

HZS

2 CBRNE

*Dedicated to Global
First Responders*

DIARY

December 2021



IOI
International
CBRNE
INSTITUTE



HOTZONE
SOLUTIONS
GROUP



C²BRNE
DIARY

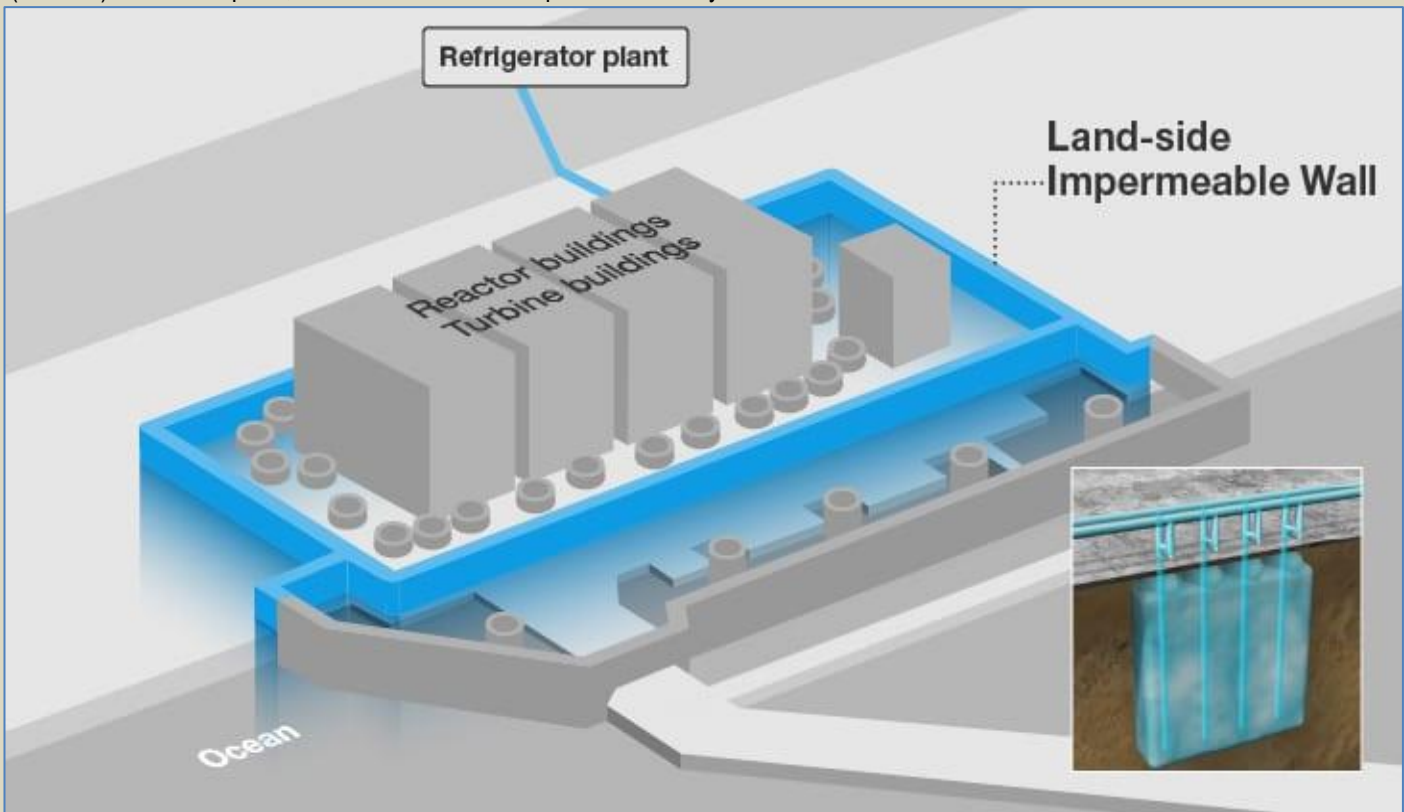
DIRTY R-NEWS



The ice wall at the port of Fukushima Japan can melt well: NHK

Source: <https://alexatimes.com/the-ice-wall-at-the-port-of-fukushima-japan-can-melt-well-nhk/>

Nov 26 – An ice wall intended to stop underwater expansion in Japan’s Fukushima Daiichi Power Plant operated by Tokyo Electric (TEPCO) could melt parts, an NHK broadcaster reported on Friday.



The 1,500-meter (m)-long “ice wall” encircling Units 1 to 4—which TEPCO calls “land-side impermeable walls”—is actually a barrier of soil that is frozen by a refrigerant flowing from a freezing plant through pipes buried 30 meters underground. It is designed to block groundwater flowing down from nearby mountain ranges from entering the devastated reactor buildings. + [Video](#).

TEPCO plans to strengthen the health wall by early December and is considering alternative prevention measures, NHK said. The ice wall was built to prevent groundwater pollution and damaged nuclear power plants, part of a costly and costly effort to protect the site following an earthquake and tsunami in 2011. TEPCO did not immediately confirm the details of the report.

Separating isotope facts from fallacies: nuclear weapons proliferation in the eyes of three intelligence communities



By Alexander K. Bollfrass

Source: <https://www.tandfonline.com/doi/full/10.1080/02684527.2021.1992153>

Oct 22 – The belief that another country is pursuing nuclear weapons can determine whether a state wages war, signs a treaty, or builds its own arsenal. Governments crafting policies to influence the nuclear choices of others through normative, economic, or military pressures prize accurate and timely proliferation assessments.¹ For example, counter-proliferation strikes and sanctions are most effective when directed against a programme’s early stages.² Export controls also rely on intelligence assessments of the end use.³

From the beginning of the nuclear age, governments have erred in assessing the scope and purpose of other countries’ programmes.⁴ Public evidence is scarce, limiting knowledge about the frequency and causes of nuclear misestimation. Individual episodes of one intelligence agency tracking a sole nuclear programme have been scrutinised, usually



seeking to explain an ‘intelligence failure’.⁵ More recent work has examined US intelligence analysts’ performance in tracking multiple nuclear programmes over time.⁶

Despite the United States government being only one of many employers of proliferation trackers, few researchers have systematically studied the assessment performance of multiple intelligence agencies tracking the same nuclear programmes.⁷ This article provides such an international comparison, making it possible to contrast their accuracy and test for recurring patterns that are not idiosyncratic to individual intelligence assessments.

In more than seven decades of intelligence scholarship, no general theories have emerged.⁸ However, the intelligence literature has produced bountiful insights on the institutional and psychological processes that can bias intelligence assessment.⁹ Less attention has been directed at how the assessed country’s behaviour and external environment affect its perception by intelligence analysts. Because the international relations (IR) literature dedicates itself to the above-mentioned dynamics, this article distils three generalisable propositions from various orientations of IR theory on the accuracy of proliferation assessments. Drawing from three levels of analysis, these propositions are not hypotheses intended to compete directly. Instead, they probe the power of these theoretical schools to reveal useful generalisations about the work of intelligence assessors.

These propositions will be tested on efforts by the American, British, and West German intelligence services to assess the Indian and Argentinian nuclear programmes for signs of weapons intent from the 1960s through the 1980s. After presenting the theoretical foundations of these propositions, this article describes each nuclear programme’s evolution. It scores the relevant intelligence agencies’ assessments of that programme, followed by an evaluation of whether the above IR-derived propositions explain a portion of the variation in analytic accuracy and how they compare to findings in the intelligence studies literature.

Propositions on proliferation predictions

Some structural IR theories predict that governments overestimate most dangers as part of a general paranoid pattern that animates interstate phenomena like the security dilemma and the ‘spiral model’.¹⁰ The difficulty of judging other states’ intentions and capabilities has long occupied grand theoretical investigations of interstate phenomena like alliance behaviour and war.¹¹

In ‘presupposing eternal rivalry and potential conflict’, the perennial challenges of intelligence analysis are compatible with many realist approaches.¹² In this tradition, states compensate for dangerous uncertainty by erring on the side of overestimation because making worst-case assumptions about each other’s intentions and capabilities amounts to ‘prudent insurance’.¹³ For conventional armaments, this impulse might be tempered by geographic distance or other signs that a foreign state is non-threatening. However, the destructive power of nuclear weapons makes even their potential acquisition by faraway governments a global security event.¹⁴ Consistent with these theoretical predictions, previous empirical investigations of nuclear proliferation forecasting by US intelligence indeed have found an overestimation trend interspersed with instances of underestimation.¹⁵

Which structural circumstances make overestimation more likely? Realism’s defensive varieties suggest that suspicion is more likely to target states perceived to be in a nuclear-tinged security competition within this paradigm. If a state is seen to be pursuing nuclear arms, its rivals would fear the effect on the balance of power – or even their use as an offensive capability – and be expected to follow suit. This can be illustrated with a prominent example: US assessments of Iraq’s unconventional weapons programmes before the 2003 invasion were most likely influenced by the latter country’s policy of deliberate obfuscation to deter Iran.¹⁶

Evidence of this alarmist tendency would be found in intelligence assessments of proliferation. If intelligence analysts believe in a security model for the spread of nuclear weapons, they would be expected to overestimate states’ propensity to fight proliferation with proliferation.¹⁷ The construct of proliferation as a biological process of contagion – in which states respond to nuclear programmes of rivals by developing weapons – has deep roots in nuclear thought.¹⁸ This suggests the first proposition:

Proposition 1. Intelligence analysts overestimate states that they perceive as having a proliferating rival.

Despite the systemic incentives for paranoia, liberal institutional theories aim to explain why some cooperation nevertheless takes place between states.¹⁹ This approach is useful in testing whether any of the international institutions that have been built to deal with a problem particular to nuclear weapons: Nuclear infrastructure and technology are inherently dual use, and the ‘line between safe and dangerous activities’ is ever-changing.²⁰ Even states seeking nuclear weapons are incentivised to claim peaceful intent. This makes it difficult to discern which states are pursuing weapons by tracking capabilities, raising the relative importance of accurately understanding governments’ intentions.²¹

States seeking to assure others that their nuclear development poses no threat can signal their non-aggressive intent by creating and joining diplomatic commitments and constraints, often in the form of international institutions.²² These commitments are not ironclad, although violating them risks consequences – if only to a state’s reputation.

Verification provisions may also serve as ‘a means to cull the sincere from the insincere’ when states promise to limit their nuclear capability.²³

Nonproliferation commitments should aid intelligence analysts in at least three ways. The first of these is screening: While rife with potential for misuse, signing a declaration of non-



weapons intent is a potentially resource-saving heuristic of where *not* to direct attention. Second, the difference between what documents states will sign and those they refuse could be rich in information. This includes diplomatic postures as treaties and other nonproliferation agreements that are negotiated with the target country's input. Lastly, assessors may acquire information through cooperative monitoring mechanisms that would be costly or impossible to collect on their own. Possible clandestine proliferators will know this, so a state with nuclear weapons intent is less likely to agree to formal limitations and thereby reinforces the screening logic.²⁴

Returning to the Iraq example provides cause for scepticism. The country had previously successfully misled IAEA inspectors about its nuclear programme, was cooperating inadequately with international inspectors, and 'US intelligence (was) unable and/or unwilling to grasp the reality that the inspections ... had succeeded'.²⁵

The NPT is the principal vehicle for states to record their nuclear armament intentions.²⁶ From safeguards on nuclear energy installations to treaties prohibiting nuclear testing, many other agreements have accumulated into a 'nonproliferation regime' with which governments can signal their nuclear intent for intelligence analysts to interpret.²⁷

Proposition 2. Nonproliferation commitments aid intelligence assessors.

The third proposition draws upon rationalist models with a tradition of explaining nuclear behaviour. Conspicuously, theories of deterrence among nuclear-armed competitors involve intelligence interpretations of other states' capabilities and intentions.²⁸ These models of state perception are optimistic about states' abilities to update their assessment of external threats with new information.²⁹ After all, an intelligence advantage should be a decision advantage.³⁰ Rational states should invest in intelligence accuracy in proportion to its value for making policy decisions.³¹ These models also predict a linear relationship between information availability and assessment accuracy: 'the more that it invests in intelligence, the less likely it is to be mistaken in its estimate', if all else is equal.³²

An important reason for variation in the information available to assessors would be their intelligence collection capability.³³ For example, overhead imagery to locate and analyse clandestine facilities is not available to every intelligence service. The target's difficulty, such as counter-intelligence competence or its society's general informational openness is another factor. In this perspective, any intelligence community assessing the same information should arrive at identical conclusions about a country's proliferation risk and additional information should improve accuracy.

Proposition 3. Assessment accuracy is a function of collected information.

IR theories subscribing to a model of states as smooth information processors diverge from the results of much work in the intelligence literature, which grapples with key analytical challenges like tradecraft, organisational knowledge management, and the effects of domestic politics on analysis.³⁴ The misestimation of Iraq's WMD intentions and capabilities by US intelligence has become synonymous with flawed analysis, including integrating 'technical and political analysis sufficiently'.³⁵

Testing these three propositions against the historical record requires variation in the assessed countries' (1) presence of proliferating rivals and (2) relationship to the nonproliferation regime, as well as the assessing country's (3) intelligence collection capacity. The next section creates that variation by tracing three intelligence communities' assessments of two nuclear programmes.

Comparing proliferation assessment accuracy

German, US, and UK assessments of India and Argentina were selected as case studies for the abundance of ambiguous and non-linear variation in their nuclear programmes' intentions and capabilities over time. Argentina did not develop nuclear arms and likely never intended to do so, even if some government elements pushed for the creation of a weapon option that may have shaped the pursuit of an independent and full nuclear fuel cycle. On the surface, India shared several similarities: interest in peaceful nuclear explosions, antipathy towards the global nonproliferation regime, and regional security competition. The main difference was that it eventually chose to construct a nuclear arsenal.

The criteria for inclusion as a proliferation assessment were that comprehensive analytical findings about a country's proximity to nuclear weapons possession were presented to high-level decision-makers as a complete analysis for internal use.³⁶ They had to be 'corporately authored' by intelligence services or other government bodies.³⁷ The United States has produced National Intelligence Estimates (NIE) to capture the entire intelligence community's views since 1950, which warrants their inclusion.³⁸ The Joint Intelligence Committee's (JIC) reports serve a similar function in the UK.³⁹ Reports from individual intelligence services or other government offices were only included if they fulfilled these criteria, which excludes the vast majority of regular intelligence reporting on individual events or developments. West Germany had a single foreign intelligence service, so any assessments by the Bundesnachrichtendienst (BND) transmitted to the country's political leadership were included. The evaluation of the propositions draws upon a broader range of government documents relevant to the analytical process.



This comparative research design is based on original archival research, formal declassification requests, and previously released intelligence assessments from Germany, Great Britain, and the United States.⁴⁰ Reflecting greater document availability, the respective countries' interest in tracking proliferation, and their collection capability, the United States intelligence community generated the most individual assessments. Argentina received less attention than India.

Assessments of India's winding path to weaponisation

Projecting ambiguity throughout, India took a circuitous path to building a nuclear arsenal.⁴¹ Its nuclear programme was born with a covert interest in weapons applications in 1948, when the country secretly established a nuclear commission that was publicly directed to begin work on 'peaceful' nuclear explosives (PNE) in 1964.⁴² The project was shut the same year, and India did not advance its nuclear explosive capabilities. After this time, 'New Delhi's proliferation drift was sealed by mid-to-late 1967'.⁴³ Scientists were authorised to conduct theoretical work on explosive designs and formally restarted work on nuclear devices in 1972.⁴⁴ The project produced a detonation in May 1974, which India described as a PNE. India did not undertake to convert its nuclear explosive capability into one that could be weaponised and delivered as a warhead, working instead more broadly on its nuclear capabilities for the rest of the 1970s. In 1980, India seems to have become committed to pursuing non-peaceful nuclear explosives and decided on an arsenal in 1989.⁴⁵ The ability to deliver weapons likely appeared around 1990.⁴⁶

Britain observes a former colony

British foreign policy had a persistent high-level interest in the possibility of proliferation in South Asia. For instance, the cabinet discussed creating a joint nuclear deterrent force in the Pacific region to dissuade India from arming in response to China's bomb in 1965.⁴⁷ The next year, it was proposed that India be dissuaded from contemplating the construction of an arsenal by sharing the high costs of British proliferation.⁴⁸ As a US-allied permanent member of the UN Security Council, interest in China and Pakistan motivated British regional policies throughout the Cold War. With its nuclear weapons status codified by the NPT, Britain sought to prevent other states from acquiring these arms.

At first, the British government tracked the early stages of India's nuclear development as an energy and scientific matter, relying on open sources.⁴⁹ Formal British nuclear intelligence assessments of India began in 1961, when the JIC reported that India was developing the preconditions for a weapons programme and that 'a government decision to make a weapon would inevitably be affected by' China's nuclear policy.⁵⁰ This first superficial assessment, probably based on open sources, accurately reflected the state of the Indian programme; the same applies to a September 1963 update that deemed it 'unlikely that the country has yet committed itself to producing nuclear weapons, but the wide scope of the nuclear programme and her evident aversion to being tied to outside sources involving safeguards suggest that the possibility of weapons production has been kept in mind'.⁵¹

This cautious tone fell away in the next assessment of July 1965, which overstated that 'India could rapidly develop nuclear weapons, and could test an initial device based on plutonium within 12–18 months of making the decision to do so'.⁵² Following India's summer war with Pakistan, an October 1965 JIC report indicated that it was on the way to developing a technical nuclear capability but the government had not decided whether to activate that option: 'India also has the capability to manufacture a nuclear weapon within twelve to eighteen months of a decision (which as far as we know has not yet been taken)'.⁵³ Coming a few months before India's governmental interest in developing its nuclear technology towards non-peaceful uses, in going from 'an initial device' to 'a nuclear weapon', the JIC overestimated the former British colony's capability.⁵⁴

A 1969 JIC report predicted that India would not 'develop a nuclear capability' over the next five years.⁵⁵ Taken literally, the prediction was correct: India's nuclear test took place five years and four months after this estimate. While the report acknowledged that India's position on the NPT might in part reflect the desire to maintain a weapons option, exercising the option was deemed unlikely. The test later demonstrated that India wanted to exercise its weapons option.

Later that year, the JIC presented a deeper investigation of the country's nuclear capabilities and concluded that it was 'unlikely that India has decided to start a nuclear weapons programme, or that she will do so over the next five years, unless she has reason to expect large-scale Chinese military hostilities'.⁵⁶ British intelligence had detected no signs of test preparations, promising policymakers that they could provide them with 'six months' warning of an atmospheric test and a longer warning of a full-scale underground test'.⁵⁷ But if the explosion were 'only to demonstrate an Indian ability to detonate a nuclear device, it could be carried out at short notice and the preparations probably concealed for some time'.⁵⁸ The six months' warning was not given when India detonated its first nuclear device less than five years later. Arguably, the PNE fell under the 'demonstration' caveat. However, the assessment's assurance that policymakers need not worry about an Indian nuclear weapons was unfounded.

The possibility of a test under the guise of peaceful applications was at the heart of a 1971 analysis, concluding that India had 'rejected the option of producing nuclear weapons, it has preserved the option of developing the capability to produce them and, in order to do so, has reserved the option of conducting nuclear explosions for peaceful purposes'.⁵⁹ The analysis predicted that a successful PNE would generate 'domestic pressures for developing nuclear



weapons'.⁶⁰ This Foreign Office memorandum moved the British understanding of Indian policy close to its later manifestation, although the delay between the first test and weaponisation suggest that whatever domestic pressures emerged were not the main force behind that development.

In late December 1973, the JIC wrote presciently:

India is very well placed to make a simple device and to conduct initial nuclear tests and could develop nuclear weapons suitable for her bombers well within the period. A decision actually to develop weapons is unlikely unless there is evidence of Chinese long-term intentions to launch a full-scale attack on her or of practical steps by Pakistan to develop nuclear weapons. But India may develop nuclear explosives for peaceful purposes, which would certainly imply that she could produce similar devices for military purposes.⁶¹ After the May 1974 test, the JIC assessed that India had been 'mainly (though not exclusively) concerned with developing a nuclear weapons capability' and would 'not be able to catch up with even the least advanced of the 5 existing nuclear powers in the foreseeable future'.⁶² British intelligence understood that India would not be sprinting to field a nuclear arsenal.

