries included the US-made M4 rifles.

In January 2021, the Jammu and Kashmir Police caught two persons as they were picking up drone-dropped arms consignment.



Does Pakistan have such developed drone technology?

Pakistan does not have indigenous drone-making factories in abundance. But Pakistan and terrorist outfits operating from Pakistan get drones easily from China, which is the number-1 drone-maker in the world. Seized consignments dropped by Pakistan-sent drones often have arms and ammunition made in China.

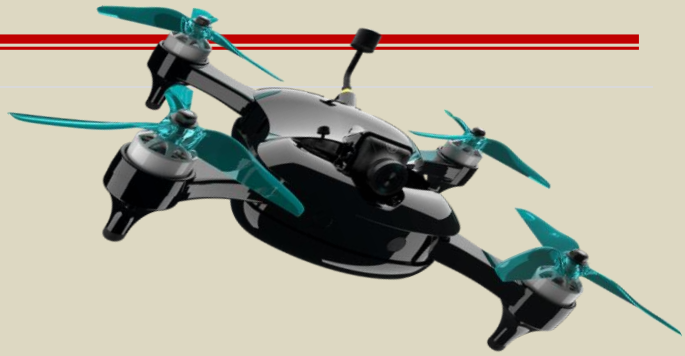
Why preventing drone terror attack is difficult?

The surveillance technology including radar systems that India has deployed at the borders or lines of control is meant for tracking bigger objects, helicopters, planes and missiles.

Drones are smaller in size — as small as 2 feet or only 60 cm — than previously popular UAVs but can fly for several kilometres at a speed ranging from 125 kmph to over 950 kmph, according to the AUSA report.

Preventing drone attacks requires jamming of drone systems and shooting them down. Laser-based Directed Energy Weapons (DEWs) are being talked about as a defence system against drone attacks.

In India, the Defence Research and Development Organisation (DRDO) has developed two anti-drone DEW systems. They can use powerful 10-kilowatt laser to engage aerial targets at a distance of 2 km. However, mass production of these systems is yet to take place.



What's a drone?

- Drone is a flying robot
- It can click photos and also drop bombs.

What are drones used for?

- Drones are used in both civilian and military fields
- US used drones to drop bombs in 1991 Gulf War
- US Air Force's X-37B space plane is a drone.

Drone for terror

- In 2013, Al-Qaeda attempted drone attacks in Pakistan but failed
- In 2014, Islamic State used drones in Iraq and Syria
- Islamic State, Hezbollah, and Pakistan-based terror groups use drones for terrorism

Drone attack threat from Pakistan

- In 2019, India reported 167 drone sightings
- In 2020, there were 77 drone sightings along border, LoC
- Punjab Police seized drone-dropped arms in 2019
- In June 2020, seizures made in Punjab, Jammu
- In January 2021, J&K Police held 2 receiving drone delivery of arms

Why drones are difficult to detect?

- Surveillance and radar systems are meant for larger objects
- Drones could be as small as 2 feet in size
- Laser-based Directed Energy Weapons (DEWs) are being developed
- DRDO has made two DEWs but mass production is yet to begin

Using Intelligent Drones for Search and Rescue

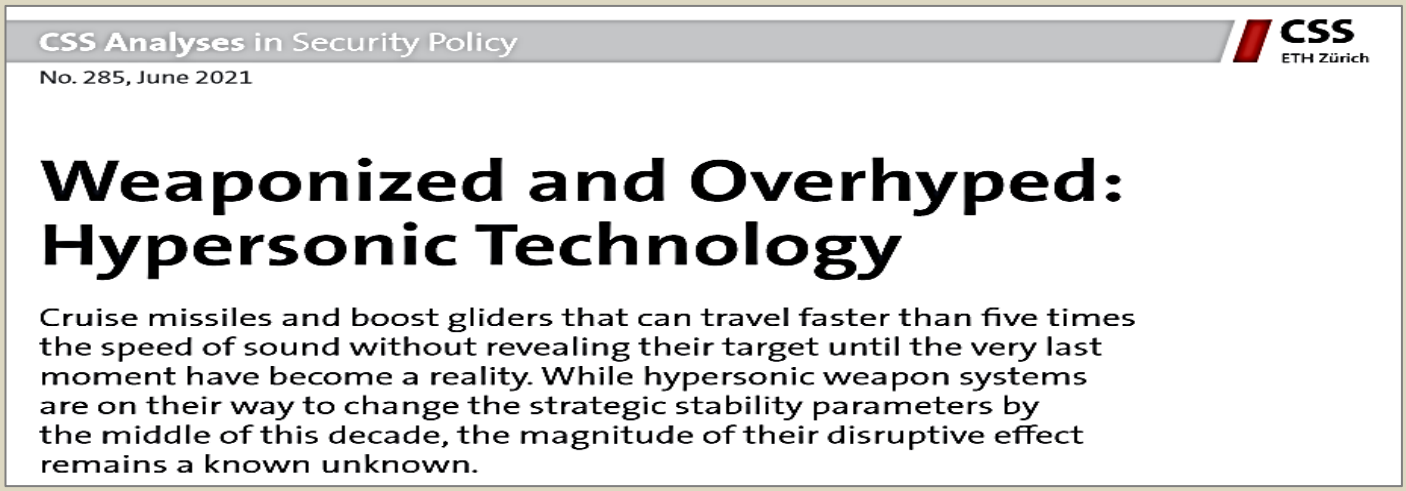
Source: http://www.homelandsecuritynewswire.com/dr20210628-using-intelligent-drones-for-search-and-rescue

June 28 – In 2019 alone, the ÖAMTC (*Austrian Automobile Association*) dispatched helicopters to fly over 2000 alpine search and rescue missions. The search and rescue of missing or injured persons often takes place in rough terrain and with air search. Whereas thermal cameras can detect differences between body heat and ambient temperature, using these types of cameras in forested areas can be difficult as trees and ground vegetation may be too dense. Manned search and rescue flights not only become challenging, but costly and time-consuming as well. In addition, these missions may often be unsuccessful or, in the worst-case scenario, succeed too late.