The next assessment appeared in the archives in 1979, reporting the absence of 'evidence of a nuclear weapon or explosive programme'.⁶³ Refraining from predictions, the assessment focused on the options that the country's technical capabilities provided and the role that Pakistan's nuclear decisions would play in Indian policy. The same year, a survey of proliferation trends identified India and Pakistan as the most likely candidates for weapons acquisition. A 'determined Pakistani nuclear weapons' effort could trigger an arms race.⁶⁴ A Pakistani programme was underway and, by one account, 'Pakistan's nuclear program was the biggest provocation for India to go nuclear'.⁶⁵

The last available declassified JIC assessment was dated February 1982. It warned that if relations with Pakistan did not stabilise, 'India might also decide to resume (PNEs), an option which Mrs Gandhi has never foreclosed'.⁶⁶ While relations with Pakistan improve, India did not resume explosive testing until 1998. Indira Gandhi reluctantly and briefly authorised a more advanced PNE shortly after this assessment.⁶⁷ The assessors offered no forewarning regarding India's establishment of a ballistic missile programme in the following year.⁶⁸

Nonproliferation and nonalignment challenges to US intelligence

Cold War American policy aimed to prevent other countries from acquiring nuclear arms.⁶⁹ India, whose feared nuclear armament was a primary US motivation for creating the NPT – although bilateral efforts to that end lacked determination and strategy in the key years of the 1960s.⁷⁰ After the country's PNE, the US objective was to inhibit the development of an overt arsenal, which was often cast as the primary aim in Indo-American diplomatic meetings.⁷¹ The broader relationship was frequently troubled over matters like US support for Pakistan and India's efforts at Cold War nonalignment.

While Indian attitudes towards nuclear weapons were explored in preparing the first global proliferation overview in 1957, the final version did not include the country.⁷² In a follow-on study of the next year, India was deemed deeply opposed to weapons development in the absence of Chinese acquisition.⁷³ The possibility of an Indian nuclear arsenal received more attention from American assessors in 1960, resulting in a vague warning that 'the government might decide to undertake a nuclear weapons program (especially if) Nehru has been succeeded by a less neutralist government'.⁷⁴ A full assessment arrived in a November 1961 NIE that evaluated global nuclear proliferation possibilities. Domestic and ideological factors were seen to work against a weapons intention, while Chinese nuclear development would push in the opposite direction.⁷⁵ The assessment reflected contemporary Indian thinking about its nuclear weapons option while being too optimistic about its technical capability.

A 1963 NIE reported that a weapons decision had not been reached and that it was 'unlikely that such a program will be authorised so long as Nehru remains in power' despite ongoing tensions with China.⁷⁶ For the analysts, indications were clear 'that India (was) actively improving its overall capabilities in the nuclear field, possibly in anticipation that a future decision to develop an operational nuclear capability may be required'.⁷⁷ International safeguards constrained the country's capabilities, but it 'could reach a position of independence from present controls in about two years, after which it would take another two or three years for India to produce its first nuclear device'.⁷⁸ The assumption that India would formally break its international agreements before using materials produced under its safeguards agreements with supplier countries would be disproven a decade later.

A year later, the State Department's Bureau of Intelligence and Research (INR) reported the community-wide consensus that 'India has the capability of producing and testing a first nuclear device in one to three years after a decision to do so'.⁷⁹ The assessment concluded that current policy was 'to use nuclear energy for peaceful purposes only' but deemed it likely 'that this policy will be kept under review during the months ahead'.⁸⁰ This underplayed Indian willingness to develop a PNE capability and the technical difficulties it would face.

Circulated days after China's first test, an October 1964 NIE assessed that 'the chances are better than even that India will decide to develop nuclear weapons within the next few years'.⁸¹ By 1970, India could produce 'about a dozen weapons in the 20 KT range' for air delivery.⁸² Such an arsenal did not appear for another two decades, although the analysis foresaw that India would not rush into production. With the dust of the Chinese test settled,



a December 1964 Central Intelligence Agency (CIA) proliferation overview announced that there was ‘a good chance that India will embark on a weapons program during the next few years’.⁸³ The State Department’s intelligence bureau (INR) contributed a memorandum to accompany NPT negotiations in July 1965: ‘New Delhi has so arranged its peaceful uses nuclear research program as to keep open the option of diverting it to weapons research and development’.⁸⁴ Both assessments were correct.

An April 1966 NIE assessed the totality of the Indian nuclear policy. On the technical side, it declared that ‘India has the capability to produce nuclear weapons’, erroneously asserting that the country ‘could test a first device within a year of a decision’.⁸⁵ According to the assessors, India’s intent was more complicated. The decision to abandon its anti-nuclear position would involve India’s relationship with the United States, China, and Pakistan. This assessment was vague but accurate when Indian policy was ‘an option on the option’.⁸⁶

After more Chinese nuclear tests later that year, an INR memorandum assessed that the Indian government would not follow domestic public opinion in favour of nuclear weapons’ development, but that it would likely not be able to ‘hold the line’ indefinitely.⁸⁷ State Department intelligence again addressed reports of Indian nuclear test preparations in January 1972, even if American intelligence collectors had not detected direct physical evidence.⁸⁸ The INR report assessed ‘that India could proceed rapidly and with little difficulty to establish a modest nuclear weapons program’, exaggerating the rapidity of India’s eventual arsenal development.⁸⁹

In August 1972, a Special NIE (SNIE) on India’s nuclear programme shortened the time between a decision to conduct a test explosion and the detonation to ‘a few days to a year’.⁹⁰ The likelihood of such a decision was ‘roughly even that India will conduct a test in the next several years and label it a peaceful explosion’.⁹¹ In the event of a test, India would ‘probably go ahead to make a small number of devices – which could be used as weapons’.⁹² The PNE became a reality; the small weaponised arsenal did not.⁹³ US intelligence attention then drifted from the Indian program, providing no warning of the May 1974 PNE. In late October, an SNIE surmised that ‘India has had all of the essential materials and facilities for production of plutonium weapons for about a decade’.⁹⁴ The assessors now deemed Indian nuclear armament more likely than not – and that it may have been underway.⁹⁵ The SNIE provided guidance on what India’s next technical steps would mean for its weapons intentions, overestimating India’s future nuclear weaponisation in the process.⁹⁶

The publicly accessible record does not include another post-1974 assessment of India’s nuclear programme until June 1981. An INR analysis led with the finding that ‘India and Pakistan have decided to keep the option of developing nuclear weapons, and signs of preparation for underground nuclear tests have been identified in both countries’.⁹⁷ Despite these concrete indicators, the assessors foresaw preparations to maintain an option without offering predictions of likely developments.

The following July, an NIE expanded the theme of Indian nuclear policy being driven more by Pakistan than China: ‘Pakistani nuclear activities have caused India to activate its own nuclear explosive development capabilities, which heretofore have been viewed by New Delhi primarily as capabilities for developing a nuclear deterrent against China’.⁹⁸ The observation appears accurate in retrospect.

West Germany’s hesitant judgment

West German policy towards India aimed to support nonproliferation principles without restricting nuclear exports.⁹⁹ Export interests tended to outweigh proliferation concerns, producing frequent friction with the United States, including over India.¹⁰⁰ In a challenge to the Federal Republic of Germany’s (FRG) foreign policy, India’s PNE came just over two months after the German parliament’s contentious vote in favour of NPT ratification, raising West German concerns that the global response would tighten global nuclear supply restrictions and onerous safeguard requirements.¹⁰¹

The Bundesnachrichtendienst (BND) wrote a study on ‘Nuclear Energy in India’ and its weapons implications in July of 1972, which has not been released.¹⁰² The foreign ministry also kept watch: A January 1967 memorandum noted that the country’s nuclear energy programme was being constructed to ‘keep open the path to nuclear weapons’ and tracked Indian plutonium production.¹⁰³

A few days after the PNE, the BND provided a background paper on India’s nuclear programme. It noted that India might have accumulated ‘60–80 kg’ of plutonium and intended to enrich uranium with centrifuges.¹⁰⁴ The plutonium figure likely underestimated Indian capacity.¹⁰⁵ At the same time, India would not build a pilot uranium enrichment facility for another decade.¹⁰⁶

The second BND assessment followed less than two months after the PNE, noting that fissile material had already been produced and reprocessed in India for several years, providing the foundation for indigenous production of nuclear weapons.¹⁰⁷ Although the development of a deliverable ‘credible deterrent against China’ was not possible because of technological and financial obstacles, additional tests were expected.

Nine years after the Indian test, German intelligence provided a brief to the foreign minister’s visit to India. The BND noted a recent increase in the prime minister’s public references to matching Pakistani efforts towards nuclear acquisition and that an unconfirmed intelligence report had recently arrived about an intensification of nuclear weapons’ development.¹⁰⁸ A later version of this report leaked to the press:



A May 1985 West German intelligence document cited an unconfirmed report that the 'leadership of the Bhabha Atomic Research Center had been given the assignment by the Indian Defense Department, after consultation with the highest cabinet officials and Prime Minister Gandhi, to continue working on the development of a thermonuclear weapon'.¹⁰⁹ Preparations were to be made so that 'within two months of a Pakistani nuclear test, the second Indian test could be carried out'.¹¹⁰

The Indian nuclear establishment was advocating for the authorisation of an operational nuclear capability at that time, and a high-level review committee was established to study the possibility. However, the BND had misread the prime minister's intent: He was personally opposed to nuclear armament and was likely using the committee to deflect those who favoured it.¹¹¹

Later that year, the chancellor's briefing included a discussion of India's nuclear energy programme. It reported that a decision had been taken earlier in the year to be able to match any Pakistani test immediately and that there had been no new reports about the possibility of Indian work towards a thermonuclear weapon.¹¹² Accounts of Indian nuclear decision-making are not conclusive about whether it explicitly aimed to match any Pakistani test, although the nuclear establishment was undoubtedly working to deliver that capability.¹¹³

The Federal Republic's BND reported on India's nuclear programme without much analysis, allowing itself little opportunity to be wrong. This was not the result of poor collection capability since the reporting was based on detailed technical knowledge and human intelligence.

Assessments of Argentina's nuclear nationalism

Argentina invested early and deeply in nuclear technology. In 1949, as part of a broader effort of importing 'useful Germans' to advance industrialisation, the Austrian Ronald Richter was allocated vast funds to produce energy cheaply with a 'thermonuclear reactor' on a remote island.¹¹⁴ Already in March 1951, President Perón and Richter announced experimental success in having achieved fusion through 'a totally new way of obtaining atomic energy that does not use materials hitherto thought indispensable', which was greeted by global scepticism and derision.¹¹⁵ Perón shuttered Richter's project in September 1952.¹¹⁶

A slower, second path using the materials Richter thought dispensable proved more lasting under the auspices of the National Commission for Atomic Energy (Comision Nacional de Energia Atomica, CNEA). Established in 1950, CNEA initially focused on purchasing nuclear reactors from abroad. Plutonium reprocessing in the laboratory succeeded in 1967.¹¹⁷ Nuclear technology investment grew under the military junta, which assumed control in 1976.¹¹⁸ Argentina's nuclear programme expanded to pursue a uranium enrichment capability through gaseous diffusion in 1978 near Pilcaniyeu.¹¹⁹ The enrichment facility was initially kept secret so that 'about a dozen people in the country knew of the entire project'.¹²⁰

In addition to laboratory-scale reprocessing from 1969 to 1973, there was also an effort to produce 'metallic plutonium' – the form that it would need to take for an explosive purpose – between 1980 and 1982.¹²¹ None of these activities were under safeguards, which Argentina persistently resisted in its negotiations for imported materials and facilities, as well as by refusing to sign treaties that would obligate their acceptance.

In November 1983, Argentina's president announced Pilcaniyeu's existence. The facility did not produce enriched uranium until 1986.¹²² While many scholars have taken the secret construction of the Pilcaniyeu facility to have indicated weapons intent, the configuration was not optimised for HEU production and may have been the 'reckless' result of 'expressive nationalist policies in the nuclear field'.¹²² The low-enriched uranium was likely intended for naval propulsion.¹²³ Defeat to the United Kingdom in the 1982 Falklands War briefly accelerated its nuclear work.¹²⁴ In 1983, Argentina announced that it was able to enrich uranium at its previously secret facility.¹²⁵ However, CNEA's budget was cut deeply a few months later and arrested its development.¹²⁶

The history of Argentina's nuclear intentions remains disputed. Scholars who maintain that Argentina attempted to acquire nuclear weapons do so to argue that US pressure caused the country to refrain.¹²⁷ While much of the evidence regarding Argentine behaviour is consistent with a proliferator – especially the clandestine construction of a uranium enrichment facility – these activities are more likely to have resulted from idiosyncratic political reactions to US nonproliferation policies.¹²⁸

West German investigation of its customer

Argentina was a top priority for West German nuclear policy. The two states broadly enjoyed a 'very good' relationship.¹²⁹ Nuclear cooperation was especially close, including the personnel exchanges (a legacy of Perón's 'useful Germans').¹³⁰ Based on the principle of 'uranium for technology', several bilateral deals – including Germany building a heavy water plant in Patagonia – were explored.¹³¹ This was scuttled in response to US pressure, which was a persistent problem for the German nuclear export business. This pressure was always presented as proliferation concerns over insufficient safeguards, although it was often motivated by commercial interests.¹³² The most significant export was ultimately Argentina's first nuclear power reactor, which started operation in 1974.¹³³ Bonn promoted and subsidised these exports.¹³⁴

In the first available assessment, the BND evaluated Argentina as part of a global proliferation survey in July 1974:



The South American state with the most advanced nuclear research and technology possesses not only several research reactors, but also the first power production reactor, from which plutonium can be extracted beginning in 1975. Fuel is produced domestically. It is especially important that Argentina has a reprocessing facility – even if it is small – with which to extract plutonium. Argentina has possibly already generated plutonium not under international safeguards from its largest research reactor.¹³⁵

Not reporting that Argentina had indeed already separated small quantities of unsafeguarded plutonium made the assessment – based on an in-depth analysis of the country's capabilities produced for the chancellor's information – a mild underestimation.¹³⁶ Around the same time, the Federal Republic's intelligence service composed a formal assessment of Argentina's nuclear potential for its political leadership. The report surveyed the country's technical capability (to which a German firm had made the most significant contribution) and stopped short of making any definite predictions.

Fuel for the nuclear power station comes from its own uranium resources; a small reprocessing facility is available for the separation of the burned-up fuel rods. There is no information about international controls of the Argentinian fuel cycle. Technical preconditions for plutonium production are available (around 80 kg annually from Atucha as of 1975). Argentina must be seen - next to Israel and the Republic of South Africa - as the third non-industrialised state that could produce its own nuclear weapons in a relatively short period.¹³⁷

The characterisation of Argentina's technical capability was accurate, despite hardly qualifying for the same proliferation league as Israel and South Africa. The BND's uncertainty over which international safeguards applied is perplexing since there were none for the fissile material-producing facilities.

In July 1985, the BND returned to Argentine nuclear activities. It reported work on a reprocessing facility that was not expected to be completed before 1987, after which Argentina would be capable of producing nuclear weapons.¹³⁸ However, now only spent fuel under international safeguards was available. The assessment did not report on Argentina's previously secret uranium facility.

British pre-war inattention

British assessments of Argentina are available from 1979 and 1980, during which the Falklands Islands dominated the UK-Argentina policy agenda. Until the conflict, the British Foreign Office was engaged in active negotiations over supplying Argentina with a reactor, having lost the bid to build the first reactor to West Germany.¹³⁹ Simultaneously, Britain was working through multilateral mechanisms and with the United States to limit Argentinian imports of dual-use nuclear technology.¹⁴⁰

Ignored in prior proliferation surveys, Argentina was dismissed in 1973 as among the unlikely 'candidates for military nuclear power'.¹⁴¹ British intelligence first paid serious attention to Argentina's nuclear programme in May 1979. Describing it as 'one of the countries in the developing world which will arrive soonest at the point where she can produce much of her own nuclear equipment' and nearing the 'capability to make nuclear weapons', there was 'no evidence of any intention on the part of the present Government to embark on a weapons programme'.¹⁴² This was a fair conclusion but overlooked the fact that Argentina was building a clandestine enrichment facility.

An April 1980 assessment described Argentina as 'a country capable of creating a nuclear weapons option, and Argentine government has consistently sought to avoid formal renunciation of it'.¹⁴³ The following month, both Brazil and its rival were seen as proliferation candidates, even in the absence of 'current evidence of weapons intentions'.¹⁴⁴ In July, Argentina's impending complete and independent fuel cycle was again flagged as a proliferation concern.¹⁴⁵ In October, the nuclear assessment office warned that they had a 'more skeptical view of the Argentine position': "We would accept that she has no current military nuclear programme. There are however powerful forces working within the regime there against formal renunciation of the nuclear option".¹⁴⁶ Like the prior year's assessment, these were accurate sketches of Argentinian intent written without awareness of the uranium facility.¹⁴⁷

The United States and Argentina

The United States saw Argentina as the key to keeping its hemisphere's nuclear monopoly intact. In engagements with the Argentine government, the nuclear subject was consistently at or near the top of the agenda. In these meetings, US representatives sought Argentinian acceptance of international inspections of its infrastructure, the NPT, and the signing of the regional nonproliferation agreement – the Treaty of Tlatelolco.¹⁴⁸

US intelligence tracked Argentina's nuclear development early, beginning with its post-War recruitment of German scientists and uranium mining plans.¹⁴⁹ The collected intelligence was first assembled into a formal proliferation assessment in the context of the campaign to gather signatures for the NPT in 1969.¹⁵⁰ A deeper examination appeared in an October 1974 global assessment, which concluded that Argentina was working towards nuclear technological self-sufficiency and that any future weapons crash programme would take close to a decade to succeed.¹⁵¹ In December of the following year, a CIA paper found that Argentina 'could conceivably graduate to nuclear explosives'.¹⁵² A November 1977 briefing mentioned that 'Argentina's rush toward nuclear reprocessing raises the spectre of its becoming a member of the nuclear club'.¹⁵³ An assessment, found in National Security Council files of September 1978, described Argentina's intention not only to



'become self-sufficient in nuclear energy', but to export regionally.¹⁵⁴ Whether this meant that Argentina would seek nuclear weapons was not conclusively predicted. These short assessments were accurate.

Following the 1982 Falklands War, American intelligence took a much closer look at Argentine nuclear policies than it had before. Argentine incentives were assessed to be tilted against weaponisation.¹⁵⁵ American intelligence missed Argentina's clandestine uranium enrichment facility but correctly assessed the limitations on incentives for a nuclear weapons push and the financial constraints. A global proliferation survey that summer described an Argentinian PNE as unlikely – and concluded that weapons development 'considering the nature of Argentina's defence requirements, the military utility of such a program probably would not be worth the effort'.¹⁵⁶

Another NIE was commissioned in July 1984 to investigate the effect that the democratic transition had on the country's nuclear policies, grappling with whether these decisions would remain the purview of the military and announcing that Argentina was two to three years away from a plutonium separation capability.¹⁵⁷ The NIE missed that much of the programme had been abandoned. The prediction about Argentina's unwillingness to sign the regional nonproliferation treaty and subject itself to safeguards was also unduly pessimistic.

In November of the following year, the CIA circulated a detailed assessment of Argentina's nuclear policy and infrastructure. It still could not provide a definite assessment of the weapons' dimension, as it lacked evidence of the intentions that animated the decision-making.¹⁵⁸ There was likely little evidence of weapons intent to be uncovered. The document also claims that the enrichment facility had been known since 1981, despite not having mentioned it in previous assessments.¹⁵⁹ One possible explanation for this discrepancy is that US intelligence had detected and inspected the facility without determining its purpose. According to a former Argentinian official, 'the nuclear affairs attaché of the U.S. embassy' requested an inspection based on satellite imagery.

We misled him and organized a false visit in which everything was camouflaged. He left without having talked to anyone, which cost him his post.¹⁶⁰

The United States intelligence community has yet to declassify documents that would shed further light on whether Argentina had indeed evaded its detection.

Correlates of misestimation

Proposition 1. Intelligence analysts overestimate states that they perceive as having a proliferating rival.

The assessments reviewed above show that intelligence analysts occasionally overestimate. Frequent analysis of how a government *could* use its current nuclear capabilities to create an arsenal may have made policymakers more alarmed about proliferation than warranted by separate individual analytical judgments. However, unambiguous overestimates were a minority of the analytical judgments reviewed above. Were these overestimates associated with perceptions of an arms race? The retrospective understanding that India was indeed party to nuclear rivalries with varying intensity over time – which Argentina was not – helps test this first proposition.

The weapons aspiration in India's nuclear programme was initiated by China's 1964 nuclear test, which came two years after the countries had fought a war.¹⁶¹ The eventual decision to pursue an operational nuclear capability was, in one accounting, 'in response to Pakistan's acquisition of nuclear weapons with Chinese help and US indulgence'.¹⁶² India therefore had two rivals with nuclear ambitions that were being tracked by the intelligence assessors. Most assessments presumed that Indian intent was conditional on Chinese and Pakistani decisions, including developments in their nuclear programmes.

Early overestimates of Indian progress towards a nuclear arsenal in the 1960s regularly invoked the Chinese programme. For example, in 1965 British intelligence flagged 'further Chinese testing' as a cause of 'a decision to begin a nuclear weapons programme' if the country could not be provided with an extended deterrence.¹⁶³ A contemporary State Department report on the problem identified US and Soviet policy as a potentially powerful determinant of Indian weaponisation.¹⁶⁴ Hindsight has shown that discussions about guarantees did not produce satisfactory guarantees, although it is difficult to know whether stronger guarantees would have led to Indian nuclear restraint.

Western intelligence analysts' focus on China's nuclear programme contributed to their blindness towards India's preparations for a PNE. As late as December 1973, British intelligence would write that weapons development was unlikely 'unless there is evidence of Chinese long-term intentions to launch a full-scale attack on her or of practical steps by Pakistan to develop nuclear weapons'.¹⁶⁵ Having been alerted to India's position under China's growing nuclear arsenal, the estimates above overweighted the role of external nuclear threats in Indian decision-making, producing underestimates in the early 1970s.

Following the PNE, intelligence assessments portrayed India as more eager for nuclear weapons than it actually was. Arms race dynamics played a part in these overestimates:

The military rationale for this has been the hope of producing an effective deterrent against China. Maintaining a decisive lead over Pakistan has probably been a secondary consideration. Prestige has also been an important element. The Indians are very unlikely



to stop at a single test. Pakistani attempts to catch up will make it hard for the Indians to abandon a weapons programme even if they now wished to do so.¹⁶⁶

However, compensation for failing to have foreseen the PNE and making a straight-line prediction were complementary factors in creating these overestimates.

In strong contrast to India's two-front insecurity, Argentina's competition with Brazil was ultimately more about prestige than security, although it takes the luxury of hindsight to conclude 'security dilemma dynamics' were not driving Argentina's partially clandestine programme.¹⁶⁷ Even Argentina's revelation of a clandestine enrichment plant produced only a muted Brazilian response. The two countries arrived at a comprehensive bilateral nuclear agreement in 1991.¹⁶⁸

Intelligence assessors regularly presumed that Argentina's intentions were linked to those of Brazil. The review above showed that the systematic US overestimation of Argentina in the 1970s was created by the latter's purported interest in PNEs. That misjudgement was grounded more in Argentine resistance to external limitations on its nuclear programme than hedging against a Brazilian nuclear weapons programme. Writing in the immediate aftermath of Argentina's defeat against a nuclear-armed UK and revelation of the secret uranium enrichment facility, US intelligence later understood that nuclear weapons were not an attractive solution to Argentina's defence needs.¹⁶⁹

Presumed nuclear competition introduced uncertainty into intelligence analysts' work by creating linked expectations of how one state would influence the other. In most of the above cases, this helped produce analyses that hold up:

India has the capacity to develop its own nuclear weapon but not for at least twelve to eighteen months after a decision to do so. As far as we know this decision has not yet been taken. But the knowledge that India had embarked on a military nuclear programme would have a considerable effect on Pakistan, which has not got any comparable nuclear capability and would be likely to seek assistance from elsewhere, probably from China.¹⁷⁰

The West German BND also accurately reported that India wanted the ability to match any Pakistani tests in the latter half of the study period. In the early assessments, however, British and American assessors created analytic complexity that overvalued the effect of China's nuclear evolution on India. On occasion, it generated uninformative analysis.¹⁷¹

On the whole, the first proposition receives no empirical support in the Argentine case but it was more successful with India. The possibility of a three-pronged arms race focused analytic attention on India's opaque nuclear intentions and contributed to some overestimates. The historical record examined above suggests that whatever analytic errors were made in assessing the two nuclear programmes, a deterministic proliferation domino theory was rarely the culprit.

Proposition 2. Nonproliferation commitments aid intelligence assessors.

Both countries were selective in making international commitments, decisions that received bountiful attention in their proliferation assessments. Did any of the three mechanisms – screening, differentiation, or monitoring – influence intelligence analysts' ability to assess India's and Argentina's nuclear intentions and capability?

Screening

In both cases, a reluctance to pledge nuclear abstention ensured that intelligence services paid regular attention. India's refusal to join the NPT's limitations helped foreign intelligence officers understand that an Indian nuclear armament was a possibility, even if it did not help them predict the time frame of its development. The same was true for the country's reluctance to accept expansive safeguards on imported nuclear equipment.¹⁷² While Indian leaders presented their opposition to the treaty as a principled stand against the NPT's discriminatory nature, this did not bamboozle the intelligence analysts.

Argentina, in doing what it (and India) preached, posed more of a challenge. Driven by a nationalistic insistence on nuclear self-determination, Argentina invited suspicion in refusing to accept the NPT, the Treaty of Tlatelolco, and leveraged potential international suppliers against one another in minimising safeguards.¹⁷³ For example, an entire June 1984 CIA memorandum sought an explanation for why the country exhibited 'a strong reluctance to make any major nonproliferation commitments', which produced a line of thinking that echoed how a former Argentinian official described the motivation: 'Argentina wanted to improve its image in the nuclear field, to make it more transparent before the international community, but was not willing in any way to pay the price of full scope safeguards'.¹⁷⁴ This consistent rejection of the nonproliferation regime invited suspicion, although much analysis examined this ideological impulse for nuclear independence as a serious hypothesis.

Differentiation

While Argentina's consistency offered little to analyse, India had a more differentiated stance on international proliferation agreements. Unfortunately for the assessors, the assumption that India would honour the agreements that it had voluntarily accepted proved misleading. The assumption that India would not involve foreign technology safeguarded by suppliers for explosive purposes led to the American and British failures to anticipate the PNE. In October



1969, for instance: 'Safeguards attached to the purchase of the first two power stations should make this difficult if not impossible in those cases'.¹⁷⁵ German and US intelligence shared the assumption that India would not break safeguards on internationally supplied materials and equipment.¹⁷⁶ British intelligence allowed for the possibility that safeguards evasion at 'the Canadian reactors is a possibility', but excised that judgment before sharing the assessment with Five Eyes partners.¹⁷⁷ The assumption that India would not use the plutonium generated in its Canadian-supplied reactor persisted despite open warnings that India believed an underground PNE violated neither the Limited Test Ban Treaty nor the supplier agreements.¹⁷⁸ After the test, assessors relied less on international commitments in their studies of Indian nuclear intent but still prized information resulting from these agreements' implementation.

Monitoring

Both countries reluctantly accepted some inspections and safeguards on their foreign-supplied nuclear facilities. When the International Atomic Energy Agency (IAEA) was tasked with this monitoring, intelligence assessors used its information as raw intelligence in writing their assessments. For instance, British intelligence closely tracked safeguards information on individual Indian facilities following the PNE.¹⁷⁹ Their American counterparts weighed 'the adequacy of the IAEA inventory controls, surveillance equipment and inspection procedures in place' at an Argentinian reactor.¹⁸⁰ Revealing a symbiosis, the United States was sending leads regarding Argentina to the IAEA.¹⁸¹ Beyond safeguards, while US intelligence could not 'independently confirm Argentina's capability to enrich uranium', IAEA officials were the first international eyes to visit Argentina's uranium enrichment facility after its unveiling.¹⁸² Information exchanged among political representatives at the IAEA's headquarters in Vienna appears to have been a productive intelligence channel.¹⁸³

Viewed in summation, the existence of formal international commitments aided intelligence assessments at multiple junctures.¹⁸⁴ The IAEA's limited monitoring of the Indian and Argentine programmes were important inputs to proliferation assessments, supporting the monitoring mechanism most. Except for India's surprising use of foreign-supplied technology in the 1974 PNE, these two cases provide the most robust evidence for the screening mechanism of nonproliferation agreements. Although it was not much use for Argentina, the differentiation mechanism's effectiveness could be observed in India's post-PNE approach to safeguards.

Proposition 3. Assessment accuracy is a function of collected information.

Because the precise information available to intelligence analysts when the assessments were written is not accessible, directly tracking the acquisition and processing of intelligence is not possible. A circumstantial analysis is still feasible by first establishing that the three intelligence communities had sufficient means, motives, and opportunities to gather information about both nuclear programmes before evaluating how efficient they were in converting that information into knowledge. This section concludes with a consideration of the obstacles that stood in the way of using available information effectively.

As intelligence targets, the two nuclear programmes presented different challenges. India did not hide its facilities and, as an unfettered democracy, produced a great range of nuclear signals. The task for the assessors was to sort through the abundance. The country may even have been unusually accommodating to foreign intelligence services.¹⁸⁵ Argentina operated a clandestine facility under a closed political system for much of this period.

The United States intelligence community exceeded the others in its global collection capability, followed by the United Kingdom. The two actively exchanged raw intelligence and finished analyses on the Indian nuclear programme through the Five Eyes arrangement.¹⁸⁶ West Germany was far behind in its collection capability and not a part of Five Eyes intelligence exchanges. However, like the others, it had the theoretical advantage of reading Argentina's 'naval and diplomatic communications', something Britain did not invest in collecting before the Falklands War.¹⁸⁷

The three assessors varied in information sources from intelligence channels. West Germany was the most active nuclear exporter, enjoying unusually close ties to Argentina's nuclear sector. Its connection to India included the expectation that German scientists would not have been surprised by the PNE and that it would receive technical data resulting from the test.¹⁸⁸ Their harmonic views on nuclear matters were discussed at the highest levels between the two governments.¹⁸⁹ Britain and the United States exported to India, at least in the early stages of the programmes. Britain entered a competition with West Germany to supply a reactor to Argentina in the years leading to the Falklands War. For much of the study period, the US Atomic Energy Commission had a representative in Buenos Aires to follow nuclear developments.¹⁹⁰

These variations in information access are in part reflected in the accuracy of proliferation assessments. Nuclear technology cooperation appears to have increased accuracy, allowing West Germany deep insight into nuclear capabilities despite its intelligence collection disadvantage. The effect was pronounced as Argentina relied less on international cooperation in its infrastructure, making German intelligence less more hesitant about its South American partner's capabilities. Further fulfilling the proposition's expectations, the United States with its intelligence collection reach was closest to detecting the Pilcaniyeu uranium enrichment facility.¹⁹¹



In the assessments, current target country capabilities were usually reflected accurately. Making predictions about the future direction of nuclear programmes proved far harder, especially when this required modelling the intent animating their development.¹⁹² The many instances in which analysts confessed their ignorance resulted from confusion about state intent far more frequently than over capability.

Assessing intent requires estimating how foreign decision-makers will react to possible future developments and who those decision-makers will be and who might influence their decisions. There were frequent references to political considerations, like the hawkishness of the governing party that might result from India's elections or a coup in Argentina. Budget constraints occasionally appeared in the assessments without adding much analytical value.¹⁹³ However, these were rarely treated with the same rigour as the technical and external security analyses, demonstrating that technical and political analyses require different skillsets.¹⁹⁴

Subjective analytical spaces marked by 'the complexity of the subject matter, the small and biased sample of cases available for study, the conditions under which learning takes place, and the decision-makers' failure to realise how much they are influenced by their views of the past' offer cognitive biases the opportunity to thrive.¹⁹⁵ For example, US analysts were drawn to security competition to explain nuclear conduct, perhaps mirroring their own competition with the Soviet Union. Assessors may be trained to recognise and combat biases.¹⁹⁶ However, even sophisticated analysts and policymakers are susceptible to cognitive errors.¹⁹⁷ In addition to peer review, being part of a community of like-minded analysts can also be a source of error.¹⁹⁸

Finally, internal information management difficulties obstructed the translation of available intelligence into accurate assessments. British and American intelligence were not efficient in converting sizeable resources into accurate assessments of the Indian programme. In the post-mortem of its failure to give warning of the PNE, the US intelligence community found:

Inadequate priority against an admittedly difficult target, and lack of adequate communications among those elements of the community, both collectors and producers, whose combined talents were essential to resolving the problem. (...) The few reports which did provide indications of Indian intentions were given scant attention by the production analysts and were inadequately followed up by the collectors. Compounding this lack of priority was the general assumption by (...) collectors that the other guy was primarily responsible for producing hard evidence of Indian intentions.¹⁹⁹

Knowledge management while protecting secrets is a perennial problem for intelligence work and can be observed interfering in the cases. In 1970, for example, British intelligence had difficulty accessing relevant information on India – from the FCO.²⁰⁰

The three intelligence communities did not operate as efficient information processors. While it was true that the more analysts knew about their target's nuclear infrastructure, the better they could describe it, intent was a different matter: More raw intelligence on state intent did not reliably lead to a clearer picture of the target's nuclear present and future. These cases demonstrate the limits on how much information states can acquire about another state's nuclear decision-making.

Conclusion

Foreign nuclear programmes are challenging intelligence targets. The empirical and comparative evidence presented in this article shows how factors related to the target nuclear programme and the relationship with the assessing state systematically contribute to greater and lesser accuracy.

First, if a state is believed to be in a nuclearised security competition with a rival, it is more likely for intelligence agencies to overestimate its proliferation potential. Second, international nonproliferation agreements' screening function provides useful information, although the correct interpretation poses challenges. Finally, the relationship between information quantity and assessment accuracy is far more complex than rationalist models of perception and even deterrence can accommodate. This ought to be cause for alarm.

Intelligence scholars may share the alarm, but not the surprise. While they may marvel at the naiveté of some IR assumptions about governments' talents in rational information processing, they may appreciate that the above results have demonstrated the value of structural theories for the study of intelligence.

These observations are drawn from a narrow set of Cold War circumstances. Intelligence agencies presumably have drawn their own conclusions and adjusted their practices, but technological progress has not made it any easier to assess intent. Intelligence will continue to err. As wide as the gap between them appears, abstract IR theories and practical intelligence scholarship can at least agree to be pessimistic about the ability to separate proliferation facts from fallacies.

Alexander K. Bollfrass is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich and a Research Affiliate with the Nuclear Knowledges program at CERISciencesPo. The work for this paper was conducted within the ANR funded VULPAN project and early results were presented at a VULPAN workshop in November 2018.





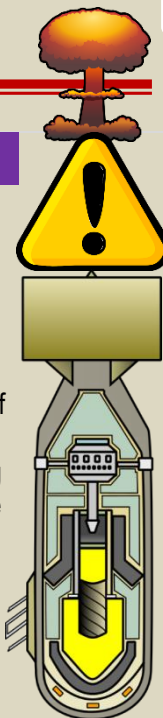
Iran Can Produce One Nuclear Weapon in as Little as Three Weeks

Source: <https://www.homelandsecuritynewswire.com/dr20211126-iran-can-produce-one-nuclear-weapon-in-as-little-as-three-weeks>

Nov 26 – The [Institute for Science and International Security](#) has issued a [study](#) summarizing and assessing information in the International Atomic Energy Agency’s (IAEA) quarterly safeguards report for 17 November 2021. The IAEA’s quarterly report, [Verification and Monitoring in the Islamic Republic of Iran in Light of United Nations Security Council Resolution 2231 \(2015\)](#), includes Iran’s compliance with the Joint Comprehensive Plan of Action (JCPOA).

The IAEA’s latest report details Iran’s rapidly advancing nuclear activities and steps to limit IAEA monitoring, indicating the inspectors’ diminished ability to detect Iranian diversion of assets to undeclared facilities. The Institute for Science and International Security notes that, at the same time, the IAEA has made no progress on resolving outstanding safeguards issues relating to the presence of undeclared nuclear material and activities in Iran.

Here are the highlights of study by the Institute for Science and International Security:



Highlights and Breakout Estimate

- ❖ Iran has enough enriched uranium hexafluoride (UF₆) in the form of near 20 and 60 percent enriched uranium to produce enough weapon-grade uranium (WGU), taken here as 25 kilograms (kg), for a single nuclear weapon in as little as three weeks. It could do so without using any of its stock of uranium enriched up to 5 percent as feedstock. The growth of Iran’s stocks of near 20 and 60 percent enriched uranium has dangerously reduced breakout timelines.
- ❖ Iran could continue producing more weapon-grade uranium, using its substantial stock of uranium enriched between two and five percent. In just over two months after the commencement of breakout, Iran could have produced enough additional WGU for a second weapon. After about 3.5 months, it would have enough for a third weapon. The additional production of enough WGU for a fourth weapon would be slower, taking six months, reflecting the depletion of Iran’s pre-existing stocks of enriched uranium.
- ❖ Iran appears to have continued producing near 20 percent enriched uranium metal, although the IAEA does not provide details in its latest report. Despite Iran’s claims of civil use, uranium metal is a key material in nuclear weapons. Iran’s move to create the wherewithal to make uranium metal as well as making the metal itself is concerning because Iran is both instituting a nuclear weapons capability and increasing its knowledge and experience in this key area.
- ❖ Iran experimented with using near 20 percent enriched uranium as feed in advanced centrifuges at the Natanz Pilot Fuel Enrichment Plant (PFEP), likely gaining important new knowledge in producing highly enriched uranium (HEU) using advanced centrifuges. This is also the first time Iran has started feeding a centrifuge cascade with uranium enriched more than 5 percent at any of its three enrichment plants, possibly gaining additional, irreversible knowledge in setting up and using equipment designed for smaller feed quantities and higher enriched uranium feed.
- ❖ In essence, Iran is effectively breaking out slowly by producing 60 percent enriched uranium and continuing to accumulate it. As of November 6, Iran had a stock of 17.7 kg of near 60 percent enriched uranium (in uranium mass or U mass), or 26.1 kg (in hexafluoride mass). If Iran accumulated about 40 kg of 60 percent enriched uranium (U mass), it would have enough to be able to further enrich it and quickly produce 25 kg of weapon-grade uranium (U mass) in just a few advanced centrifuge cascades.
- ❖ Alternatively, 40 kg of 60 percent enriched uranium is more than enough to fashion a nuclear explosive directly, without any further enrichment, although Iran’s known nuclear weapons designs use WGU.
- ❖ Iran’s current production rate of 60 percent enriched uranium is 42 kg per year (U mass), meaning that it could accumulate its first amount of 40 kg in about 6.4 months, or by the spring of 2022.
- ❖ Iran is learning important lessons in producing WGU and breaking out to nuclear weapons by experimenting with skipping typical enrichment steps as it enriches up to 60 percent uranium-235. It is starting from a level below 5 percent LEU and enriching directly to near 60 percent in one cascade, rather than using two steps in between, a slower process entailing the intermediate production of 20 percent enriched uranium. Iran is also implementing a plan to allow IR-6 cascades to switch more easily from the production of 5 percent enriched uranium to 20 percent enriched uranium. As such, Iran is experimenting with multi-step enrichment while seeking to shortcut the process.
- ❖ Iran is also improving its ability to recycle tails from its 60 percent enriched uranium production, recovering about 50 percent of the needed 5 percent LEU feed and producing tails closer to 2 percent enriched uranium.
- ❖ The production rate of 20 percent enriched uranium at the Fordow Fuel Enrichment Plant (FFEP) and PFEP remained constant for this reporting period, at a monthly average of 13.2 kg (U mass), or 19.5 kg (hex mass).