As technology becomes an increasingly important part of search and rescue, the first responder community will be involving more autonomous drones as these drones can aid in covering more ground as well as shortening search times. These drones, however, must be reliable and independently capable of finding individuals before a search team can be alerted to undertake a rescue mission. Whereas technological advances in the field of Artificial Intelligence are fundamental milestones, they do not solely solve the problem.

Prof. Oliver Bimber and his team at the Institute for Computer Graphics at the JKU have introduced a globally unique drone prototype that is up to the task. Subjects in individual thermal images often appear completely or partially hidden; the drone instead combines several individual images into one integral image that can be used for classification and to better detect people. As the integral images significantly reduce concealment (see image), modern deep-learning methods can aid in correctly detecting individuals up to a probability of well over 90%. When using conventional individual images, the same procedure attains a recognition rate of less than 25%. As there is little to no data available to support this kind of classification, over the past few months, the team had to create its own training database. This database is now publicly accessible. Many JKU employees and students served as test subjects.

Initial field study findings and pivotal early insight indicate that when it comes to concealed objects, combined images significantly support classification purposes better than individual images. These findings have now been published in the renowned scientific journal *Nature Machine Intelligence* and will not only aid in search and rescue missions, but will also be used effectively in other areas, such as police and military surveillance, developing autonomous vehicles, and in wildlife observation, particularly in support of conservation efforts. The team is currently working on advanced methods aimed at improving search speed and radius.



Source: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse285-EN.pdf

Dominika Kunertova *is a Senior Researcher in the Global Security Team at the Center for Security Studies (CSS) at ETH Zürich.*

Killer Flying Robots Are Here. What Do We Do Now?

Source: https://foreignpolicy.com/2021/07/05/killer-flying-robots-drones-autonomous-ai-artificial-intelligence-facial-recognition-targets-turkey-libya/

July 05 – In the popular Terminator movies, a relentless super-robot played by Arnold Schwarzenegger tracks and attempts to kill human targets. It was pure science fiction in the 1980s. Today, killer robots hunting down targets have not only become reality, but are sold and deployed on the field of battle. These robots aren't cyborgs, like in the movies, but autonomously operating killer drones. The new Turkish-made Kargu-2 quadcopter drone can allegedly autonomously track and kill human targets on the basis of facial recognition and artificial intelligence—a big technological leap from the drone fleets requiring remote control by human operators. A United Nations Security Council report claims the Kargu-2 was used in Libya to mount autonomous attacks on human targets. According to the report, the Kargu-2 hunted down retreating logistics and military convoys, "attack[ing] targets without requiring data connectivity between the operator and the munition."

The burgeoning availability and rapidly expanding capabilities of drones pose urgent challenges to all of humanity. First, unless we agree to halt their development and

distribution, autonomous killer drones like the Kargu-2 will soon be affordable and operable by anyone—from rogue states all the way down to minor criminal gangs and individual psychopaths. Second, swarms of killer drones may, through sheer numbers, render irrelevant the defenses against terrorist threats deployed by technologically advanced nations. Third, in creating a challenging new asymmetry in warfare, autonomous killer drones threaten to upset the balance of power that otherwise keeps the peace in various regions. The increasing ubiquity of affordable drones is an open invitation to one power and another to turn stable regions into battle zones.

The arrival and rapid proliferation of robot-like killer drones comes as no surprise. For decades, consumer technology has been outpacing military adoption of advanced technologies. Because a drone is essentially a smartphone with rotors, today's affordable consumer drones are largely a byproduct of the rapid development of smartphone technology. They are making access to the third dimension essentially free and creating new commercial opportunities: Drones can already deliver groceries and medical supplies directly to your doorstep. But in endowing drones with human-like cognitive abilities—for instance, by combining rapidly improving facial recognition with artificial intelligence—will make powerful targeted weapons available to tin-pot despots, terrorists, and rampaging teenagers at a fraction of the cost of the fancy drones flown by the U.S. military. And unless we take concrete steps now to oppose such developments, instructions to turn cheap off-the-shelf drones into automated killers will be posted on the Internet in the very near future.

Sailors move an X-47B combat drone aboard the aircraft carrier USS George H.W. Bush in the Atlantic Ocean on May 14, 2013. Mass Communication Specialist 2nd Class Timothy Walter/U.S. Navy via Getty Images

To date, artificial intelligence has struggled to provide accurate identification of objects and faces in the field. Its algorithms are easily confused when an image is slightly modified by adding text. An image-recognition system trained to identify an apple as a fruit was tricked into identifying an apple as an iPod, simply by taping to the apple a little strip of paper with the word "iPod" printed on it. Protesters in Hong Kong have used sparkly paint on their faces to confound government facial-recognition efforts.

Imagine attacks on 100 different locations in a single day—the effects of the 9-11 terrorist attacks on the United States could pale in comparison.

Environmental factors, such as fog, rain, snow, and bright light, can dramatically reduce the accuracy of recognition systems employing artificial intelligence. This may allow a defense against drones using relatively simple countermeasures to confound recognition systems at their present level of development. But to actors who already place a low value on collateral damage and innocent victims, accuracy is not much of a concern. Their drones might be programmed to kill anyway.

What's more, any defense against the drones zeroing in on individual targets does not prevent their deployment as new weapons of mass destruction. A swarm of drones bearing explosives and dive-bombing a sports event or populated urban area could kill numerous people and would be hard to stop. Various companies are now selling drone countermeasure systems with different strategies to stop rogue flying objects, and advanced militaries have already deployed electronic countermeasures to interrupt the drones' control systems. But so far, shooting down even one drone remains a challenge. Although Israel recently demonstrated an impressive flying laser that can vaporize drones, shooting down an entire swarm of them is still well beyond our capabilities. And with the new generation of autonomous drones, simply blocking communication to the drones is not enough. It may be critical to develop ways to safely bring them back to Earth in order to avert random chaos and harm.