- ❖ As of November 6, 2021, Iran had an IAEA-estimated stock of 113.8 kg of 20 percent enriched uranium (U mass and in the form of UF₆), an increase from the previous reporting period's 84.3 kg of 20 percent enriched uranium in UF₆ form. Iran also has an additional stock of 34.2 kg (U mass) of 20 percent uranium in other chemical forms.
- ❖ In a new development, as of November 9, 2021, Iran installed 166 IR-6 centrifuges in a cascade at the FFEP. It also has a total of 23 IR-6 centrifuges in a second cascade. At the end of the last reporting period, only ten IR-6 centrifuges had been installed in this second cascade. The installation of advanced centrifuges at the FFEP enhances Iran's ability to break out using a declared but highly fortified facility.
- ❖ Using uranium metal, Iran made 20 percent uranium silicide and two fuel plates using the new silicide fuel for the Tehran Research Reactor (TRR). The fuel has yet to undergo quality control, but Iran's production of this type of fuel plate is unnecessary and a major violation of the JCPOA. It is likely a pretext to add to its nuclear weapons capabilities.
- ❖ The number of enriching IR-1 cascades and IR-2m cascades at the Natanz Fuel Enrichment Plant (FEP) appears to have almost fully recovered from a sabotage incident in April. Iran has installed 31 cascades of IR-1 centrifuges, six cascades of IR-2m centrifuges, and two cascades of IR-4 centrifuges at the FEP. Of those, as of November 13, 28 IR-1 cascades, six IR-2m cascades, and two IR-4 cascades "were being fed" with uranium.
- ❖ Iran's current operating enrichment capability is estimated to be about 12,400 separative work units (SWU) per year, compared to 11,700 SWU per year at the end of the last reporting period.
- ❖ Iran's total usable stock of below 5 percent LEU decreased just slightly compared to the previous reporting period. This stock did not change much because its increased use as feed to produce 60 percent enriched uranium at the PFEP was offset by a simultaneous increase in production at the PFEP.
- ❖ Near 5 percent LEU production during this reporting period, which spanned 69 days at the Natanz FEP, totaled 339 kg (U mass), with a daily average production rate of 4.9 kg (U mass), a slight decrease from the previous reporting period's daily average production rate of 5.26 kg (U mass). This reflects Iran's slightly increased enrichment capacity at the FEP, combined with its reverting to natural uranium feed rather than 2 percent LEU feed, which Iran had used intermittently during the previous reporting period.
- ❖ The IAEA report does not discuss the status of Iran's construction of a new advanced centrifuge assembly facility in a tunnel near the main Natanz complex.
- ❖ As noted in a separate IAEA report,³ and independent of problems caused by Iran's suspension of the AP and JCPOA monitoring, Iran has failed to cooperate with the IAEA regarding the agency's finding of uranium particles at three undeclared sites and answer questions about a fourth site, leading Director General Grossi to state, "The lack of progress in clarifying the Agency's questions concerning the correctness and completeness of Iran's safeguards declarations seriously affects the ability of the Agency to provide assurance of the peaceful nature of Iran's nuclear program."
- ❖ Iran has not turned over to the IAEA a missing recording unit and storage data from a camera that was destroyed at the TESA (or TABA) centrifuge manufacturing facility near Karaj, the site of a sabotage event in June.⁴ Iran has also not permitted the IAEA to re-install cameras at the site, reneging on a September 2021 agreement with the IAEA to permit the IAEA to service measurement devices and video cameras at the Karaj site and other nuclear sites. The IAEA states the agreement did not exclude the Karaj facility.
- ❖ Around five months have passed since the IAEA has had video monitoring at the TESA facility, raising concern that the IAEA cannot restore continuity of knowledge of events at the site. The IAEA has not had insight into how many advanced centrifuges Iran has made at the site since February, and therefore no awareness of whether Iran has diverted advanced centrifuges to a secret storage site, or for that matter, a clandestine enrichment plant.
- ❖ Even if Iran continues to permit the IAEA to service agency equipment, the verification process may now face such serious gaps that it is impossible to restore the IAEA's continuity of knowledge of Iran's nuclear activities, which is so vital to verification.
- ❖ Combined with outstanding safeguards issues in Iran, the IAEA has a significantly reduced ability to monitor Iran's complex and growing nuclear program, which notably has unresolved nuclear weapons dimensions. The IAEA's ability to detect diversion of nuclear materials, equipment, and other capabilities to undeclared facilities has greatly diminished.

Is China Plotting an EMP Attack? Only If It Wants World War 3

By Brian Hudson

Source: <https://sofrep.com/news/is-china-plotting-an-emp-attack-only-if-it-wants-world-war-3/>

Nov 27 – With China's recent hypersonic cruise missile test and its ever-expanding reach in the South China Sea, people wonder if perhaps China is plotting an electromagnetic pulse (EMP) attack on the United States. Problem is, in order to generate an EMP field large





enough to cause widespread outages, they would have to toss a multi-megaton nuke over the U.S., and then detonate it at the right altitude. Who thinks that would NOT start World War 3?

What Is an EMP?

EMP, or electromagnetic pulse, is a sudden burst of electromagnetic energy. Solar flares are the most common causes of EMP, but those are rarely large enough to cause more than minor disruptions on Earth. Good thing, too, because the right solar flare could knock out the entire Earth’s electrical grid. One old crusty civilian I worked with, blamed solar flares for most of the [C-5’s navigation problems](#). Interestingly, during times of increased solar activity, phantom communication and navigation problems were more abundant. Anyone in maintenance can tell you intermittent problems are the bane of every maintainers’ existence.



A right front view of an E-4 advanced airborne command post (AABNCP) on the electromagnetic pulse (EMP) simulator for testing. (Photo by Sgy Ernie Stone/U.S. Army)

Here on Earth, though, the mechanics of producing large-scale EMPs have only been accomplished through the use of nuclear weapons. Smaller EMP bursts can be produced using energy weapons, but these have a limited range and are more suited to disrupting individual systems or small areas. These non-nuclear EMP (NNEMP) weapons have promise, though.

EMP as Weapons

Fifth-gen fighter jets [loaded with NNEMP missiles](#), could conceivably penetrate enemy airspace and target air-defense systems, communications systems, and radar sites. With the right placement, these non-destructive weapons could cripple the command and control functions of an enemy state. Non-destructive is a relative term, however. While there will be



little to no physical carnage, electrical systems would be completely destroyed, requiring millions of dollars in repairs. All while having no communications and with no way to track further airspace penetration.

Numerous world powers, including the U.S., Russia, and China, all have some sort of NNEMP research and development programs. For obvious reasons that research is shrouded in secrecy, and very little has been done openly with this. In the 1960s, both the U.S. and Russia were hard at work developing more and more powerful nuclear weapons. During the Starfish Prime tests in 1962, a 1.4 megaton bomb was detonated 250 miles above the earth, roughly between the Marshall Islands to the west, and the Hawaiian Islands to the east. While EMP was already a known side effect of nuclear explosions, the range and effect of Starfish showed that these after-effects were a weapon in their own right.

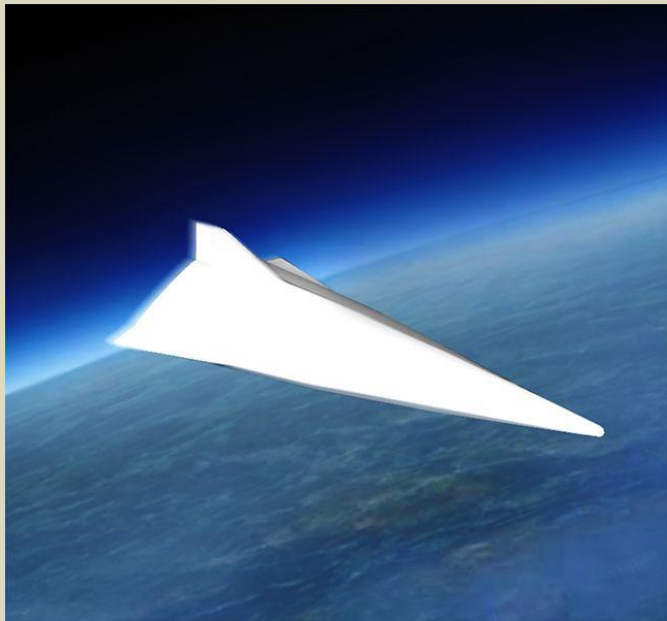
Shortly after the explosion, and in the months following, several unintended consequences of the test emerged. In Hawaii, about 900 miles from the detonation area, electrical grids failed, telephone systems were knocked out, and automobiles reportedly malfunctioned. Three satellites in low Earth orbit were quickly disabled, with at least six more failing over the next few months. These later failures were attributed to man-made radiation belts orbiting the Earth as a result of the testing.

Benefits to Nuclear Testing

One positive fallout from atmospheric and space testing (no pun intended) was the [Partial Test Ban Treaty](#). In 1963, the U.S., U.K., and Russian governments signed a treaty that would ban the nuclear weaponization of space. In part, the treaty banned atmospheric and underwater testing, and any testing that would allow fallout to stray outside the testers' control. The real meat of the treaty was a ban on placing nuclear weapons or any other weapons of mass destruction either in Earth's orbit or on any celestial body (the moon). By tacking on the descriptor "weapons of mass destruction," the treaty includes any weapon that can kill or incapacitate mass amounts of people, or cause massive damage to people, places, and things.

However, China did not, and has not, signed on to this treaty. The Republic of China (Taiwan for the non-politically correct bunch) ratified the treaty in 1964 before the UN recognized the People's Republic of China as the "One True China."

With [China testing out its newest hypersonic weapons](#), the idea of an EMP attack gains weight. While NNEMP weapons are still in development, tests of these systems will have to occur. At Eglin AFB, in 1993, an EMP generator being tested accidentally destroyed electrical systems in automobiles about 300 meters away from the testing site. Where is China in this testing cycle? That is anyone's guess.



One of the Chinese hypersonic gliding vehicle projects. Its configuration was first exposed by Military Report on CCTV-7. (Wikimedia Commons)

'It's The End of the World as We Know It!'

A famous quote often [attributed to Albert Einstein](#) goes like this: "I know not what weapons World War III will be fought with, but World War IV will be fought with sticks and stones." As glib as this quote may sound, its logic is chilling.

If the worlds' superpowers began lobbing nukes at each other, the aftermath would scar the Earth forever, most likely ending whatever technological advancements we have made. The idea of creating equal levels of destruction without the added benefit of making the Earth unlivable makes NNEMP weapons much more attractive.

Until the time when NNEMPs become more widespread and reliable, the most effective way of generating an EMP capable of more than minimal damage is through nuclear weapons. The problem of nuclear-weapon use is the doctrine of mutually-assured destruction. Once the enemy launches the first missile, the rest is history. Better start sharpening those sticks and stockpiling rocks; we're all going to need them.

Brian Hudson is a retired Air Force avionics technician. He spent twenty years working on multiple airframes, including the C-5 Galaxy, E-8 Joint STARS, C-130 SOF variants, and the B-1B Lancer, finishing his career at AF Global Strike Command HQ as the B-1B avionics manager.

EDITOR'S COMMENT: (title:) What if China does it first and in a big scale?



Who gave Israel nukes?

By Steve Sattler (Former Clinical Maxillofacial Surgeon (1974–2011); lecturer on WW1 in the ME, volunteer/Police)

Source: <https://www.quora.com/Who-gave-Israel-nukes>

This is a general question; and obviously there was an evolutionary process of both scientific and political intrigue.

1949–1956

Israel's first PM [David Ben-Gurion](#) was "nearly obsessed" with obtaining nuclear weapons to prevent the [Holocaust](#) from recurring. He stated, "What [Einstein](#), [Oppenheimer](#), and [Teller](#), the [three of them are Jews, made for the United States](#), could also be done by scientists in Israel, for their own people".

1... Ben-Gurion decided to recruit Jewish scientists from abroad even before the end of the [1948 Arab–Israeli War](#) that established Israel's independence. He and others, such as head of the [Weizmann Institute of Science](#) and defense ministry scientist [Ernst David Bergmann](#), believed and hoped that Jewish scientists such as Oppenheimer and Teller would help Israel.

2... In 1949 a unit of the IDF Science Corps, known by the [Hebrew](#) acronym HEMED GIMMEL, began a 2-year [geological survey](#) of the [Negev](#). While a preliminary study was initially prompted by rumors of [petroleum](#) fields, one objective of the longer 2-year survey was to find sources of [uranium](#); some small recoverable amounts were found in [phosphate](#) deposits.

3... That year Hemed Gimmel funded 6 Israeli physics graduate students to study overseas, including one to go to the [Uni/ Chicago](#) and study under [Enrico Fermi](#), who had overseen the world's first artificial and self-sustaining [nuclear chain reaction](#).

4... In early 1952 Hemed Gimmel was moved from the IDF to the [MOD](#) and was reorganized as the Division of Research and Infrastructure (EMET). That June, Bergmann was appointed by Ben-Gurion to be the first chairman of the [Israel Atomic Energy Commission](#) (IAEC).

5... Hemed Gimmel was renamed Machon 4 during the transfer, and was used by Bergmann as the "chief laboratory" of the IAEC; by 1953, Machon 4, working with the Department of Isotope Research at the [Weizmann Institute](#), developed the capability to extract uranium from the phosphate in the Negev and a new technique to produce indigenous [heavy water](#). The techniques were 2 years more advanced than American efforts.

6... Bergmann, who was interested in increasing nuclear cooperation with the French, sold both patents to the [Commissariat à l'énergie atomique](#) (CEA) for 60 mil. francs. Although they were never commercialized, it was a consequential step for future [French-Israeli cooperation](#). In addition, Israeli scientists 'helped' construct the G-1 plutonium production reactor and UP-1 reprocessing plant at [Marcoule](#). France and Israel had close relations in many areas. *France was principal arms supplier for the new Jewish state, and as instability spread through French colonies in North Africa, Israel provided valuable intelligence obtained from contacts with [Sephardi Jews](#) in those countries.*

7... At the same time Israeli scientists were also observing [France's own nuclear program](#), and were the only foreign scientists allowed to roam "at will" at the nuclear facility at Marcoule. In addition to the relationships between Israeli and French Jewish and non-Jewish researchers, the French believed that cooperation with Israel could give them access to international Jewish nuclear scientists.

8... 1955:- After [U.S. President Eisenhower](#) announced the [Atoms for Peace](#) initiative, Israel became the 2nd country to sign on, and signed a peaceful nuclear cooperation agreement with the United States on July 12, 1955. This culminated in a public signing ceremony on March 20, 1957, to construct a "small swimming-pool research reactor in [Nachal Soreq](#)", which would be used to shroud the construction of a much larger facility with the French at [Dimona](#).

9... In 1986 [Francis Perrin](#), [French high-commissioner for atomic energy](#) from 1951 to 1970 stated publicly that in 1949 Israeli scientists were invited to the [Saclay Nuclear Research Centre](#), this cooperation leading to a joint effort including sharing of knowledge between French and Israeli scientists especially those with knowledge from the [Manhattan Project](#).

10... **The Dimona project, 1956–1965.** The French justified their decision to provide Israel a nuclear reactor by claiming it was not without precedent. *In September 1955 Canada publicly announced that it would help the [India](#) build a heavy-water research reactor, the [CIRUS reactor](#), for "peaceful purposes".*



11... When Egyptian President [Nasser](#) nationalized the [Suez Canal](#), France proposed that Israel attack Egypt & invade the Sinai as a pretext for France and Britain to invade Egypt posing as "peacekeepers" with the true intent of seizing the Suez Canal. In exchange, France would provide the nuclear reactor as the basis for the Israeli nuclear weapons program.

12... [Shimon Peres](#), sensing the opportunity on the nuclear reactor, accepted. In September, 1956, Peres and Bergmann reached a tentative agreement in [Paris](#) for the CEA to sell Israel a small research reactor. *Israel benefited from an unusually pro-Israel French government during this time.*

13... After the Suez Crisis & the British & French were being forced to withdraw, then Ben-Gurion sent Peres and [Golda Meir](#) to France. During their discussions the groundwork was laid for France to build a larger nuclear reactor and chemical reprocessing plant, and PM [Guy Mollet](#), ashamed at having abandoned his commitment to fellow [socialists](#) in Israel, supposedly told an aide, "I owe the bomb to them." The [Chief of the Defence Staff](#), said, "We must give them this to guarantee their security, it is vital."

14... 1957:- The French–Israeli relationship was finalized on October 3, 1957, in two agreements whose contents remain secret:

*The result was that Israel was now able to produce 22 [kilograms](#) of [plutonium](#)/yr.

15... When the reactor arrived in Israel, PM Ben-Gurion declared that its purpose was to provide a pumping station to desalinate seawater & thus turn the desert into an "agricultural paradise". 6 of 7 members of the Israel Atomic Energy Commission promptly resigned, for political reasons.

16... 1957: Building it:- Before construction began it was decided that the project would be too big for the EMET and IAEC team, so Peres recruited Col. [Manes Pratt](#), then Israeli [military attaché](#) in Burma, to be the project leader. Building began in late 1957 or early 1958, bringing hundreds of French engineers & technicians to the [Beersheba](#) and Dimona area.

17... **LEKEM** 1959:- Peres had established and appointed a new intelligence service assigned to search the globe and clandestinely secure technology, materials and equipment needed for the program, by any means necessary. The new service would eventually be named [LEKEM](#), & Peres appointed IDF Internal Security Chief, Blumberg, as CEO. *As head of the LEKEM, Blumberg would rise to become a key figure in Israel's intelligence community, coordinating agents worldwide and securing the crucial components for the program.*

18... 1958:- When [de Gaulle](#) became [President](#) in late 1958 he wanted to end French–Israeli nuclear cooperation, and said that he would not supply Israel with uranium unless the plant was opened to international inspectors, declared peaceful, and no plutonium was reprocessed.

19... Through a series of negotiations, Shimon Peres finally reached a compromise with FM [de Murville](#) over 2 yrs later, in which French companies would be able to continue to fulfill their contract obligations and Israel would declare the project peaceful. Due to this, French assistance did not end until 1966. However the supply of uranium fuel was stopped earlier, in 1963.

20... Despite this, the French uranium company based in [Gabon](#) may have sold Israel uranium in 1965.

21... **British aid** [late 50s & early 60s] ...meanwhile, Britain made hundreds of secret shipments of restricted materials to Israel in the 1950s and 1960s. These included specialist chemicals for reprocessing and samples of fissile material—[uranium-235](#) in 1959, and plutonium in 1966, as well as highly enriched [lithium-6](#), which is used to boost fission bombs and fuel H bombs.

22... 1959–60:- Britain shipped 20 tons of [heavy water](#) directly to Israel in 1959 and 1960 to start up the [Dimona](#) reactor.

23... The transaction was made through a Norwegian front company called [Noratom](#), which took a 2% commission on the transaction. Britain was challenged about the heavy water deal at the IAEA after it was exposed but, the British claimed - this was a sale to Norway.

24... Israel admits running the Dimona reactor with Norway's heavy water since 1963. French engineers who helped build Dimona say the Israelis were expert operators, so only a relatively small % of the water was lost during the years since the reactor was first put into operation.

25... 1961:- [PM Ben-Gurion](#) informed the [Canadian PM Diefenbaker](#) that a pilot plutonium-separation plant would be built at Dimona. British intelligence concluded from this and other information that this "can only mean that Israel intends to produce nuclear weapons".

26... The nuclear reactor at Dimona [went critical](#) in 1962.

27... After Israel's rupture with France, the Israeli government reportedly reached out to Argentina. The **Argentine** government agreed to sell Israel [yellowcake](#) =uranium oxide.

From '63-'66 about 90 tons of yellowcake were allegedly shipped to Israel from Argentina in secret.

28... By 1965 the Israeli reprocessing plant was completed and ready to convert the reactor's [fuel rods](#) into [weapons grade plutonium](#).





29... **Costs:-** The cost \$80 mil. in 1960: half of which was raised by foreign Jewish donors, including many American Jews. Some of these donors were given a tour of the Dimona complex in 1968.

30... Israel begun full-scale production of N-weapons following the 1967 6-day war, although she had built her first functional N-weapon by Dec. '66.

EDITOR'S COMMENT: Quora is a website posting various (debate) questions that are answered by various experts or people with special knowledge on certain issues.

After acquiring nuclear weapons, Pakistan became more aggressive in using terrorist groups

Source: <https://www.timesnownews.com/international/article/after-acquiring-nuclear-weapons-pakistan-became-more-aggressive-in-using-terrorist-groups/836064>



Nov 28 – After becoming an overt nuclear power, Pakistan became emboldened to prosecute conflict at the lower end of the spectrum, confident that nuclear weapons minimise the likelihood of an Indian military reaction, The Rand Corporation said in a report in 2009 post the Mumbai attacks of 26/11.

In the wake of nuclearisation, substate conflict expanded dramatically. In 2001, a RAND analysis of the aforementioned Kargil crisis found that the Pakistani operation was enabled by the protective nuclear umbrella ensuring that India's conventional response would be constrained. Similarly, groups that were previously limited to the Kashmir theatre expanded into the Indian hinterland following the 1998 nuclear tests, the report said.

It added that the connections between LeT and Pakistan's Directorate for Inter-Services Intelligence (ISI) are well known, as are LeT's various camps and offices in Pakistan.

Moreover, India has been victimised by a host of militant groups based in and supported by Pakistan for decades. With the possible exception of the militant groups associated with Jamaat-Islami, the so-called Kashmir tanzeems have been raised, nurtured, assisted, and trained by the ISI. As such, these groups are not strictly nonstate actors but rather extensions of the state intelligence apparatus, albeit with some degree of plausible deniability, the report had said.



Compelling Pakistan to roll up Lashkar-e-Taiba's terrorism infrastructure was identified as a key priority in US Senate hearings in 2009 in the aftermath of the Mumbai attacks of 26/11.

US officials testified that LeT's vast infrastructure of terrorism within Pakistan is directed not only at India, but fundamentally today against US operations in Afghanistan, secondarily against US operations in Iraq, and finally against Pakistan itself.

"We have to work with both the civilian regime, the Zardari government that detests the LeT and detests extremist groups in Pakistan, as well as the Pakistani military with whom we cooperate in our operations in Afghanistan, but regrettably still seems to view support to groups like LeT as part of its grand strategy vis-a-vis India," the testimonies said.

Pakistan continues to play a prominent and problematic role in the overlapping armed conflicts and terrorist campaigns in India, Afghanistan, and in Pakistan itself, the hearings noted. Al Qaeda, the Taliban, LeT, and other insurgent and terrorist groups find sanctuary in Pakistan's turbulent tribal areas. Historically, some of these groups have drawn on support from the Pakistan government itself, officials said.

Indeed, some analysts suggest that Pakistan, since it acquired nuclear weapons, has been willing to be more aggressive in the utilisation of these groups, confident that with nuclear weapons, it can deter or contain violence from going to the higher levels. On the other hand, Pakistan's principal defence against external pressure may not be its nuclear arsenal but its own political fragility, that is, that its government's less than full cooperation may be preferable to the country's collapse and descent into chaos.

Officials said the attackers were able to exploit India's vulnerabilities and create a political crisis in India. They also sought to create a crisis between India and Pakistan that would persuade Pakistan to deploy its forces to defend itself against a possible action by India, which in turn would take those forces out of the Afghan frontier areas and take the pressure off Al Qaeda, Taliban, and the other insurgent and terrorist groups that operate along the Afghan frontier.

"On the diplomatic front, we clearly must redouble our efforts to persuade and pressure states like Pakistan that tolerate terrorist safe havens. It is particularly important in Pakistan, given that many of the attacks against the United States and our allies, both failed and successful, have had links to Pakistani-based groups, particularly Pakistani-based training camps," officials said.

A uniquely Turkish nuclear energy tale

By Şebnem Udum

Source: <https://thebulletin.org/2021/11/a-uniquely-turkish-nuclear-energy-tale/>

Nov 24 – Turkey's founders drew lessons from the role of foreign debt in the collapse of the Ottoman Empire. That is, prior to the proclamation of the republic in 1923, they focused on economic development. The country's energy mix of coal, hydroelectricity, and natural gas came to be dominated by natural gas imports from Russia starting in the 2000s. Turkey had tried and failed to add nuclear to its energy basket in the 1970s, 1980s, and 1990s for political and economic reasons. During that time, Turkey either consulted with or engaged in nuclear cooperation talks with Argentina, Canada, Germany, France, South Korea, Sweden, and the United States. Later, in 2007, Turkey solicited bids. Only Russia responded, but its bid failed as the proposed unit price was too high. Eventually, Russia and Turkey signed an intergovernmental agreement in 2010 in which the former would provide the latter with nuclear technology and fuel, which in some quarters deepened Turkey's concern about being dependent on Russia for energy.

International proponents of nuclear energy tout its affordability, environmental friendliness, and ability to provide abundant, uninterrupted electricity. Meanwhile, international nuclear energy opponents born from the 1960s and '70s antinuclear movement were first concerned with nuclear testing and later with nuclear waste disposal. Since Turkey maintained a closed economy until the 1980s, its nuclear energy debate remained independent as well. Unlike the international debate, Turkey's nuclear energy debate has been shaped by its struggle with development, progress, and identity.

Turkish citizens began to grow concerned about nuclear safety in the mid-1970s, but anti-nuclear opposition started in earnest after 1986, when the Chernobyl nuclear accident affected the northern coast of Turkey. Though official government statements underplayed Chernobyl's impact on the region, Turkish public perception of nuclear hazards remained—and remains—high. This is due, in part, to an increase in cancer deaths in the Black Sea region, including a famous rock singer, Kazim Koyuncu, who died of cancer in 2005, at the age of 32. Turkish citizens engaged in anti-nuclear protests, demonstrations, and rock concerts highlighting Chernobyl's impacts. When Greenpeace later arrived in Turkey, the organization added environmental concerns to the discussion. Before and around the 2011 Fukushima nuclear disaster, Turkey entered what many have dubbed a "nuclear renaissance." Demand for oil and natural gas had increased at the same time global availability of these resources decreased, due in part to Chinese and Indian economic policies. The Fukushima disaster reminded Turkish citizens of Chernobyl, while also highlighting the potential for natural disasters. On the one hand, anti-nuclear advocates both in Turkey and abroad felt emboldened. On the other hand, proponents trumpeted Japan's continued reliance on nuclear energy while strengthening safety measures.

Both sides of the nuclear energy debate in Turkey offer convincing arguments for uninformed audiences. They use words like “development,” “energy security,” and “environmental protection,” though with different expected policy outcomes. I attended a nuclear energy panel in 2008 in Ankara; one presenter highlighted the benefits of nuclear power on the basis of energy security criteria (reliability, affordability, and environment-friendliness), while anti-nuclear audience members argued against nuclear power because it was dangerous, expensive, and harmful to the environment. After both sides had accused each other of “treason,” the debate intensified—and I worried a physical fight would break out.

In Turkey’s nuclear energy debate, both proponents and detractors emphasize a need for reducing dependence on foreign energy sources and for promoting economic development. While the antinuclear coalition ranks environmental preservation higher, even it supports the state’s drive to maintain political and economic power.

Some Turkish terms are unique to the country. For example, Ankara formulated the concept of *yerli ve milli*, meaning “indigenous and national,” to reduce dependence on foreign sources in technology-intensive energy and defense sectors. Russia and Japan had planned to build Turkey’s nuclear power plants in Akkuyu by the Mediterranean and Sinop on the Black Sea coast respectively. As the current government sought to overturn previous administrations’ reliance on foreign suppliers, particularly in the defense, energy, and metals industries, “indigenous technology” became *synonymous* with “self-reliance.”

Turkey’s first nuclear power plant is under construction in Akkuyu, with an expected operational date in 2023—the 100th anniversary of the republic’s establishment. Turkish nuclear energy proponents anticipate celebrating their country’s entrance into the global “nuclear club.” Opponents worry that, as a newcomer, Turkey will struggle to establish sufficient nuclear safety measures. For example, they point to a lack of environmental impact assessments.

Citizens near the Akkuyu nuclear power plant construction site appear to have accepted the plant in their midst, at least based on my observations during a trip to Taşucu—the closest town to Akkuyu—in the summer of 2021. The construction site’s large security perimeter has quieted anti-nuclear and environmental activist activity. Social unrest is focused on the significant influx of Syrian refugees in Mersin, the central town of the formerly İçel province, where Akkuyu is located. Yet Taşucu’s long coastline has recently become a point of attraction, in a way similar to the French Riviera or Miami Beach. White- and blue-collar Russian employees of the nuclear power plant and their families have turned the environs into a collection of natural and historical sites for tourism. Residents are thriving economically, because of increasing demand for agricultural products, fish, hotels, rental houses, and restaurants. The Taşucu harbor’s importance has risen as ships transport construction materials. Infrastructure renovations have improved land transportation as well. New social facilities and construction have revitalized the local economy—none of which likely would have happened without the construction of a nuclear power plant.

Şebnem Udum earned a BSc. in international relations with a minor in international economics at Middle East Technical University, an MA in international policy studies and a Certificate in nonproliferation studies at MIIS, and an MA and PhD in international relations at Bilkent University. She was a research associate at the James Martin Center for Nonproliferation Studies (2002-2003) and former chair and member of International Nuclear Security Education Network (INSEN) at the IAEA. She is an associate professor in the Department of International Relations, Hacettepe University, Turkey and Director at the Center for Strategic Research at Hacettepe University.

EDITOR’S COMMENT: Author’s high-profile CV is in contrast with the unilateral focus of her article.

UN chief calls for nuclear weapons-free Middle East

By Ella Geris | Victoria U. Wellington Faculty of Law, NZ

Source: <https://www.jurist.org/news/2021/11/un-chief-calls-for-nuclear-weapons-free-middle-east/>

Nov 30 – The UN Secretary-General António Guterres, at the second session of the Conference on the Establishment of a Middle East Zone Free of Nuclear Weapons and Other Weapons of Mass Destruction on Monday, [called](#) on all Middle East states to put into reality the vision of a region with [no weapons of mass destruction](#).

Guterres stated that “achieving a zone free of nuclear weapons and other weapons of mass destruction will eliminate the possibilities of nuclear conflicts in the region and contribute to realizing a world free of nuclear weapons.” He noted that it would contribute to achieving just, lasting and comprehensive peace in the Middle East. He also called on all invited states to join the conference process and to contribute to this endeavor.

Since 1967, **five zones free of nuclear weapons and other weapons of mass destruction** have been established in Latin America, the Caribbean, the South Pacific, Southeast Asia, Africa, and Central Asia. This includes 60 percent of all UN member states and covers almost all of the Southern Hemisphere.

The Conference on the Establishment of a Middle East Zone Free of Nuclear Weapons and Other Weapons of Mass Destruction held its first session from November 18 to November 22, 2019 in New York. It adopted a [political declaration](#) and released a [final report](#).

Guterres congratulated all participating states for their determination and commitment to “an open and inclusive approach, as demonstrated by the Political Declaration reached at the first session of the Conference, under the Presidency of the Hashemite Kingdom of Jordan.”

EDITOR'S COMMENT: Either the Secretary-General is a man of great humor or the UN is a big joke. Do they think that certain Middle East countries (e.g., Turkey @ Akkuyu) is building a nuclear power plant just for electricity production (as naively described in the previous article)? Does the UN think that they share utopic proposals such as a Middle East Zone Free of Nuclear Weapons and other WMD? Come on! Be pragmatic!

Hesiod describes an ancient nuclear holocaust

Source (in Greek): https://www.diadrastika.com/2012/10/blog-post_4754-4.html

In the texts of ancient peoples, there is a description of a terrible war that shook the whole Earth. This war, which may have been the cause of the beginning of the decline of that civilization, was waged with the use of sophisticated weapons.

The descriptions of the ancient texts convey the image of a conflict, which caused severe destruction. That age-old conflict probably resulted in a nuclear holocaust.

It seems extreme, but reading the descriptions of ancient traditions one cannot help but think of such a possibility. References to "a missile that shut down the power of the universe", to a "white-light glow" and an "unprecedented fire that poured everywhere", to "a deadly dust" that covered those who survived the catastrophe, can hardly be to go unnoticed. It is worth quoting the texts of the peoples, in which, among other things, the reader can discern the great similarities that exist, and draw his own conclusions.

From the Theogony of Hesiod, where the description of that terrible war between the "Gods" and the "Titans" is made, we transfer the following characteristic passage: "The land was boiling and the sea was endless, and the Titans were engulfed in a hot breath. And as the flame went up in the sky, no matter how brave they were, the Titans were blinded. They were blinded by the white light from the lightning. Heat, unprecedented fire was pouring everywhere. And what the eyes saw, and what the ears heard, it was as if heaven and earth were mixed.

One researcher might well have suspected that the "lightning of Jupiter" that was the weapon that gave the "Gods" victory over Titans was nothing different from today's nuclear bomb.

Even more characteristic is the description in the Indian text "Popol Vux":

". An iron thunderbolt fell from heaven to earth. The corpses of the men of the tribe of Vrishnes, and Anchikas. became unrecognizable. "Their hair and nails had fallen out, the birds' feathers had changed color, the food had been poisoned and those who survived the catastrophe had been covered in deadly dust."



The Indian Bible, the Mahabharata¹, states:

"It was a missile that enclosed the power of the Universe. It was a pillar of smoke and flame brilliant, like ten thousand suns, rising with all its might 'H It was a new and unknown weapon, an iron thunderbolt that reduced the tribes of Vrishnes and Andakas to ashes...

The bodies were burned, and no one could recognize them. Hair and nails fell from the bodies. The birds turned white... A few hours later all the food was contaminated... To escape this fire, the soldiers fell into the rivers with their clothes and weapons... A hot wind started blowing...

The Universe was shrouded in heat as if it were sick with a high fever. The elephants and other war animals were struck by the force of the weapon... The waters became so hot that whatever lived inside them caught fire...

... A fatal spear, like a stick of death. It measured three cubits and six feet. Endowed with the power of lightning 'lthe man with a thousand eyes... devastating to all living creatures... "

The striking resemblance between the descriptions of "Voroι Vux" and "Mahabharata", as well as the provocatively similar names of the tribes "Vrishnes and Anchikas" on the one hand and "Vrishnis and Andakas" on the other, lead us to the conclusion that these two texts describe the same event.


Elsewhere in the Mahabharata, we read about the collision in the air of two of the above-mentioned weapons: "δύο The two weapons met each other in the middle of the air. Then the earth began to tremble along with all its mountains and seas and trees, and all living creatures were burned by the energy of the weapons and badly affected. The heavens were on fire and the ten points of the horizon were filled with smoke... "

The Old Testament description of the destruction of Sodom and Gomorrah can also be described as a mythological depiction of the sufferings of that great war:

"Lord rained upon Sodom and Gomorrah Pheon, and fire from heaven, and destroyed these cities, and all that is round about them..."

Another interesting element that the ancient traditions convey to us, is that of the construction of the famous lightning of Zeus by the Cyclops. According to Ancient Greek mythology, the Cyclops were the ones who created this invincible weapon, which they gave to Zeus to defeat the Titans.


From the "Comments of Artemis," we read the opinion of Eratosthenes who claimed that the conspiracy of the Gods against the Titans took place in the "altar", where the Cyclops made the terrible weapon, "I have a cover over the fire, so as not to see the lightning power". Are we talking here about a nuclear power plant, whose walls protected it?



OAK RIDGE INSTITUTE FOR SCIENCE AND EDUCATION
Managed by ORAU for DOE

reacts
The Radiation Emergency Assistance Center/Training Site

The Medical Aspects of Radiation Incidents



¹ The Mahābhārata is one of the two major Sanskrit epics of ancient India, the other being the Rāmāyaṇa. It narrates the struggle between two groups of cousins in the Kurukshetra War and the fates of the Kaurava and the Pāṇḍava princes and their successors.

America Needs Better Information About Nuclear Weapons States

By Alexandra B. Hall

Source: <https://nationalinterest.org/blog/skeptics/america-needs-better-information-about-nuclear-weapons-states-196865>

Nov 22 – It has been over a year since candidate Joe Biden ran on a [platform](#) that emphasized diplomacy with key nuclear powers and called for a [reassessment](#) of the reliance on nuclear weapons in U.S. national security policy. However, a year in, Terrell Jermaine Starr says, “I have to ask, is Biden really serious about nuclear disarmament?”

Starr is the founder and host of the foreign policy podcast [Black Diplomats](#), which is dedicated to discussing international politics and culture from the perspective of people of color. On the latest episode of [Press the Button](#), Starr joins co-host Michelle Dover to discuss what truly makes a secure and safe world when it comes to nuclear weapons.

Starr first points to the lack of understanding in the U.S. media and policymaking on Iran. He notes, “Iran is talked about in mainstream media with little to virtually no context. We’re already dealing with a press corps that severely misunderstands how nuclear weapons work, doesn’t understand disarmament, and our media have picked Iran as the boogeyman.” Furthermore, he notes the media and policymakers inaccurately portray the reality of the current challenge regarding the Iran nuclear agreement. He highlights that we need to be more clear that it was the United States, under then-President Trump, that withdrew from the [Joint Comprehensive Plan of Action](#) (JCPOA) and that until the U.S. withdrawal, Iran was complying with the agreement. Starr also points out that Iran has “sworn that they don’t have an interest in...enriching uranium to the point where they can create a weapon,” consistent with its obligations under the Non-Proliferation Treaty.

With negotiations to return to the JCPOA set to resume at the end of November, Starr says he will be interested to see how it is covered by the media, and what the United States and Iran bring to the negotiation table. Starr’s own podcast, *Black Diplomats*, will feature Iranian experts in an upcoming series called “Iran in Context” in the hopes of increasing deeper education on the country.

The lack of context and understanding of nuclear weapons issues is not unique to Iran. Starr pivots to China to highlight another case in point. After China’s recent [hypersonic missile](#) test General Mark Milley said it was “very close” to a “Sputnik moment.” Starr calls the reference an “extreme exaggeration,” especially given the [little information](#) about the test. But more importantly, Starr points out that China has already had capabilities to strike the United States with a nuclear weapon and “this is just another piece of technology that most people are not going to get, but they’re going to overreact to.”

the bigger picture, Starr sees China playing the long game—building up weapons systems based on their expectation that Trump will be the Republican Party’s 2024 Presidential Nominee—rather than focusing on the current Biden administration’s posture. “Given that Trump has attacked our own democracy, I think that the concerns of Beijing are quite legitimate...I think they are worried about their own defenses,” he explains. The fact that Iran desires confirmation that the United States will not renege on the JCPOA also expresses their concern that another president, after Biden, might have another policy preference.

Starr fears this rhetoric in the media and among policy makers about the danger of enriching uranium, or new weapons developments, simply stokes a “ratcheting up the potential of an arms race.” One of the biggest challenges Starr notes—and hopes to address in his upcoming *Black Diplomats* series—is getting people to ponder: “why are people telling me that these violent weapons are going to make me secure when we have hundreds of thousands of people who are dying from COVID-19, and millions who are getting sick by it?”

So, where do we go, and how do we get a return to the JCPOA, a shift away from overblown Pentagon budgets and new missile tests, and avoid an arms race with China? Starr hopes that the Biden Administration will take bold steps towards disarmament as promised on the campaign trail. Unfortunately, thus far, he notes “the Biden administration has not signaled that they are ready to have a cultural shift” when it comes to the nuclear status quo.

To change this, Starr says the disarmament and nonproliferation communities “need to educate the American public about what safety and security is, and make this a coffee table conversation where we discuss how ridiculous and how useless these weapons are, and how much of a burden they are on the taxpayer, and talk about the benefits of what it means to divest from nuclear weapons development and to invest in things like education, in climate change, [and] in food.”

Looking ahead, Starr says this movement “is going to have to be as grassroots as the Defund the Police movement.” This is the energy we need to redefine ‘safety’ and to get the message across that nuclear weapons do not make the world more secure.

The entire interview with Terrell Jermaine Starr is available [here](#) on *Press the Button*. You can learn more about Starr’s work on his [website](#), and listen to [Black Diplomats](#) wherever you get your podcasts. Starr’s upcoming series ‘Iran in Context’ is funded by the Ploughshares Fund’s Mary Estrin award, which Starr was awarded earlier this year. You can also look for his upcoming book, *Black Man on the Steppes: An Odyssey from Detroit to Eastern Europe*.



Alexandra B. Hall is the policy associate and special assistant to the president at Ploughshares Fund, a global security foundation.

US begins production of its latest air-dropped nuclear munition

Source: <https://newatlas.com/military/usa-production-b61-12-air-dropped-nuclear-munition/>



The B61-12 is the latest variant of the B51 Cold War bomb (NNSA)

Dec 09 – The United States Department of Energy’s National Nuclear Security Administration (NNSA) has begun production of the country’s latest air-dropped nuclear weapon variant. The agency announced that on November 23, the **B61-12 Life Extension** Program First Production Unit rolled off the line as the first of a projected 400 to 500 warheads.



Developed during the Cold War, the B61 has been America’s main air-dropped nuclear bomb since it was deployed in 1968. Unlike the larger strategic B83 bomb, it can not only be carried by heavy bombers like the B-52 and the B-2, but also by a wide variety of fighter aircraft flown by the US Air Force and NATO countries.

EDITOR’S COMMENT: Since “Life Extension” is a bit ironic name for a nuclear bomb, we propose a more suitable name for the new human achievement!