To a group intent on causing significant damage, autonomous drones open an entire new field of possibilities. Imagine attacks on 100 different locations in a single day—the effects of the 9-11 terrorist attacks on the United States could pale in comparison.

Though all countries are at risk of killer-drone attacks, the most likely victims of the first wave of these weapons are poorer countries with porous borders and weak law enforcement. The same gap between rich and poor states in the effects of COVID-19 is likely apply to the vulnerability to autonomous drones. The first such battles are more likely to play out in Africa rather than America—and with heavier tolls.

The companies producing the new wave of autonomous flying weapons are heavily marketing their wares. Meanwhile, the United States and China have thus far refused to back calls for a ban on the development and production of fully autonomous weapons. Washington and Beijing are thereby providing a cover of tacit legitimacy for weapons makers and governments deploying the new killer drones in the field.

Israel uses AI-guided drone swarm to target Hamas militants in Gaza

Source: https://us.newschant.com/world/israel-uses-ai-guided-drone-swarm-to-target-hamas-militants-in-gaza/

July 06 – Israel has utilised an AI-guided drone swarm to perform assaults on Hamas militants in what's believed to be a world-first use of the know-how.

An Israeli Defence Force (IDF) assist unit deployed the swarm to find and target Hamas militants who had allegedly fired rockets into Israel in May.

Drones are usually guided by a human operator, however drone swarms signify a step ahead in army know-how by flying as one built-in community managed by synthetic intelligence.

The swarm requires solely a single human operator to direct your entire swarm and earlier than the drones information themselves to find the targets as a related unit.

The information comes simply weeks after Israel introduced the profitable testing of a brand new laser defence system that may shoot down enemy missiles by burning a gap in them.

The drone swarm solely requires a single human to management it and flies as a community related by synthetic intelligence

The swarm can proceed to function even when a number of the particular person drones are destroyed, and may be deployed for a spread of functions together with target identification, reconnaissance, and payload supply (pictured: Israeli air strike unrelated to drone operation)

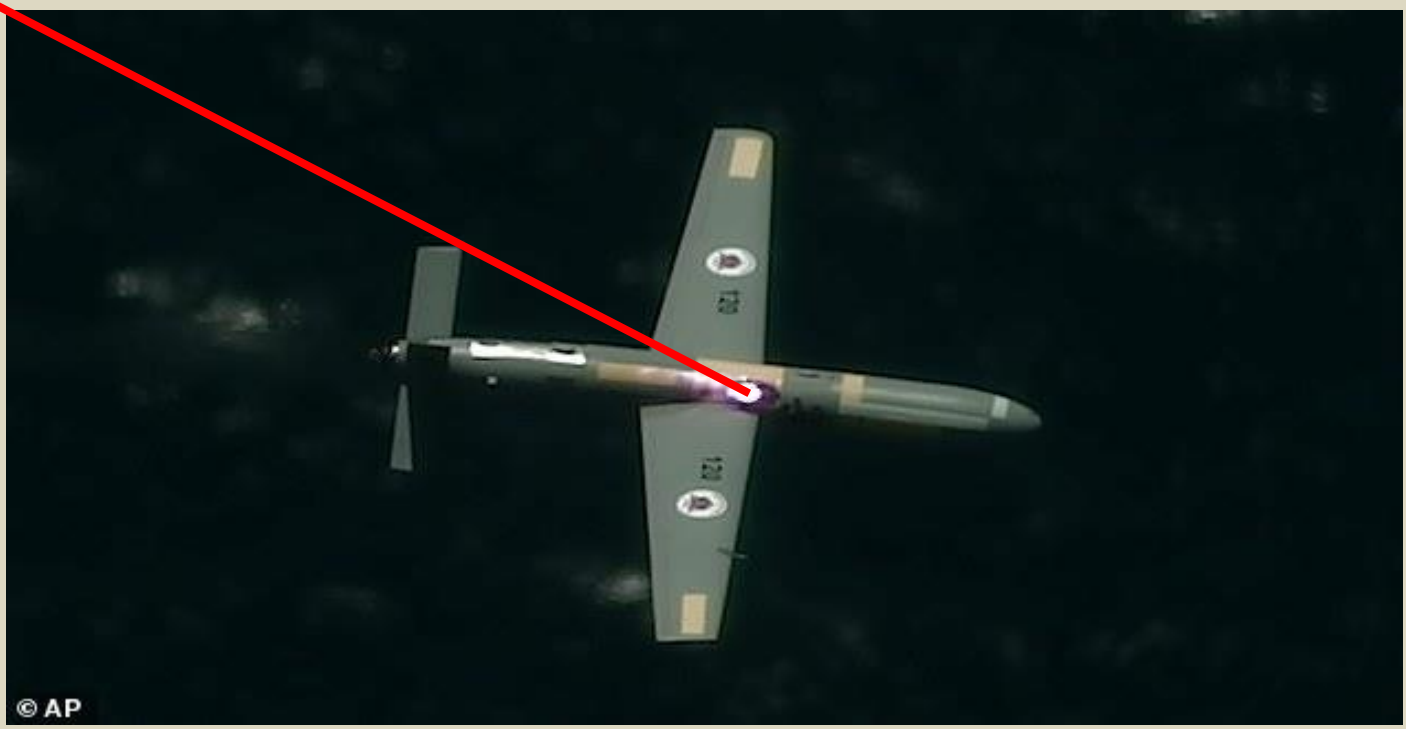
The swarm has been used to determine and supply focusing on data to guided mortar weapons to destroy enemy forces and weapons caches (pictured: Israeli air strike unrelated to drone operation)

"As far as we all know, that is the primary use of the sort of instrument,' mentioned an IDF spokesperson of the drone swarm.

'The operation of the swarm is by a single operator who controls all of the drones.

'There is a commander subsequent to him for making vital choices and different troopers for the logistical operation of the swarm.'

In this occasion, the drones offered focusing on data for guided mortar weapons which destroyed a number of Hamas targets and weapons caches.
According to the spokesperson, the drone swarm is a particularly adept instrument that can be utilized for a number of functions together with intelligence gathering, target finding and payload supply.
But IDF commander informed native information shops that the swarm unit has already carried out greater than 30 profitable operations and that the IDF are planning to make extra drone swarms obtainable to assist forces.

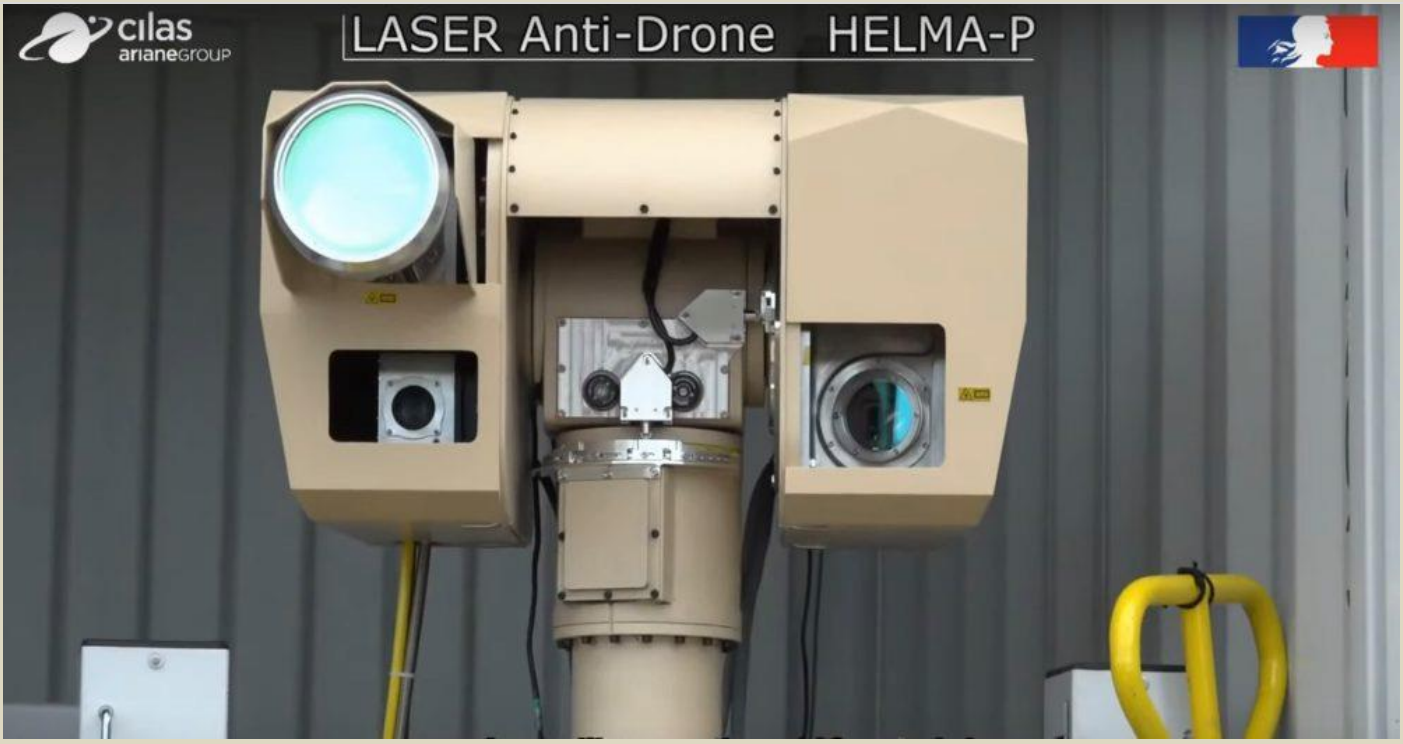


The deployment of the drone swarm comes simply weeks after Israel introduced the profitable testing of a brand new laser defence system that may shoot down enemy drones and missiles by burning a gap in them
The United Nations Institute for Disarmament Research in Geneva was fast to level out that the present capabilities of the drone swarm are usually not but these of extremely superior, totally impartial AI programs.
But institute official Arthur Holland warned that using a drone swarm is 'a notch up in the incremental development of autonomy and machine-to-machine collaboration in warfare.'
An analyst on the National Consortium for the Study of Terrorism and Responses to Terrorism in the US mentioned that whereas using a small drone swarm is much less regarding, 'we could also be trying on the emergence of a brand new weapon of mass destruction,' if militaries are ready to deploy giant numbers of drone swarms in fight.
The use of weapons programs and army know-how managed by synthetic intelligence has lengthy been a topic of science fiction, however latest years have seen AI-backed programs launched by army forces world wide.
US and China are each reportedly growing their very own drone swarms, while Chinese media reported final month that AI-controlled fighter jets have efficiently outsmarted and shot down human pilots in a number of exams.
Fang Guoyu, an aerial fight champion, informed state media he was not too long ago 'shot down' by an AI throughout a simulated dogfight after it realized his ways and used them in opposition to him

Counter-Drone Technology Ready for Paris Olympics in 2024

Source [+video]: https://i-hls.com/archives/109497

July 10 – France has been testing an anti-drone laser system for the 2024 Paris Olympic Games.
The French Directorate General of Armaments demonstrated the destruction of a drone by laser weapon, a protection system that the Ministry of the Armed Forces hopes to see fully operational during the Paris Olympic Games.