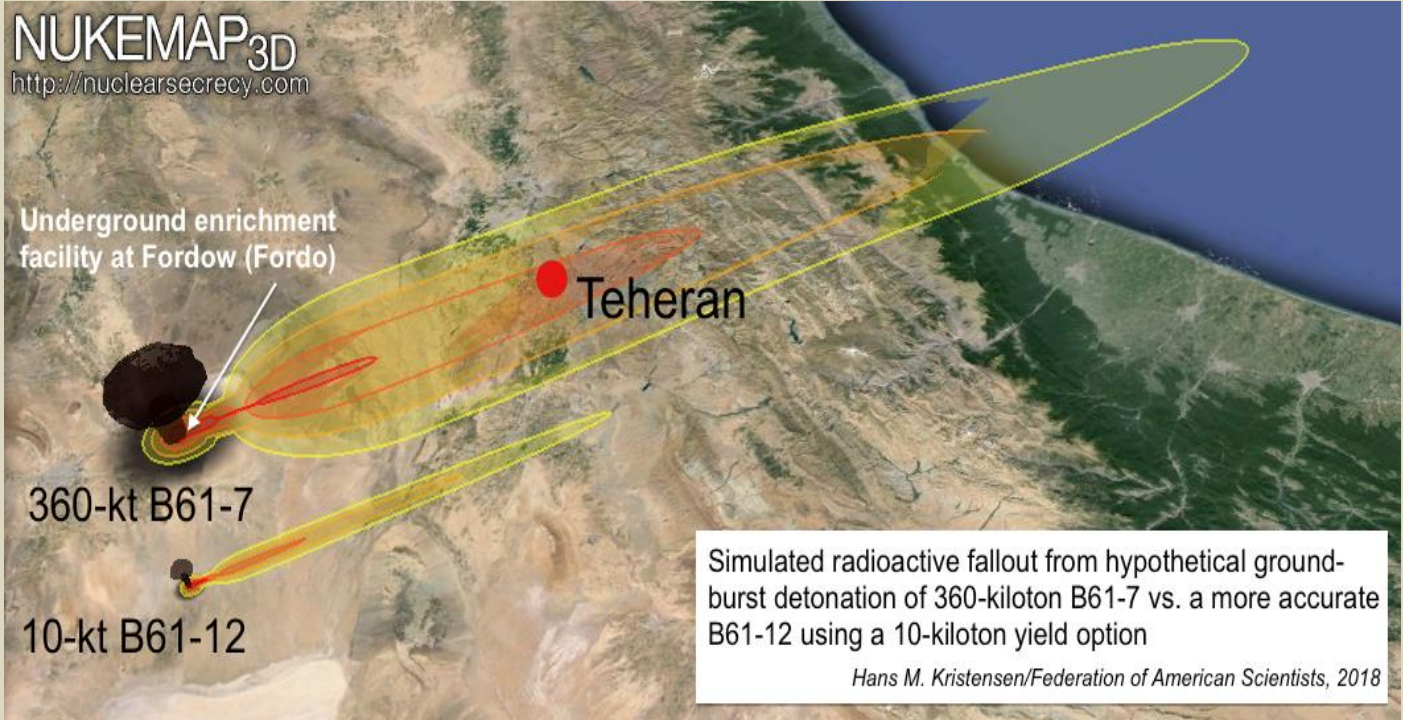
There are currently four versions of the B-61: the 3, 4, 7, and 11. Three of these are tactical nuclear weapons and one is a strategic nuke, but they share a variable yield design that allows them to explode with a force between 0.3 and 340 kilotons of TNT as desired. In addition, they can carry a variety of fuses and can either drop on a ballistic arc or retard their forward flight by using air drag to drop almost straight down.

Unfortunately, these variants are not only obsolete, they are also so old that they are in danger of no longer functioning. After decades of debate and nine years of development, the





US Defense Department decided to upgrade the B61 by introducing a new variant called the B61-12, which refurbishes, recycles, or replaces all the nuclear and non-nuclear components.



The reason for this is not only to replace three of the previous four variants with one that will remain in service for another 20 years, but also, eventually, to replace the one-megaton yield B83. With the Cold War over, it would be hard to justify fielding such a large bomb in Europe or Asia and by equipping the B61-12 with the Boeing Tailkit Assembly, the new bomb can land within 30 m (100 ft) of its target, which means it can use a much smaller explosive yield of 0.3 to 50 kilotons to destroy it with much less collateral damage. The first B61-12 will enter service in May 2022 and the last production unit will be completed by 2026 at a cost of US\$28 million each. These 700-lb (320-kg) bombs will be compatible with most current bomber and fighter aircraft, as well as the new F-35 and the B-21 Raider.

"With this program, we're delivering a system to the Department of Defense that improves accuracy and reduces yield with no change in military characteristics, while also improving safety, security and reliability," says Jill Hruby, DOE Under Secretary for Nuclear Security and NNSA Administrator. "The work on the B61-12 will also ensure the warhead can be air-delivered on both current and future platforms to meet Department of Defense requirements."

ANN IST SUPER SANITÀ 2009 | VOL. 45, NO. 3: 246-250 

Types of radiation mass casualties and their management

Alicja Jaworska
*Department of Emergency Preparedness and Environmental Radioactivity,
 Norwegian Radiation Protection Authority, Oesteraas, Norway*



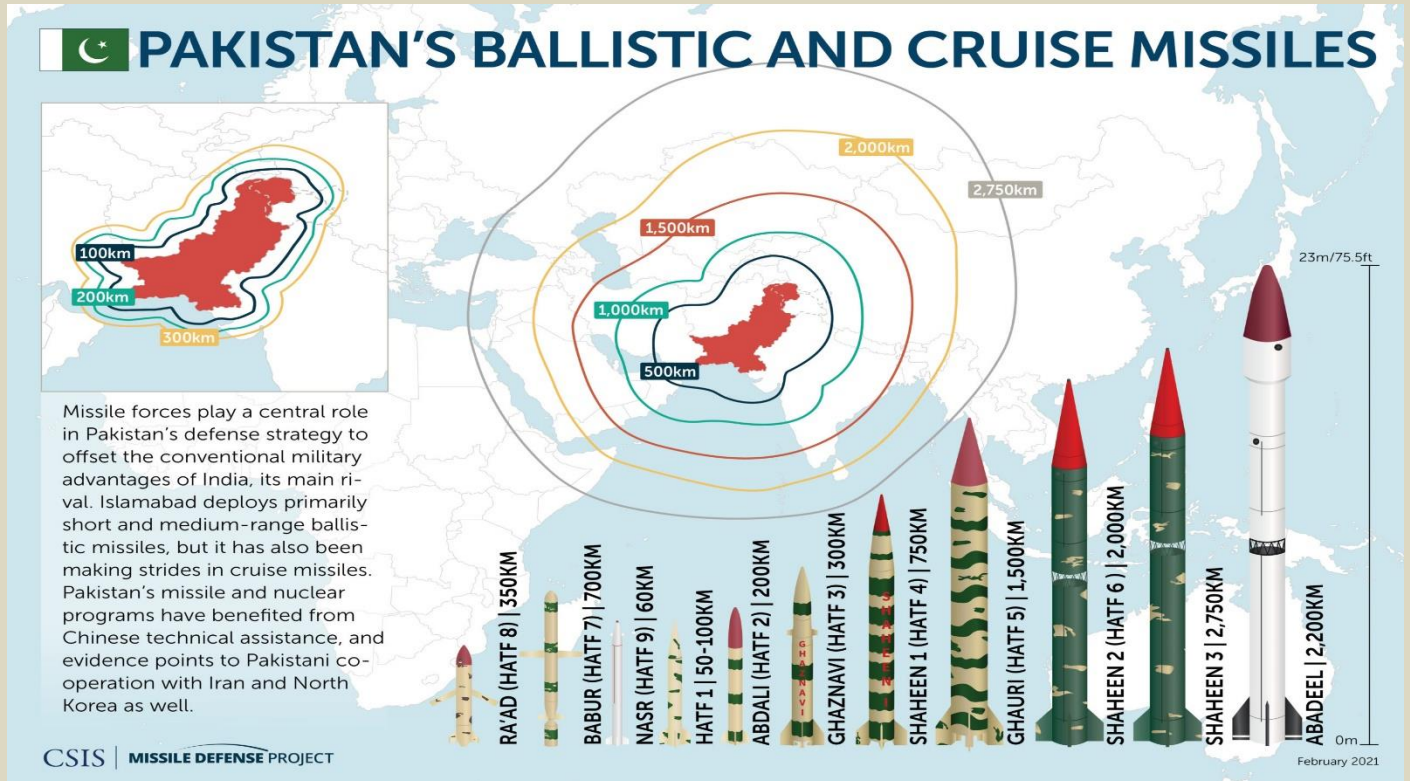
Shaheen 1A Test: Pakistan Maintaining Deterrence Stability In South Asia – OpEd

By Amber Afreen Abid

Source: <https://www.eurasiareview.com/15122021-shaheen-1a-test-pakistan-maintaining-deterrence-stability-in-south-asia-oped/>



Dec 15 – The flight test of Shaheen 1A has been conducted by Pakistan, recently on November 25, 2021. Shaheen 1A is a nuclear capable, surface-surface ballistic missile. It is a solid-fueled, road mobile launched ballistic missile, having the range of targeting at 900km, and has a weight of 10,000 kg. The ballistic missile was first tested in 2012, and can hit the target with great accuracy, as



the ballistic missile has the exceptionally developed guidance system; it thus, includes it amongst the utmost accurate ballistic missiles systems. According to ISPR, the flight test was conducted to revalidate the designs and practical considerations of the ballistic missile. The missile tests are performed to enhance Pakistan's credibility of nuclear missiles and to augment the nuclear posture of credible minimum deterrence. According to 2005 Bilateral Missile Pact between Pakistan and India, both countries notify each other before performing such tests.



The strategic policy making of the south Asian nuclear rivals accounts for several aspects, including the geographical factors, economic, military aspect, and relations with other states. The foreign policy of states on these factors and considering the long state rivalry with the neighboring country-India, Pakistan has to regularly update and modify its military capability, in order to counter for any aggressive action coming from India. For this purpose, Pakistan has designed its policy of credible minimum deterrence, which would be adequate to halt the enemy from going into adventurism.

The purpose of deterrence has always been to deter wars. Wherever, there is a nuclear dyad, the deterrence theory works. The purpose of that is to threaten and coerce the enemy to not to take any undesirable action, keeping in view the costs in response to that. In case of South Asia, the deterrence theory is visibly seen. But in order to maintain this deterrence, Pakistan has to keep up with the developments made by India, and respond efficiently to that, for maintain the balance, strategic stability and for the deterrence to work. Pakistan reserves the option of Nuclear First Use when it comes to the nuclear weapon state, however, considers nuclear weapon as a weapon of mass destruction. By maintaining the policy of credible minimum deterrence vis-a-vis India is entirely based upon security.

Indian military posture is aggressive in nature, which enhances the need for Pakistan armed forces to cater for their operational and military preparedness. Pakistan needs to augment its capabilities in view of the growing Indian technological and military capabilities. Pakistan, therefore, is pushed to adopt the strategic measures in line with the nuclear posture of credible minimum deterrence. The sole purpose of acquisition of nuclear weapons by Pakistan is security vis-à-vis India. Pakistan's nuclear use doctrine is clearly based upon the policy of Credible Minimum Deterrence posture. The 'minimum' and 'credible' in the nuclear posture are entirely dependent upon the advancements made by the rival state, and thus changes in accordance with its technological advancements and force postures.

Pakistan is playing field at par with the adversary. The posture of credible minimum deterrence serves as a stabilizing factor in South Asian strategic environment. It is to be certain of having dealt with up with the growing aggressive Indian strategies and force postures, and has thus wiped the chances of a total war in the region.

The nuclear deterrence of a state must depends upon three Cs-Credibility, Capability, and Communication. Hence, to maintain a credible deterrence, the capability of the nuclear forces should be communicated effectively, and the demonstration should be credible enough to restrain adversary from taking any aggressive action. The test of nuclear missiles are an effective way to showcasing the capabilities and a successful test enhances the credibility of the forces. The three Cs are always interdependent and thus creates a strong deterrence. This is the core of deterrence and is extremely important in rapidly advancing technological developments in south Asia.

The overt nuclear in south Asia has diminished the chances of a total war in south Asia has considerably been reduced. The unstable peace in the region, between two nuclear rivals remains vulnerable to animosity and competition. The unstable peace is there in south Asia, which depends highly on robustness of deterrence and strategic stability in the region. Pakistan has been compelled by the nonpareil conventional superiority of India and its aggressive military designs, to go for the option of aggressive defensive nuclear postures. Thus, by maintaining the nuclear and non-nuclear security measures, the deterrence and strategic stability in the region can prevail.

Amber Afreen Abid is a Research Associate, Strategic Vision Institute (SVI), Islamabad. She holds an M.Phil degree in Strategic Studies from National Defence University (NDU), Islamabad.

Tolerating a nuclear Iran?

By Shlomo Ben-Ami

Source: <https://www.aspistrategist.org.au/tolerating-a-nuclear-iran/>

Dec 17 – In 1977, Israel's deputy prime minister, Yigael Yadin, asked Egyptian President Anwar el-Sadat, who was on his historic trip to Jerusalem, why the Egyptian army had not proceeded to the Sinai passes during the 1973 Yom Kippur War. 'You have nuclear arms, haven't you heard,' was [Sadat's reply](#).

Of course, Israel's nuclear capabilities were the stuff of rumour. To this day, Israel has never officially confirmed the existence of a nuclear program. Yet Israel's [worst-kept secret](#) has long shaped the region's politics, including by deterring its enemies. But can it deter Iran?

In 1967, David Ben-Gurion, Israel's first prime minister, and Shimon Peres, who would later serve as both prime minister and president, argued for Israel to test a primitive nuclear device, in order to deter an Egyptian attack. At the time, Israel was virtually on its own in a hostile neighborhood. France—which had been its main arms supplier—had recently deserted it, and Israel had not yet achieved its current strategic intimacy with the United



States. Ben-Gurion's position reflected his view that Israel was an intrinsically fragile entity surrounded by mortal enemies with which war was inadvisable absent the backing of a major foreign power.

Prime Minister Levi Eshkol, Deputy Prime Minister Yigal Allon and Chief of Staff Yitzhak Rabin—all principled opponents of nuclearisation in the Middle East—[recognised](#) the country's precarious position but resisted the temptation to demonstrate a nuclear capability. When, during the dark days of the 1973 Yom Kippur War, Defence Minister Moshe Dayan [revived](#) the proposal, Israel's leaders again resisted the temptation to flaunt—let alone deploy—nuclear weapons.

Nearly half a century later, Israel has fewer enemies in the region, having made peace with several of its neighbours. But it has gained a powerful new one in Iran, since that country's 1979 Islamic revolution. And some are arguing that in order to deter Iran from pursuing its nuclear program, Israel should [abandon its policy](#) of 'nuclear opacity'.

But if Israel announces its capabilities and Iran persists in its nuclear drive anyway, would Israel really mount a nuclear response against what is clearly a strategic challenge but certainly not an existential threat? Moreover, Israel's acknowledgement of its nuclear arsenal might lend legitimacy to Iran's own quest for nuclear weapons and encourage other regional powers, such as Egypt, Saudi Arabia and Turkey, to follow suit.

The risks are apocalyptic. The kind of mutual deterrence that existed during the Cold War, or even today in the binary India–Pakistan conflict, would not work in the Middle East, a dysfunctional region where non-state actors and unstable regimes abound.

Iran has been dogged in its nuclear efforts. It has endured years of crippling economic sanctions, ultra-sophisticated Israeli cyber warfare against its strategic infrastructure, assassinations of its nuclear scientists, and attacks on its military targets across the Middle East.

Yet Iran is now closer than ever to mastering the full nuclear fuel cycle. It has also managed to maintain its proxy armies throughout the Middle East, and to extend its strategic influence from Yemen through Iraq and Syria to Lebanon.

Israel's 'Begin doctrine'—a counter-proliferation policy focused on using pre-emptive strikes to halt potential enemies' development of weapons of mass destruction—will not stop Iran. A decade ago, Israel [spent billions](#) of dollars on preparations for a massive strike on Iran's nuclear installations. But that strike never materialised.

Israeli air strikes did destroy Iraq's Osirak nuclear reactor in 1981 and a similar installation in Syria in 2007. But those were surgical operations. Using air strikes to destroy Iran's well-dispersed, well-camouflaged and well-protected nuclear installations is unrealistic, and the effort would almost certainly lead to a major war.

While Israel's military capabilities are unmatched by any other Middle Eastern power, it would still face serious threats. Iran would certainly respond to an attack on its nuclear installations by retaliating against Israeli targets, and perhaps against the countries that allowed Israel to use their airspace to reach Iran.

Meanwhile, Iran's Lebanese proxy, Hezbollah, would begin to deploy its 150,000 missiles and rockets, which can reach every corner of Israel. Israel's vulnerable home front, and possibly some of its vital infrastructure, would be hit hard before its air force neutralised Hezbollah—likely razing Lebanon in the process.

An international agreement is probably Israel's—and the world's—best hope for preventing Iran from becoming a nuclear power. But while that is precisely what negotiators are currently attempting to achieve in Vienna, Iran has taken a tough bargaining position.

That is not entirely unjustified. After all, it was the United States (with Israel's complicity) that withdrew unilaterally from the 2015 nuclear agreement in 2018, even though Iran had not violated its obligations. And Europe failed to keep its promise to help Iran bypass the sanctions the US subsequently reimposed. Furthermore, Iran's interlocutors in Vienna—the countries that are preaching against proliferation—are mostly nuclear powers themselves.

This perceived hypocrisy likely reinforces Iranian leaders' belief that the real danger lies in *not* developing nuclear weapons. If Ukraine had not surrendered its Soviet-era nuclear arsenal (then the world's third largest) in 1994, in exchange for American assurances that Russia would respect its sovereignty, it might still have Crimea, and it might not be watching with concern as Russian troops mass on its border. Likewise, a nuclear-armed Iraq would not have been attacked by the US and its allies in 2003. North Korea's nuclear capabilities have so far kept it immune from such an attack. With this in mind, Iran's leaders might be thinking like Pakistani Prime Minister Zulfikar Ali Bhutto was 50 years ago. Pakistanis, Bhutto [declared](#), would 'eat grass, even go hungry' if that is what it took to develop their own nuclear bomb. The talks in Vienna can still lead to an agreement. But, with Iran's leaders largely convinced that a nuclear weapon is their best protection, the only durable way to prevent Iran from mastering the enrichment cycle and, ultimately, building an operational nuclear weapon probably lies in regime change. This was the position of key intelligence authorities in Israel a generation ago, when Iran's nuclear program was still in its infancy. Given how resilient the Islamic Republic has proven to be, it seems that the world may well eventually have to tolerate an Iranian nuclear bomb, just as it has learned to live with the Indian and Pakistani arsenals.

Shlomo Ben-Ami, a former Israeli foreign minister, is vice president of the Toledo International Center for Peace. He is the author of [Scars of war, wounds of peace: the Israeli–Arab tragedy](#).

QUESTION

Pakistan is home to one of the largest concentrations of terrorist groups in the world including at least five identified and sanctioned by the U.N. Security Council. Lashkar-e-Taiba, Jaish-e-Mohammad, Harakat ul Mujahidin, Lashkar-i Jhangvi, and Jamaat-ul-Ahrar all operate in Pakistan in addition to the TTP (Tehrik-e-Taliban Pakistan – Pakistani Taliban) and ISIS-K.

So, why is everybody worrying only about the possibility of Iran acquiring nuclear weapons and not about Pakistan's nuclear arsenal that might fall in the wrong hands or the possibility/intention to transfer nuclear know-how to other countries (e.g., Turkey)? And do something about it!

Iran's Centrifuges: Models and Status

Source: <https://www.iranwatch.org/our-publications/weapon-program-background-report/irans-centrifuges-models-status>



Dec 16 – Iran possesses thousands of gas centrifuges that are the mainstay of its nuclear program. Gas centrifuges spin uranium hexafluoride gas (UF₆) to separate uranium isotopes suitable for nuclear fuel, a process known as uranium enrichment.^[1] The number and capacity of these machines determine Iran's "breakout" time: how long it would take Iran—if it decided to do so—to produce the fuel for a small nuclear arsenal. The machines are also key to Iran's ability to "sneakout" by producing nuclear weapon fuel at secret sites.

In recent years, Iran has developed and deployed centrifuge models that can enrich greater amounts of uranium with fewer machines relative to its original IR-1 design. Iran's increasing mastery of centrifuge design and manufacturing raises the risk of a "sneakout," and it reflects an acquisition of knowledge that cannot be reversed.

The table below sets out the capacity and primary materials of each of Iran's currently-deployed centrifuge models, as well as the number of each model known from publicly-available IAEA reports^[2] to be installed and/or producing enriched uranium at Iran's three declared enrichment sites: the Fuel Enrichment Plant (FEP) and Pilot Fuel Enrichment Plant (PFEP) at Natanz and the Fordow Fuel Enrichment Plant (FFEP) at Fordow.

In addition to the models listed in the table, Iran has developed several other centrifuge designs that are not currently installed at any of its declared sites, either because they are still under development or have so far proven unsuccessful in operation. These include the IR-2, IR-3, IR-6m, IR-6sm, IR-6smo, IR-8s, and IR-9s.