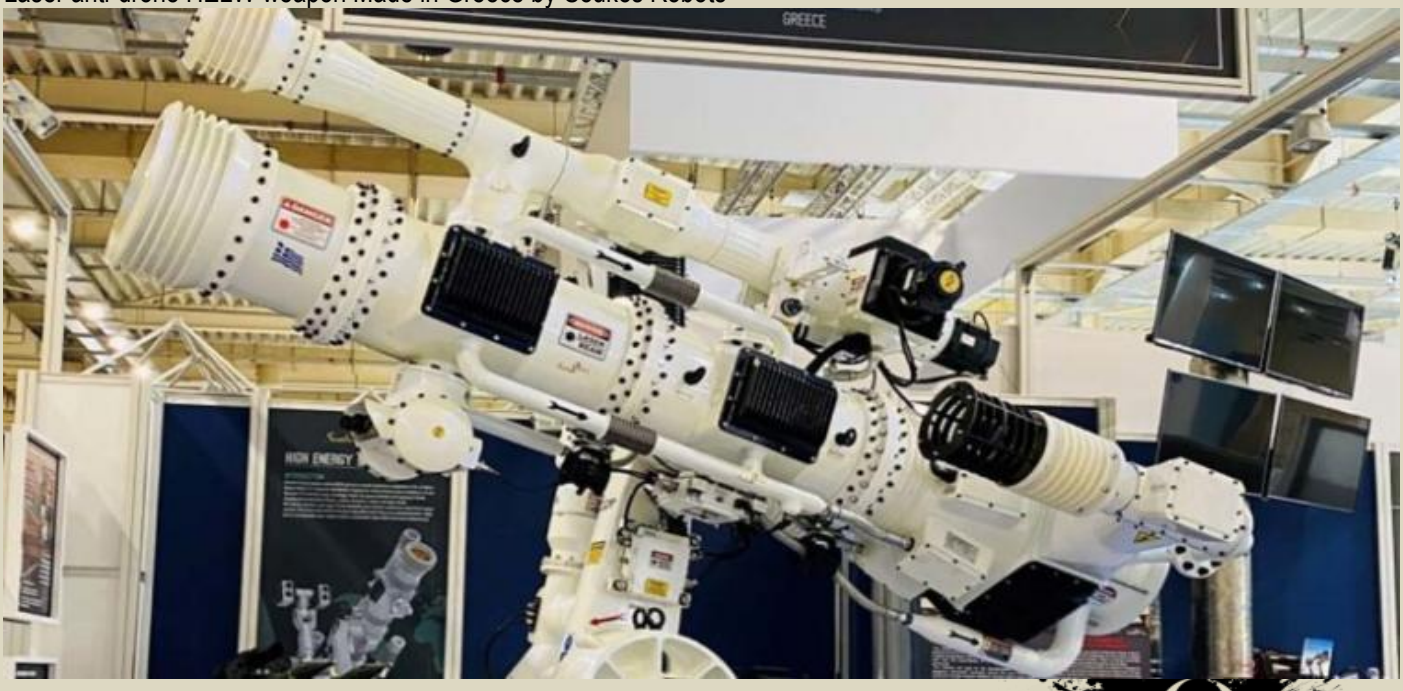


Designed by the French company CILAS with public funds, the new anti-drone laser system called **HELMA-P** will have the mission of securing the bases of the French army in external operations, but also sensitive sites in France, such as nuclear power plants, or still large public gatherings, according to international news agencies.

EDITOR'S COMMENT: The point is not how to shoot down the drones but how the International Olympic Committee selects the city that will host the Olympics. Given its past terrorist history, is Paris the right candidate for the biggest sports mega event? Not to mention that Olympic Games have gone far from being real sports' games; instead, they are becoming World Military Games where defense companies sell their latest products like the one above.

Athens DEFEA 2021

Laser anti-drone HELW weapon Made in Greece by Soukos Robots



Technical specs of HELW:

- Output Power: 100 kW
- Operational Voltage: 380-420 V
- Operational Frequency: 50-60 Hz
- Wavelength: 9-11 μm
- Power Efficiency: 10-60%
- Effective Range: 1 to 5 km
- Elevation: -25 deg to +85 deg
- Speed in Elevation: 50-115 deg/sec
- Traverse: 0-360 deg
- Speed in Traverse: 70-115 deg/sec
- Passive Detection: 25 km
- Stabilizing capability

Enter the new IED: Improvised Explosive Drone

Source: https://tribune.com.pk/story/2311111/enter-the-new-ied-improvised-explosive-drone

July 18 – For the Taliban, the mere mention of "drone" has long conjured up images of flying, buzzing death, and rightly so. They lost some of their senior leaders in US drone strikes in the border regions of Pakistan and Afghanistan. The drones were perhaps one US weapon they dreaded the most, for these remotely-piloted 'Predators' carrying 'Hellfire' could incinerate their unsuspecting target with pinpoint accuracy. The drone became the most potent weapon in the US hunt for al Qaeda and the Taliban, though the untenable collateral damage made it highly controversial. The Taliban might always have envied these sophisticated machines which require a massive amount of money, time and technological knowhow to develop and fly. But easy-fly, easy-buy hobby drones could help overcome this asymmetry. Though these off-the-shelf UAVs are not weaponised and have a range of hardly a few hundred yards, a little engineering could easily turn them into homemade flying bombs.

The Taliban in Afghanistan have been using commercially available quadcopters for surveillance and aerial shooting of their attacks for propaganda videos since early 2016. But now they appear to have started improvising these benign drones for combat roles. A short video clip shared by their spokesperson Zabihullah Mujahid on Twitter earlier this month showed a purported attack on an airport in the northern province of Kunduz. Apparently shot with a drone, the video shows a dense column of black smoke billowing upwards from what the description claims are two UH-60A Black Hawk helicopters of the Afghan air force destroyed in the attack. The video was released after Kabul denied the

incident had happened. Mujahid only described it as a "tactical attack", but pro-Taliban Twitter handles called it a "drone strike". A few days later, Mujahid shared on Twitter purported images of a second "tactical attack" also on Kunduz airport in which, according to him, a third Black Hawk was neutralised.

Afghan security officials, however, claim that the use of weaponised drones by the insurgents is not a new phenomenon. In November last year, Afghanistan's spy chief told the parliament that the militia was using hobby drones strapped with explosives for attacks on government forces. "The drones they are using are available in the market," said Ahmad Zia Shiraj, the head of the National Directorate of Security (NDS). Days before Siraj's revelation, Afghanistan's ToloNews reported on the authority of unnamed government officials that the Taliban had used improvised armed drones in some attacks. "The Taliban embed mortar rounds or small bombs with the drones and drop them on military and government installations," the channel quoted one official as saying. Such attacks were reported in the provinces of Kunduz, Logar, Balkh, Paktia and Faryab.

A month later, Afghan journalist Bilal Sarwary shared a video on his Twitter handle with description saying that an Afghan military officer in "Khost claims that a small drone of the Taliban stroked them with small bomb-like missiles. They have captured an exploded bomb, which seems locally prepared." Two days later, he shared photos of a quadcopter saying that Afghan commandos downed a drone in Charkh district of Logar province. "Weapons and ammunitions attached to drones are becoming the latest lethal trend on the Afghan battlefield," he wrote on Twitter.

The Taliban have fought a guerilla war against the US-led foreign forces for nearly 20 years. In asymmetric warfare, the insurgents are generally ingenious. They put their meager resources to good use compared to conventional militaries to fight a superior adversary. The Taliban have been doing just that.

Defence analyst Maj Gen (retd) Inamul Haq agrees that the Taliban might have been modifying consumer UAVs for combat operations long before the latest attacks. "They have been using armed drones very ingeniously," he told The Express Tribune. "In one case in Paktia province, a drone dropped a single mortar bomb on an Afghan position. Mortar is a high explosive bomb which detonates on impact. In another incident, they dropped 40mm grenades on the Afghan army positions from drones."

Experts are not sure if the Kunduz airport attack involved armed drones. "It's difficult to know exactly how it was carried out," Nick Waters, an analyst with Britain's open-source research group Bellingcat, told The Express Tribune. But he did not rule out the use of a quadcopter which could have been tweaked to use as a flying bomb to execute the attack.

"It's certainly a possibility – we've seen the proliferation of armed commercial drones across various conflict zones in the last few years, and there is evidence suggesting that the Taliban have been using armed drones," said Waters, who has also served in the British military.

Dr Peter W Singer, a US political scientist who specialises in 21st century warfare, concurs in that the Taliban may have incorporated weaponised drones into their arsenal. "It is highly possible. There have been various claims and media reports to that effect," he told The Express Tribune.

Haq, however, said he would not be surprised if the Taliban have destroyed Black Hawks using armed drones. "[If confirmed], it would be the second such incident. Earlier, they had destroyed a Black Hawk – in fact, two Black Hawks – in April [this year] as they claim – in Helmand province," he said. The helicopters had crash-landed after they were hit.

The Kunduz incident could have a huge psychological impact on the Afghan military, which is already facing a morale crisis. At the same time, it could encourage the insurgents to invest more heavily in the drone technology to turn these low-cost quadcopters into a mini air force of their own.

In Jan 2020, the Taliban flaunted a weaponised DJI Matrice 210 drone which they allegedly had seized from Afghan security forces during a night raid in the Garamsir district of Helmond province. It was equipped with a powerful Zenmuse Z30 zoom camera as well as a grenade-dropping tube.

Did the Taliban copy this advanced UAV?

"DJI Matrice 210 is a tethered drone which has multi rotors and is bigger in size. Irrespective of whether they actually captured a DJI Matrice 210 and copied it, they have been using commercial quadcopters available off-the-shelf for aerial reconnaissance and to cover their own attacks as early as 2016," said Haq.

The Taliban are often characterised as regressive, backward, and medieval, lacking modern scientific and technological knowledge. "That may be the brand, but the Taliban have long shown technical capability," said Dr Singer.

Consumer drones are easy to acquire and use, but the challenge is tweaking them to carry payloads. However, Dr Singer pointed out that it does not require sophisticated technologies. "This is not rocket science," he added. "Indeed, every insurgent group in the world now has access to everything from the Internet and cell phones to commercial drones."

Waters agrees. "Having seen the kind of IEDs that the Taliban used in Afghanistan, I'm confident they have the technical ability to improvise explosives to be dropped from commercial drones," he said.

IED, or improvised explosives device, was the weapon of choice for the Taliban during their protracted insurgency – and most of their deadliest attacks on the US-led coalition forces involved IEDs. Over the years, they mastered the science of IED-making. "Some of their IEDs were so sophisticated that it would be very difficult to neutralise them. If you neutralised one mechanism, there would be a second standby mechanism and a third mechanism," said Haq.

He doesn't agree with the stereotypical representation of the Taliban as a rag-tag medieval militia. "Well, rag-tag is a relative term. We use this terminology for them because we compare them with a super power [read: US]," he said. "Today's Taliban are educated. They have access to the Internet. They read stuff. They analyse things, watch videos and they can copy things quite effectively," he said.

The insurgents have been defeating American Humvees, which is an extremely robust tactical vehicle used by the infantry inside Afghanistan. They are the same guerilla fighters who had also neutralised the then state-of-the-art Soviet T-72 tanks using ingenious methods during the Soviet-Afghan War.

The Taliban have made significant territorial gains since the foreign forces started exiting Afghanistan. They claim to be in control of 85 per cent of the country, though they avowedly do not want to seize power militarily. They may have an edge over the Afghan security forces in ground combat, but the government has a clear advantage over the insurgency in the air.

Can the crude Taliban drones create a difference on the battlefield?

"Not major in terms of altering the very nature of the war, but it would be yet another problem for the government forces," said Dr Singer. "It is a special problem if used to take out their aerial units [because] the Afghan air force is the key to the regime's capability."

Haq, however, believes that if deployed in good numbers across Afghanistan, armed drones could become a "force multiplier" for the Taliban, especially at a time when the Americans are out of the scene. "This may help them capture cities because drones would provide them good reconnaissance on the Afghan army positions – something very important in CQC, or close-quarters combats," he added.

Waters also believes weaponised drones could make a difference, if the Taliban learn to use them effectively and at scale. "During the battle of Mosul, ISIS deployed a large number of these drones which played an important part in their strategy," he added. "Not only did these drones drop bombs, they also adjusted indirect fire, supported the tactical movement of troops and, perhaps most devastatingly, directed suicide vehicle-borne IEDs to their targets."

ISIS flew over 300 drone missions in one month when the US-led coalition forces were closing in on Mosul, Iraq, in 2017. "Over the last two months, coalition forces have observed about one adversary drone every day around Mosul," a US CENTCOM official told Defense One in a Jan 2017 interview.