HZS C²BRNE DIARY – December 2021

This table is based on a November 2021 Iran Watch report, [Beyond the IR-1: Iran's Advanced Centrifuges and their Lasting Implications](#), which contains detailed analysis of each centrifuge model. The table will be updated periodically as the IAEA releases new information.

MODEL	CAPACITY (SWU/yr) ^[3]	ROTOR ASSEMBLY MATERIAL ^[4]	FIRST TESTED ^[5]	# INSTALLED	# IN PRODUCTION MODE ^[6]
IR-1	~0.8 ^[7]	Aluminum + maraging steel	Late 1990s	Total: 6302 <i>at FEP: ^[11] 5239</i> <i>at PFEP: 18</i> <i>at FFEP: 1045</i>	Total: 5794 <i>at FEP: ^[11] 4732</i> <i>at PFEP: 18</i> <i>at FFEP: 1044</i>
IR-2m	~4-5 ^[8]	Maraging steel + carbon fiber	2009	Total: 1079 <i>at FEP: 1044</i> <i>at PFEP: 35</i> <i>at FFEP: 0</i>	Total: 1077 <i>at FEP: 1044</i> <i>at PFEP: 33</i> <i>at FFEP: 0</i>
IR-4	~4-5 ^[8]	Carbon fiber	2009	Total: 522 <i>at FEP: 348</i> <i>at PFEP: 174</i> <i>at FFEP: 0</i>	Total: 521 <i>at FEP: 348</i> <i>at PFEP: 173</i> <i>at FFEP: 0</i>
IR-5	6-10 ^[9]	Carbon fiber ^[10]	2013	Total: 36 <i>at FEP: 0</i> <i>at PFEP: 36</i> <i>at FFEP: 0</i>	Total: 34 <i>at FEP: 0</i> <i>at PFEP: 34</i> <i>at FFEP: 0</i>
IR-6	6-10 ^[9]	Carbon fiber ^[10]	2013	Total: 398 <i>at FEP: 0</i> <i>at PFEP: 209</i> <i>at FFEP: 189</i>	Total: 208 <i>at FEP: 0</i> <i>at PFEP: 208</i> <i>at FFEP: 0</i>
IR-6s	3-6 ^[9]	Carbon fiber ^[10]	2013	Total: 41 <i>at FEP: 0</i> <i>at PFEP: 41</i> <i>at FFEP: 0</i>	Total: 39 <i>at FEP: 0</i> <i>at PFEP: 39</i> <i>at FFEP: 0</i>
IR-7	11-20 ^[9]	Carbon fiber ^[10]	2019	Total: 1 <i>at FEP: 0</i> <i>at PFEP: 1</i> <i>at FFEP: 0</i>	Total: 0 <i>at FEP: 0</i> <i>at PFEP: 0</i> <i>at FFEP: 0</i>
IR-8	16-24 ^[9]	Carbon fiber ^[10]	2017	Total: 1 <i>at FEP: 0</i> <i>at PFEP: 1</i> <i>at FFEP: 0</i>	Total: 0 <i>at FEP: 0</i> <i>at PFEP: 0</i> <i>at FFEP: 0</i>
IR-8B	10-15 ^[9]	Carbon fiber ^[10]	2019	Total: 1 <i>at FEP: 0</i> <i>at PFEP: 1</i> <i>at FFEP: 0</i>	Total: 0 <i>at FEP: 0</i> <i>at PFEP: 0</i> <i>at FFEP: 0</i>
IR-s	8-12 ^[9]	Carbon fiber ^[10]	2019	Total: 10 <i>at FEP: 0</i> <i>at PFEP: 10</i> <i>at FFEP: 0</i>	Total: 10 <i>at FEP: 0</i> <i>at PFEP: 10</i> <i>at FFEP: 0</i>

MODEL	CAPACITY (SWU/yr) ^[3]	ROTOR ASSEMBLY MATERIAL ^[4]	FIRST TESTED ^[5]	# INSTALLED	# IN PRODUCTION MODE ^[6]
IR-9	34-50 ^[9]	Carbon fiber ^[10]	2021	Total: 1 at FEP: 0 at PFEP: 1 at FFEP: 0	Total: 0 at FEP: 0 at PFEP: 0 at FFEP: 0

Footnotes:

[1] Natural uranium contains about 0.7 percent of the fissionable isotope U-235. Uranium is considered enriched when the concentration of U-235 is increased. Uranium enriched to 3-5 percent concentration of U-235 is suitable for nuclear reactors. Weapons-grade uranium is usually defined as 90 percent U-235.

[2] As of November 17, 2021.

[3] The capacity of a centrifuge is measured in "separative work units" (SWU) per year. SWU reflect the effort needed to separate the two uranium isotopes (U-235 and U-238) in the enrichment process. A centrifuge with a higher SWU per year can enrich greater quantities of uranium to higher levels in shorter periods of time than a less efficient centrifuge.

[4] The rotor of a centrifuge is what spins the uranium hexafluoride (UF₆) gas to separate uranium isotopes. Centrifuges use "bellows" between rotors to form a rotor assembly that allows for flexibility when spinning at higher speeds. The bellows and the rotors themselves must be made with strong, lightweight material. Carbon fiber is an ideal material for this purpose, but aluminum and specialty steels such as maraging steel can also be used.

[5] Fed with UF₆; excludes mechanical testing.

[6] Accumulating enriched uranium

[7] Calculated from output data contained in IAEA reports.

[8] Based on the capacity of the Pakistani P2 centrifuge, the base model for the IR-2m and IR-4.

[9] The low end of the range is based on estimates contained in "A Comprehensive Survey of Iran's Advanced Centrifuges" by David Albright, Sarah Burkhard, and Spencer Faragasso, published by The Institute for Science and International Security on December 2, 2021 and available at <https://isis-online.org/isis-reports/detail/a-comprehensive-survey-of-irans-advanced-centrifuges>; the high end of the range consists of nominal claims made by Iranian officials or Iranian media (possibly referring to kg UF₆ SWU/yr, which has a value 1.47 times higher than the more standard kg U SWU/yr).

[10] Due to technological progression, centrifuges developed after the IR-4 are assumed to have their rotor assembly made entirely from carbon fiber even when not explicitly confirmed as such.

[11] IR-1 numbers for FEP are estimates based on an average of 169 machines per cascade, obtained by dividing 6064, the total number of machines planned in the April 2021 Iranian declaration, as reported by the IAEA (see GOV/INF/2021/24), by the number of planned cascades (36). That average is multiplied by the number of cascades reported by the IAEA in November 2021 to be installed or in production mode (see GOV/2021/51).

The Nuclear Weapons Ban Treaty (TPNW): Wishful daydream or Historic milestone?

By Hellmut Lagos Koller

Source: <https://moderndiplomacy.eu/2021/12/16/the-nuclear-weapons-ban-treaty-tpnw-wishful-daydream-or-historic-milestone/>

Dec 18 – The Treaty on the Prohibition of Nuclear Weapons (TPNW), adopted in 2017, has entered into force on the 22nd of January of this year and the number of ratifying states continues to grow, with Mongolia being the latest to announce its accession. This positive trend is certainly welcomed with enthusiasm by the Civil Society campaigners and growing number of supporters of this treaty that represents a huge step forward for the global movement to draw attention to the catastrophic humanitarian consequences of any use of nuclear weapons. It would certainly be dishonest to ignore the fact that this new international legal instrument remains controversial, to say the least, for most of the members of the so-called nuclear deterrence community. As preparations are ongoing for the first Meeting of States Parties, scheduled to take place in Vienna on 22-24 March 2022, it is useful to address some of the main doubts and arguments against the treaty.

In this regard, the main criticism is that it makes no sense to support a treaty on nuclear weapons if those states that possess them have not joined nor any intention to join it.

In order to address this claim, it may be useful to recall that in the case of the Mine Ban and the Cluster Munition treaties, its main promoters and supporters were also states that did



not possess those weapons, and that those international instruments also received some harsh criticism for this reason. Despite of this, there is no doubt now that both of those treaties have become remarkable success stories, not only by achieving the goal of approaching universalization, but also by consolidating a general moral condemnation of those categories of weapons. Therefore, the argument that a treaty necessarily needs to be joined by the possessors of the weapons can easily be rebutted. Despite of the current position of the nuclear weapons states, each new ratification of the treaty is not meaningless: on the contrary, it provides the treaty more authority and contributes to the growing pressure on nuclear weapons states to adopt further steps towards nuclear disarmament.

Arguments in favor of the TPNW

The other major contribution of the TPNW is that it facilitates the process of delegitimization of nuclear weapons, necessary to finally amend the well-established foundations of nuclear deterrence doctrines. The humanitarian principles that are underlying the treaty are totally incompatible with those doctrines, and therefore are having an impact on them by highlighting the inherent immorality and illegitimacy of nuclear weapons.

Another argument for the case of ratification is that it provides states the opportunity to support the process of democratization of the global debate on nuclear weapons, as this new treaty has been the result of a very open discussion with active engagement of delegations from all geographic regions and, in particular, of representatives of Civil Society. This is not a minor aspect of this process, but a key element. Indeed, unlike in negotiations of previous international legal instruments, in this era of growing complexity and interlinkages, the main challenges faced by humankind are being addressed by a diverse group of citizens, from all walks of life and regions. Traditional diplomacy is certainly not enough, and in the case of the TPNW, the positive results would clearly not have been possible without the decisive boost provided by the International Campaign to Abolish Nuclear Weapons (ICAN), which was able to mobilize Civil Society and likeminded governments towards the goal of negotiating a nuclear weapons ban treaty.

While it would be naïve to expect the establishment of the nuclear weapons states to be convinced by the humanitarian narrative and in a foreseeable future to amend its defense and security policies base on nuclear deterrence, the TPNW and its focus on the security of the human being instead of the traditional notion of the security of the state, are already having an impact on the academic and public debates in those states.

The second argument used by its critics is that the TPNW weakens the Non-Proliferation Treaty (NPT). Actually, this is not only incorrect, the opposite is true. In fact, the TPNW can serve as an initiative to help implement article VI of the NPT, by which parties are committed to undertake to “*pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament*”. This is of vital importance as the treaty clearly attaches a key role to all parties, and not only to those states that possess nuclear weapons. This commitment has also been reflected in the Final Document of the 2010 NPT Review Conference, and the TPNW can be understood as a reflection of that obligation to contribute to nuclear disarmament by non-nuclear weapons states.

Another common point is that the nuclear weapons industry is too strong and well consolidated and that it would be naïve to pretend that this treaty could actually have an impact on investment decisions.

This pessimism has also been proven wrong. In fact, in 2021, more than one hundred financial institutions are reported to have decided to stop investing in companies related to nuclear weapons production. As a result, the nuclear weapons industry is experiencing a considerable reduction and the trend towards the exclusion of this sector from investment targets is growing steadily. This is not only the consequence from the legal obligations that emanate from the TPNW but a reflection of the devaluation of the public image associated to these industries. As this public image continues to deteriorate, it is likely that this trend will continue and that the moral condemnation of these weapons of mass destruction will be absorbed into the mainstream of society.

Another common misinterpretation is that the TPNW should be understood as an instrument that is only designed to be joined exclusively by non-nuclear weapons states.

In fact, even though the treaty was developed by non-nuclear weapons states, it has been drafted and negotiated with the goal of universal adherence, including, someday, those states that still include nuclear deterrence in their national security doctrines. In particular, the TPNW establishes a clear set of steps for nuclear weapons states in order to eliminate their arsenals of nuclear weapons. Specifically, within 60 days after the entry into force of the treaty for a state party that possesses nuclear weapons, that state must submit a plan for the complete elimination of its nuclear weapons to a competent international authority that has been specially designated by states parties. The treaty also includes a process to designate a competent international authority to verify the elimination of nuclear weapons by a state before acceding to the treaty, and a process for states parties that maintain nuclear weapons in their territories for the removal of these weapons and report this action to the United Nations Secretary General.

It is also noteworthy that this treaty obliges states parties to provide adequate assistance to victims affected by the use or by testing of nuclear weapons, and to take the necessary measures for environmental rehabilitation in areas contaminated under its control. This



dimension of the treaty constitutes an important contribution both to the protection of human rights of victims and to the now inescapable obligation to protect the environment, which are aspects that are not covered by the Comprehensive Nuclear Test Ban Treaty (CTBT). This certainly does not affect the value and vital role of this key instrument of the nuclear disarmament and non-proliferation regime but complements it by addressing the fundamental issue of environmental reparation.

TPNW facing challenges

The main challenge now is not only to achieve a wider universality of the TPNW, but to engage more stakeholders and create awareness on the urgency of bringing pressure on the nuclear weapons states to finally move toward nuclear disarmament. In this regard, Civil Society initiatives have been promoting engagement of members of grassroots, parliament, the media and city governments, particularly in nuclear weapons states, which has had impressive results, with hundreds of local governments expressing support for the treaty and generating discussion among the population. These initiatives serve the purpose of putting pressure on politicians and especially, to facilitate a discussion within democratic societies about the sustainability and risks involved in the possession and harboring of nuclear weapons.

Indeed, the TPNW has a long way to go and overcome many obstacles to achieve its objective, but in its first year of entry into force, it has already had an undeniable impact on the nuclear disarmament and non-proliferation debate, despite the expected skeptics and efforts to ignore its existence stemming from the still powerful nuclear deterrence establishment. Most of its technical experts, academics and government officials honestly believe that nuclear weapons have helped to guarantee peace and stability to the world and therefore should continue as the foundation of international security doctrines. These well-established ideas have been based on the questionable assumption that the deployment of these weapons have avoided war and can guarantee permanent peace for all nations. This has served as a sort of dogmatic idea for many decades, but recent research results have shown that the risks involved are significantly higher and that the humanitarian consequences would be catastrophic for every citizen of the planet. The humanitarian impact paradigm, which underlies the process that has inspired the TPNW, has provoked a tectonic shift in the nuclear disarmament and non-proliferation debate, which had been limited to the NPT review conferences with its often-frustrating results. Certainly, the persistence of the different approaches needs to be addressed in a more constructive discussion among the supporters of this treaty and the deterrence community.

Finally, the fact that the first meeting of states parties of the TPNW will take place in Vienna is very meaningful as Austria has been one of the leading nations in this process, particularly in drafting the Humanitarian Pledge to fill the legal gap for the prohibition of nuclear weapons, which has been a decisive step towards the treaty that has already fulfilled that commitment. Despite of all the difficulties and the persistence of significant resistance, the active and committed participation of diplomats and Civil Society representatives, under the leadership of Austria, allow to envisage that this first meeting will help to strengthen the treaty and move forward in the long and burdensome road to the final objective of achieving a world free of nuclear weapons.

Hellmut Lagos Koller is a senior career diplomat from Chile. He has been alternate Permanent Representative to the International Organizations in Vienna and in Geneva and has represented Chile in the negotiations of the Treaty for the Prohibition of Nuclear Weapons in 2017. He served at numerous multilateral and bilateral posts all over the globe.

Anti-5G necklaces found to be radioactive

Source: <https://www-bbc-com.cdn.ampproject.org/c/s/www.bbc.com/news/technology-59703523.amp>

Dec 17 – Necklaces and accessories claiming to "protect" people from 5G mobile networks have been found to be radioactive.

The Dutch authority for nuclear safety and radiation protection (ANVS) issued a warning about ten products it found gave off harmful ionising radiation.

It urged people not to use the products, which could cause harm with long-term wear.

There is no evidence that 5G networks are harmful to health.

Advertisement

The World Health Organization says 5G mobile networks are safe, and not fundamentally different from existing 3G and 4G signals.





Mobile networks use non-ionising radio waves that do not damage DNA. Despite this, there have been [attacks on transmitters](#) by people who believe they are harmful.



The products identified included an "Energy Armor" sleeping mask, bracelet and necklace. A bracelet for children, branded Magnetix Wellness, was also found to be emitting radiation. The bracelet for children was found to be radioactive "Don't wear it any more, put it away safely and wait for the return instructions," the ANVS said in a statement. "The sellers in the Netherlands known to the ANVS have been told that the sale is prohibited and must be stopped immediately, and that they must inform their customers about this." Conspiracy theories have fuelled a market

of "anti-5G" devices that are typically found to have no effect. In May 2020, the UK's [Trading Standards sought to halt sales](#) of a £339 USB stick that claimed to offer "protection" from 5G. So-called "anti-radiation stickers" have also been [sold on Amazon](#). The [ANVS has published a full list of the products](#) it identified as radioactive on its website.

Tepco seeks approval for sea release of tainted water from Fukushima nuclear plant

Source: <https://www.japantimes.co.jp/news/2021/12/21/national/tepco-fukushima-water-sea-release/>



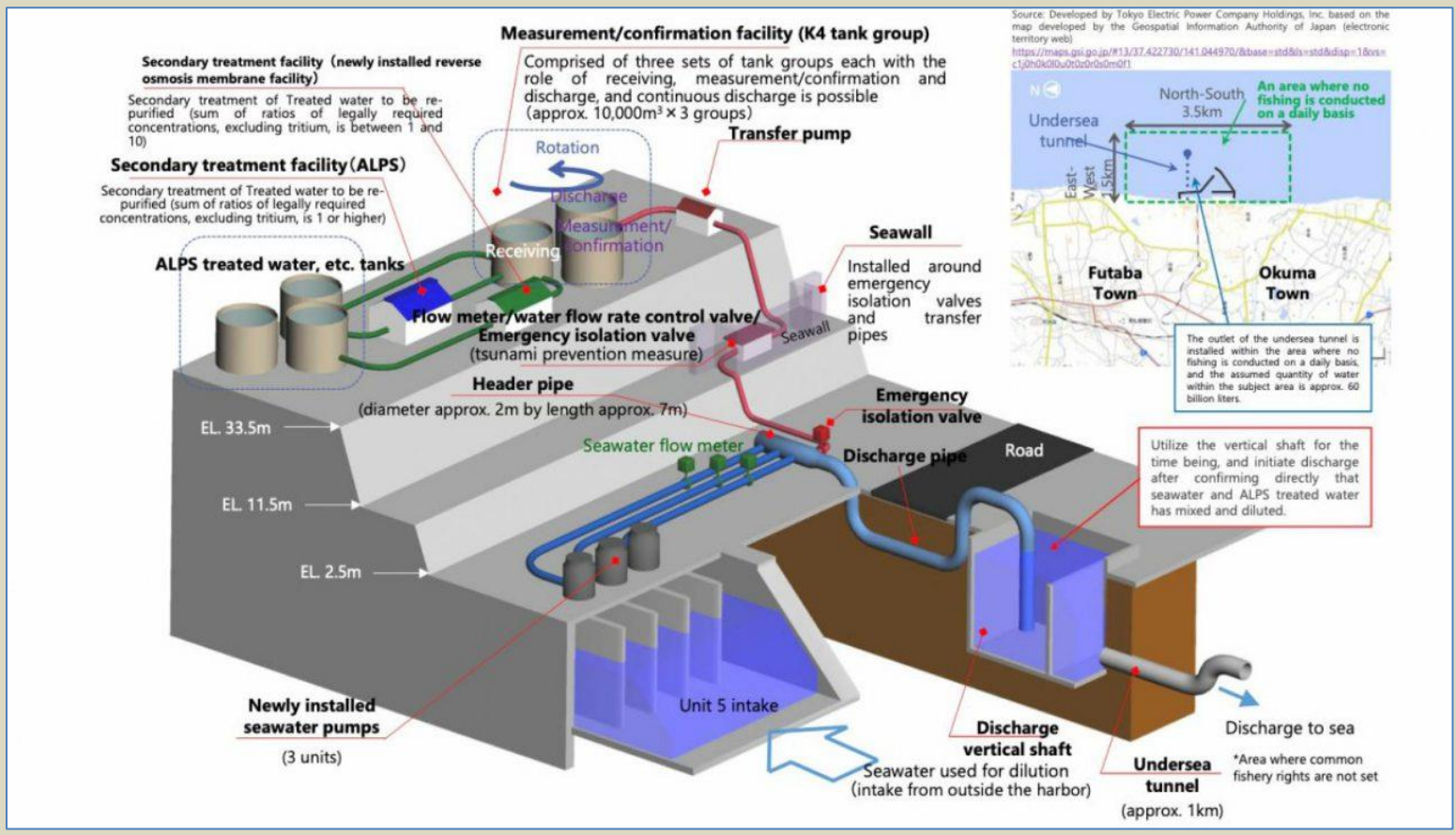
Tanks storing treated water occupy large areas around Tokyo Electric Power Company Holdings Inc.'s Fukushima No. 1 nuclear power plant. | KYODO

Dec 21 – Tokyo Electric Power Company Holdings Inc. (Tepco) filed Tuesday for regulatory approval of its plan to release treated radioactive water from its stricken Fukushima No. 1 nuclear power plant. The company will begin preparations in earnest if the Nuclear Regulation Authority approves the plan.