The ultra-radical group launched a wide assortment of deadly UAVs – including grenade-launching and mortar-dropping drones – posing a real challenge for the US ground forces which had not come under attack from enemy aircraft since the Korean War 65 years ago. These drones gave ISIS its own mini air force, enabling intelligence, surveillance and reconnaissance as well as close-air support.

Is it easy to counter these "loitering munitions"?

"It is surprisingly difficult to counter what is in effect a toy drone," said Waters. "Firstly, they're very difficult to detect: they're small and, if they're high enough you're unlikely to hear them. Shooting at them with small arms is generally ineffective, and specialised drone jammers are only effective if you can make sure they're in the right place at the right time and the user can locate the target in the first place."

According to Dr Singer, it is doable but needs additional expense and equipment. "It requires a whole new layer of defence, combining both detection and then shoot-down. The shoot-down part can be anything from electronic jammers to systems that physically fire bullets at it."

The tactical advantage of low-cost drones may be limited, but their symbolic value against a bigger, powerful adversary is significant. And that is the reason this technology was, according to Dr Singer, embraced by "pretty much every insurgency in the world now, from Iraq to Mali".

After ISIS, Houthi rebels in Yemen have effectively used the UAV technology against the Saudi Arabia-led coalition they have been fighting for more than six years now. They deployed low-cost drones to carry out attacks in the Saudi cities along the Yemen border. The coalition said on June 20, 2021 that Saudi air defences had destroyed 17 armed drones launched by the rebels in a single day. Though the Houthi "missiles have largely been intercepted by the coalition, unsophisticated UAV attacks are humiliating for a coalition led by the Middle East's largest military spender," wrote Dhia Muhsin, former assistant research analyst for Middle East and North Africa at the International Institute for Strategic Studies, in an August 2019 article.

The use of consumer UAVs is not limited to terrorists or insurgents. The trend was also mimicked by drug cartels and organised criminals. "Apart from conflicts all across the Middle East and North Africa, weaponised drones are also being used by cartels in Mexico and in an attempt to assassinate President Maduro in Venezuela," said Waters.

Mexican drug cartels use weaponised commercial drones for attacking rival gangs and smuggling drugs into the US. "Drones operated by terrorists and other malicious groups represent a wide variety of risks for security, especially at facilities such as airports, essential infrastructure, prisons, stadiums, military bases, and strategic facilities, among others," said Mexico's defence ministry in a classified document accessed by El Universal newspaper.

Globally, the militaries have long exclusively flown drones for reconnaissance and in combat operations. But this 21-century technology is now being widely employed in civilian settings. UAVs are used for leisure and to monitor crops, shoot aerial videos, protect wildlife, monitor traffic, deliver parcels, undertake search and rescue operations and monitor disaster zones.

According to a report compiled by the Drone Industry Insights, the international drone market will grow by 13.8% to more than $42.8 billion by 2025. The Asian market has already overtaken North America as the largest regional drone market. India, which legalized drones in Dec 2018, will be by far the fastest-growing commercial drone market, by 2025 becoming the 3rd largest commercial drone market in the world.

This massive commercial investment has led to civilian drones becoming cheaper, easily accessible and capable of carrying larger payloads. Paradoxically, for these very reasons, the UAVs have also become the greatest security risk as non-state actors – including

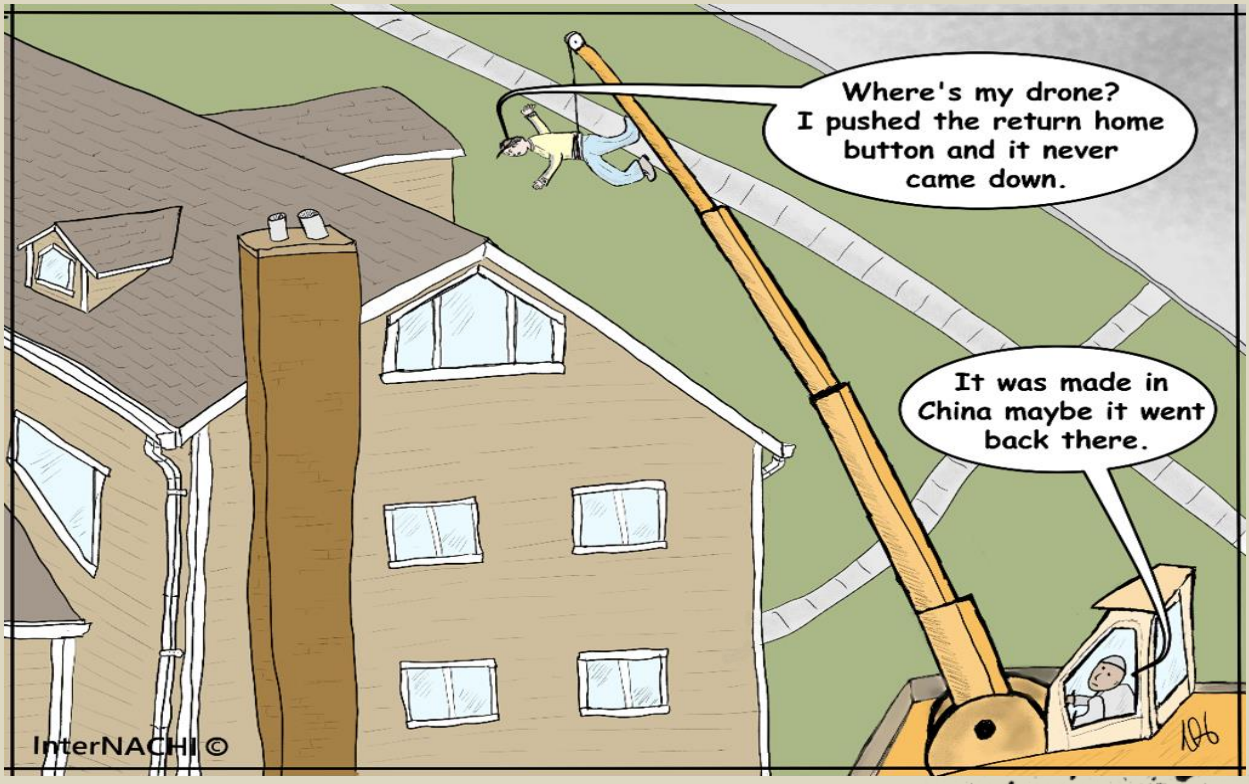
terrorists, insurgents, and criminal groups – are increasingly using these civilian drones for attacks and intelligence gathering. This makes it all the more important to regulate the use of drones. The best defence against the hostile use of this technology is to employ regulatory countermeasures, which can restrict the capabilities of off-the-shelf civilian drones and limit the ability of malicious groups to acquire and fly drones for sinister purposes.

"However, regulatory countermeasures to check the hostile use of drones by non-state actors are still not in effect. The Europeans are doing something about it but it is a half-hearted effort," said Haq. "The proliferation of drones in the hands of non-state actors and insurgents is at an alarming scale. This is considered aerial IED in future warfare."

EDITOR'S COMMENT: This article reminded me the special modifications (at the booster chrarge part of the weapon) made by mujahideen in their RPG-7 in order to be able to effectively shoot down Soviet helicopters in Afghanistan during the 1980s. Western military should study Talibans' field innovations – they might have some pretty good ideas and not that expensive.
▶ Read also: https://www.quora.com/Can-an-RPG-7-take-down-a-helicopter and https://www.rferl.org/a/1059629.html

Tokyo 2020/2021 Opening Ceremony

Towards the end of the ceremony, a fleet of **1,824 drones** took to the skies above the Olympic Stadium. Initially arrayed in the symbol of the 2020 Games, they then took on the shape of the Earth before a rendition of John Lenon's "Imagine," which was reworked by Hans Zimmer for the Olympics, played across the stadium. We've seen displays like this before. At Super Bowl LI in 2017, a pre-taped segment featuring 300 Intel drones forming the US flag punctuated Lady Gaga's halftime performance. Technically, the drone show that occurred above Tokyo isn't the biggest ever. As of earlier this year, that distinction belongs to a 3,281 display Hyundai-owned car brand Genesis put on in Shanghai, China. But even with fewer drones involved, the Tokyo drone show was still impressive.




International
CBRNE
INSTITUTE
C2BRNE
DIARY
CBRNE-Terrorism
Newsletter
W
M
O
D
HOTZONE
SOLUTIONS
GROUP
EMERGENCY
RESPONSE

MSD Medical Science and Discovery
2020; 7(12):712-6

Review Article Doi: 10.36472/msd.v7i12.447

Assessment of communication needs and planning communication actions during health crises

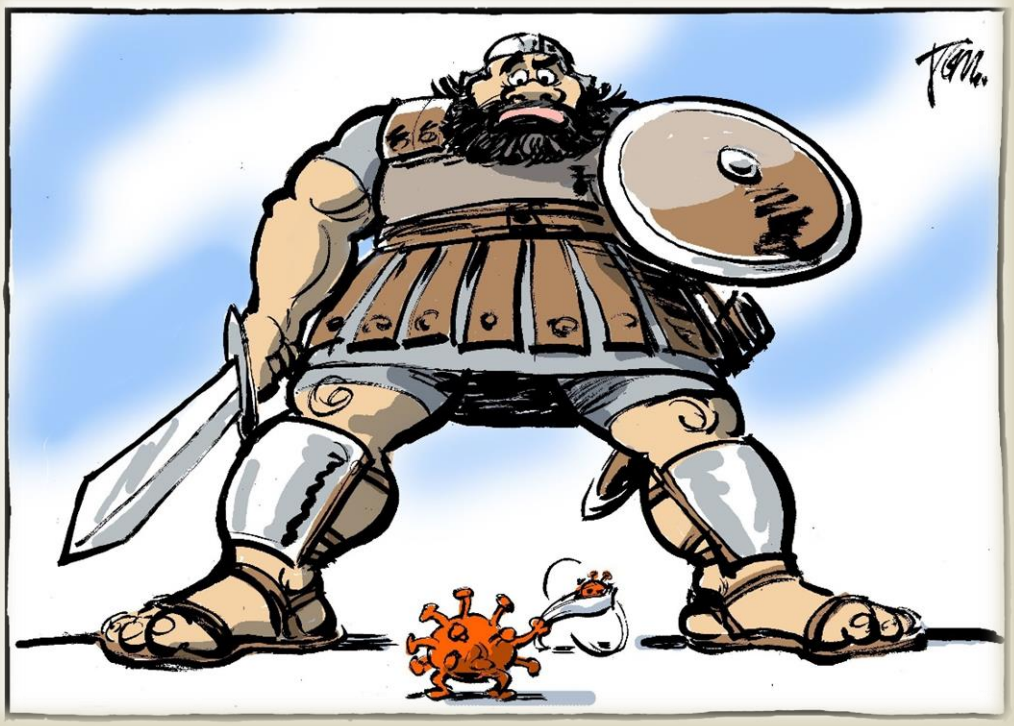
Athanasios Zafeirakis[1]*, Panagiotis Efstathiou[2]

Abstract

Health crisis communication (HCC) is a challenging and urgent task of the emergency preparedness planning of any welfare state. In this paper some particular reasons for that will be more specifically analyzed. The action flow of HCC includes the phases of preparedness, warning, response, recovery and evaluation. For a successful HCC detailed guidelines are also needed, along with profound knowledge of how the crisis stakeholders should deal with the psychological needs of the citizens and the mass media, as well as with some specific technical items. The ultimate implication of HCC is that the public is aware of its right to make informed choices after having been actively involved in the procedure of risk decisions making.

Keywords: Health crisis, crisis communication, preparedness, public emergencies

Source: https://medscidiscovery.com/index.php/msd/article/view/447



HotZone Solutions Group

Anything you need we have it!

Plus our unique field experience!

https://hotzonesolutions.org/