Tepco needs to obtain NRA approvals for designs and operational policies for equipment needed to dismantle the plant, where an unprecedented triple meltdown occurred after the March 2011 Great East Japan Earthquake and tsunami.



In August this year, Tepco announced a plan to release the treated water into the sea about 1 kilometer offshore from the Fukushima No. 1 plant, through a newly built undersea tunnel, after diluting it over 100 times with seawater.



The dilution is designed to lower the concentration of tritium in the water, which cannot be removed with available technology, to less than one-fortieth of the state-set safety standard. The exit of the tunnel will be created in an area where fishing is not conducted. Regarding the NRA's examination of the water release plan, Chairman Toyoshi Fuketa last week said, "We don't think there will be significant technical difficulties, so it will not take a long time."

The volume of water contaminated with radioactive substances at the plant is increasing as Tepco continues to cool nuclear fuel debris at the damaged reactors.

The water is processed before being stored in tanks, but the equipment used to treat it cannot remove tritium, a radioactive substance. In April, the government decided to release the water into the sea. But local parties, including fishers and local governments, are strongly opposed.

►► Read also: [Review of Risks from Tritium](#)

Alaska researcher creates method that can aid nuclear explosion detection

Source: <https://www.eurekaalert.org/news-releases/938721>

A University of Alaska Fairbanks researcher has devised a method to improve detection of distant explosions, including nuclear detonations, by taking advantage of widespread single-microphone infrasound monitors. Postdoctoral researcher Alex Witsil at the UAF Geophysical Institute's Wilson Alaska Technical Center has created a library of artificial explosion signals to train computers to detect real-world explosions. "What the work was meant to do was to detect large explosions, whether that's nuclear or chemical," Witsil said. "The methods we have worked out will allow monitoring agencies to detect explosions from distances of upward of a couple 100 kilometers." Using the library, real explosions can be detected amid background noise collected by single-channel microphones that record infrasound — sound carried at wave frequencies below what humans can hear. Today, detection algorithms generally rely on infrasound arrays that make use of multiple microphones close to each other. For example, the international Comprehensive Test Ban Treaty Organization, which monitors nuclear explosions, has infrasound microphones deployed worldwide. But they are of the multiple-microphone type. "That's expensive, it's hard to maintain, and a lot more things can break," Witsil said. Using single infrasound microphones increases detection capability because they're already in place for other uses. Their associated computers can be trained to recognize explosions by using artificial explosion signatures similar to the library Witsil created.

Why create artificial sounds of explosions rather than use real-world examples? Explosions sound different depending on how big they are, what produced them, and where they are recorded. Atmosphere, which varies by location, plays a key role in how a sound records. Because explosions haven't occurred at every location on the planet, there aren't enough real-world examples to train generalized machine-learning detection algorithms. "We decided to use synthetics because we can model several different types of atmospheres through which signals can propagate," Witsil said. "So even though we don't have access to any explosions that happened in North Carolina, for example, I can use my computer to model North Carolina explosions and build a machine-learning algorithm to detect explosion signals there." Witsil intends to continue the research to create an algorithm that can identify different types of explosions, including volcanic eruptions. His work is supported by the Nuclear Arms Control Technology Program at the U.S. Defense Threat Reduction Agency.

►► The abstract is [here](#).



ICI
International
CBRNE
INSTITUTE



HOTZONE
SOLUTIONS
GROUP



EXPLOSIVE NEWS

Jaw bombs, the deadliest threat to Sri Lanka's elephants, are scaling up

Source: <https://news.mongabay.com/2021/11/jaw-bombs-the-deadliest-threat-to-sri-lankas-elephants-are-scaling-up/>

Nov 19 — Elephant calves arriving at dusk to drink at the Weheragala reservoir tank in [Wasgamuwa National Park](#) can be particularly playful. But one day in September 2020, a lonely young elephant was spotted exhibiting uneasy behavior. After all the other members of its herd had gone back to the wilderness to retire for the night, this calf remained in the water. It appeared exhausted, and a closer inspection revealed why: its mouth had been severely mutilated, with saliva coming out of the swollen wounds. Unable to eat or drink, the calf died the next day.

This young elephant was yet another victim of “[jaw bombs](#)” — an improvised explosive device concealed in fodder bait that detonates when bitten. Its local name is *hakka patas*: jaw exploder.

Hakka patas are typically targeted at wild boars and other wildlife for bushmeat, which they kill instantly. Elephants are much bigger, so while the explosives don't kill them right away, they inflict gruesome mouth injuries and a long-drawn-out death from infection or starvation.

The first reported cases of Sri Lankan elephants (*Elephas maximus maximus*) killed by hakka patas came in [2008](#). A decade later, these explosives have become the number one killer of this endangered species. Sri Lanka has consistently recorded more than 200 elephant killings a year for the past three years, one of the highest rates per capita of any country with a wild elephant population.



Jaw bombs, or hakka patas, used by hunters and farmers mainly to catch crop-destroying wild boars, have now become the leading cause of elephant deaths in Sri Lanka. Image courtesy of the Department of Wildlife Conservation.

Easy-to-make explosives

The elephant calf at the Weheragala reservoir last year was the first reported case of a hakka patas being used in Wasgamuwa National Park, an ostensibly protected area. So the Sri Lanka Wildlife Conservation Society ([SLWCS](#)), an NGO that works closely with villagers to help minimize human-elephant conflict, sought to explore a little more this now-dominant threat to the country's elephants.

“We conducted covert investigations and found that some farmers have started to use this horrible method of killing animals since June and July of 2020” said [Ravi Corea](#), founder and president of the SLWCS.

Corea and his team tried to identify the perpetrators and raise awareness among villagers to discourage them from resorting to this inhumane method of dealing with elephants. But over the course of the next year, more elephants fell victim to the jaw bombs, showing an increase in the use of the explosive bait.



Hakka patas are easy to make. Gunpowder is mixed with gravel and metal scraps that serve as the shrapnel, and the mixture is tightly packed together. It's then balled up with fodder and left in areas frequented by animals.

"As the trade in wild boar meat has become a huge business in some of the villages around Wasgamuwa, it also has become the most common meat consumed by villagers" Corea told Mongabay.

Corea learned through SLWCS's local network that the explosive baits are manufactured by just a few people in the area, who sell them for around 1,500 rupees (\$7.50) apiece.

Pop pop crackers, the kind that explode when thrown against a hard surface, provide the ideal ingredient that make jaw exploders work, says SLWCS researcher [Chandima Fernando](#). In Sri Lanka, firecrackers are mainly used in April for the traditional Sinhala-

Hindu New Year celebrations take place, and villagers typically keep a few packets on hand throughout the year to shoo away crop-raiding elephants and other wildlife.

But the widespread availability of pop pop crackers now means it's easy for anyone in the community to make jaw bombs, Fernando said.

Out of a total of 323 elephant deaths in 2020, 54 were caused by jaw bombs, the main cause of elephant killings in Sri Lanka. Graph by Malaka Rodrigo.

The hunters

"Villagers know who the hunters in the area are and who sets the jaw bombs," says [Deepani Jayantha](#), a community worker from the Hambegamuwa community near [Udawalawe National Park](#), a known hotspot for poachers.

The community was struck by tragedy in 2016 when a [10-year-old boy was killed](#) when a hakka patas that he found while playing exploded.

The jaw bomb detonates when bitten. Elephants that survive the blast die a slow and painful death from either infected wounds or starvation because they can no longer eat or drink. Image courtesy of the Department of Wildlife Conservation.

The hotspot for hakka patas use against elephants appears to be Anuradhapura in Sri Lanka's [North Central province](#), along with parts of Eastern province. The Galgamuwa region in Anuradhapura is particularly famous for its dense elephant population.

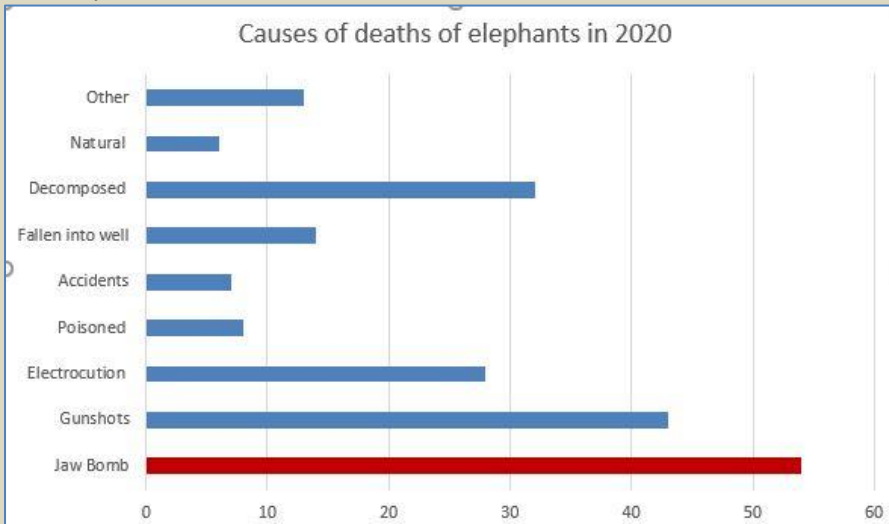
Susantha Punchi Banda, not his real name, is known within the community here for his ability to make potent jaw exploders.

"I've been hunting using this method for nearly 10 years" Banda told Mongabay. "I set up jaw bombs inside the forest patch at the edge of the village and collect the victims later. After making the explosives, we cover it with dried fish particles and this draws the wild boars. There are instances that other animals also bite on these explosives, including the occasional jackal."

Banda said he was not aware of any elephants taking his bait, "but I have seen a number of elephants suffering due to biting on jaw bombs set up by others, as our village is full of hunters like me."

He added, "I feel sorry for the elephants as they do not die instantly like other animals, but it is the fate of the beast."

Banda used to hunt wildlife with a gun, before a colleague taught him how to make hakka patas, a method he found much easier for hunting.



“It is dangerous and if the device gets unnecessarily crushed, it can prove disastrous,” Banda said, recalling an instance when one of his colleagues lost fingers while trying to make a jaw exploder.

“It is not hard to learn, but I do not teach others. Those who hunt know how to make it, but farmers come to buy jaw exploders from me to protect their crop,” he said.

Banda also said that some farmers deliberately target elephants with jaw bombs, often out of a vengeful response from extensive damage to their crops or home. The bait of choice when targeting elephants is a pumpkin, he added.

Source of explosives

Hakka patas only get attention when elephant deaths are reported, but plenty of other wildlife fall victim to these explosives, largely unnoticed, according to veterinary surgeons at the Department of Wildlife Conservation (DWC).

Due to the widespread use of hakka patas, some environmentalists say it's possible the jaw bombs are being manufactured for commercial purposes centrally and distributed throughout Sri Lanka through a covert network, though there's no evidence yet to substantiate this allegation.

What is known is that hakka patas are made by a handful of people at the local level and sold on order, which means the industry could be considered a commercial enterprise at the local level, Corea said.

If they were manufactured in factories and sold covertly through secret networks, then these factories would most likely be linked to fireworks manufacturers or people who work for them, given the need for a reliable supply of gunpowder.

For now, there's no evidence of any such practice.

But conservationists warn that with the COVID-19 pandemic bringing the fireworks industry to a grinding halt, it's possible that job losses in the industry might push some people to transfer their skills into producing jaw exploders. The risk is always there, they warn, which underscores the need for better surveillance.

Unexploded ordnance brings endless nightmare to Iraq

Source: <https://thearabweekly.com/unexploded-ordnance-bring-endless-nightmare-iraq>



A view of a 107mm warhead recovered by the Global Clearance Solutions (GCS) private demining company in an area near the village of Hassan-Jalad, north of Mosul, November 29, 2021. (AFP)

Dec 09 – In the northern Iraqi hamlet of Hassan-Jalad, almost every family has a story to tell about a time when a child, nephew or brother was lost to wartime munitions.

Located near Mosul, a former stronghold of the Islamic State (IS) jihadist group, the area is littered with unexploded ordnance, sometimes dubbed UXO.



“We are afraid for the children,” said one local man, Awad Qado. “We show them the routes to take, the places to avoid. We tell them not to pick up things they find on the ground.”

It was in 2017 that Qado’s family was struck by a landmine explosion in the hamlet of about 50 homes.

Two of Qado’s nephews were killed while tending to their herd. His son was injured and a fourth man’s legs were severed in the blast that also killed some livestock.

Across Iraq, about 100 children were killed or injured between January and September as a result of remnants of conflict, according to the UN.

In a country that has one of the world’s highest UXO “contamination rates,” almost one in four people is exposed to risk from unexploded ordnance, say non-governmental groups.

Iraq’s successive conflicts have left a deadly legacy, from the Iran-Iraq war of the 1980s to the US-led invasion of 2003 and the defeat of IS in late 2017.

In the area around Hassan-Jalad, more than 1,500 explosives were found within one year, said Alaa al-Din Moussa, head of operations for the private demining company GCS.

“In this region, every house has a story,” he added. “Many children are dead. Hundreds of animals have entered fields and triggered explosives.”

‘Contaminated urban zones’

Clearing the UXO is painstaking and dangerous work.

Ordnance awaiting disposal is left in a desert area behind a banner that reads “STOP.”

The explosives are classed in several categories including: 107-millimetre rockets, 23-millimetre projectiles and VS500 mines.

Both Mosul and the western province of Anbar are among the most affected areas, as are other former IS strongholds.

“We see a lot of contamination in built-up urban areas,” Pehr Lodhammar, programme chief of the UN Mine Action Service (UNMAS) in Iraq, said.

“Explosive hazards and explosive contamination are making it much more difficult for people to return to their homes and to resume a normal life.”

More than 1.2 million people have been displaced in the country as a result of the successive conflicts.

The fighting has left the borders with Iran, Kuwait and Saudi Arabia littered with landmines and unexploded remnants of war, according to a report by the France-based group Humanity & Inclusion.

“Iraq is one of the countries’ most heavily contaminated by explosive ordnance on earth,” the organisation said in a report in October.

“Explosive remnants of war affect more than 3,200 square kilometres of land, twice the area of London.

“A staggering 8.5 million Iraqis live amid these deadly waste-products of war.”

Helpless victims

A key challenge is raising awareness to allow people to change their behaviour in the face of danger. As a result of sessions held for children and adults, there have been “success stories”, said Ghaith Qassid Ali, who helps run GCS’s awareness programme in the Mosul area. As a result of the sessions, children playing in a field “saw a projectile, remembered the photos a team had shown them and warned us,” recounted Ali. He said the UXO phenomenon poses major economic challenges: “The majority of inhabitants of this village are farmers, but most of the land is contaminated by remnants of war.” At just 21 years old, Abdallah Fathi is living proof of the tragedy wrought by wartime munitions.

In 2014, he was tending to his herd when a mine exploded. He lost both his legs, his left hand and several fingers on his right hand. “Before, I used to work, but now I can do nothing, carry nothing, not even cement blocks,” he lamented. “I stay at home all day, I don’t go out.”

Importance of electromagnetic compliance for bomb suits and helmets

By Doug Wong, Jean-Philippe Dionne, Aris Makris, Alex Leask, and Trevor Yensen

Source: <https://counteriedreport.com/importance-of-electromagnetic-compliance-for-bomb-suits-and-helmets/>

Insurgents’ activities over the last two decades in Iraq and Afghanistan have shown an alarming trend towards command-initiated Radio Controlled Improvised Explosive Devices (RCIEDs). These devices are easy to make, inexpensive, and can be easily acquired in almost any country. With an estimated 70% of terror attacks globally involving remotely detonated IEDs, technological adaptations of equipment and operating procedures are required to ensure all-hazard protection to bomb technicians against the evolving threat of Radio-Frequency (RF) initiated IEDs.



The primary means of mitigating this threat to bomb technicians is through the use of high-energy Electronic Counter-Measures (ECM), often called “jammers”. ECM equipment can be mounted inside a vehicle or hand-carried (Figure 1) by the technician. It has the effect of jamming or blocking Radio-Frequency (RF) signals in a localized area to prevent terrorists from using a remote transmitter to activate the RCIED. This is accomplished by radiating various electromagnetic frequency patterns at high energy in the area near the jammer. The radiated power will disrupt RF signals in the jamming “bubble”, including lawful communication frequencies that may be used by the bomb technicians. In addition to the active effects of transmission blocking, the ECM equipment may induce unwanted electric signals in any electrical component carried by bomb technicians that has inadequate shielding. These spuriously induced signals can interfere with electronic operations and degrade performance in any unprotected electronic system such as communications systems and microcontrollers. Such unprotected electronic systems also risk permanent damage from high RF energy.

The level of RF interference in a jamming “bubble” may be higher than what US Federal Communications Commission (FCC) compliance testing would experience, so passing more stringent military standards tests is needed to minimize issues due to Electromagnetic Interference (EMI).



Figure 1: (left) Bomb technician hand-carrying an ECM device (RF jammer) while approaching a suspected device. (right) Bomb technician next to a vehicle equipped with mounted RF jammers.

Certain Explosive Ordnance Disposal (EOD) helmet designs available on the market today were not intentionally designed to provide sufficient RF shielding in order to permit full electronic functionality of the various on-board subsystems, e.g., speakers, ventilation, communications, under an active jammer environment. In particular, RF compliance was not included in the development of the NIJ 0117.01 standard for Public Safety Bomb Suit from the US National Institute of Justice, the only currently existing standard specific to EOD personal protective equipment. Moreover, irrespective of the use of ECM equipment, it is possible that the electronic functions (i.e. communication, ventilation, lighting, power) of the existing EOD helmets allow for short-range induction into other electrical components. This induction could potentially cause an inadvertent detonation of an IED that may contain an overly sensitive electrically-driven initiation system.

As such, it is necessary to reconfigure the conventional design of EOD helmets to permit them to be operational and safe in close proximity to IEDs and/or in conjunction with ECM equipment being deployed, from both a susceptibility and emissions perspective.

Design considerations

The first RF/ECM compatible EOD helmet was launched in 2007, developed through funding from the CBRN Research and Technology Initiative from Defence R&D Canada, the research branch of the Canadian Army. The improved design that resulted from this initiative allowed bomb technicians to work in harsh RF environments using state-of-the-art ECM equipment while maintaining the required and expected functionality currently used as a standard by most First Responders in North America, Europe, Middle East, Africa and Asia. This helmet also accommodated combined Chemical/Biological Blast protection to EOD technicians already available with conventional EOD helmets at the time.

Electromagnetic compatibility is an essential feature of any specification for military and law enforcement electrical equipment (not just EOD) and is defined as the ability of electrical and electronic equipment, subsystems and systems to share the electromagnetic spectrum and perform their desired functions without unacceptable degradation for or to the specified electromagnetic environment.

The EOD helmet (and interface) design changes necessary to ensure electromagnetic compatibility that permit close-up and safe operation in harsh RF environments included



redesign of problematic components and systems to address the RF shielding and emission challenges. The electronics systems had to be redesigned, the mechanical enclosure revamped and the entire system tested to ensure compatibility with RF/ECM standards (namely MIL-STD-461 and Def-Stan-59-411, discussed in the next section). All cabling and interfaces, including connectors, had to be redesigned and “hardened” to resist leakage (entry or emissions) of RF spectrum within the frequency range of interest, as defined by the particular standards adhered to for ECM design compatibility.

To meet the most stringent Electromagnetic Interference (EMI) and EMC tests, all systems and wiring designs must pay careful attention to high performance shielding, and maintaining shielding integrity, as well as rigorous filtering of all signals and power wiring. For instance, audio circuits, both microphone and speakers, are particularly susceptible to EMI ingress, causing a buzzing sound, especially from an ECM jammer.

Manufacturing methods are also important as RF hardening introduces a higher level of complexity in component selection and assembly methods, and consequently higher costs. For example, it is uncommon for small wearable connectors to be waterproof and still offer a full 360-degree braided shield connection capability. Likewise, it is problematic to make a high-quality EMI gasket on a small electronic enclosure that is also fully waterproof. The connectors on enclosures are also critical in allowing or preventing noise from crossing the enclosure wall. Even shielded connectors are insufficient in this regard and special techniques are needed to achieve high performance. Another example is designing good EMI filters on a printed circuit board (PCB), which requires special methods to ensure noise gets properly attenuated without bypassing the filters.

Standard electromagnetic tests

To ensure optimal functionality and safety in the view of RF threats, bomb suits and helmets, in a first step, should be tested against relevant electromagnetic military standards. Such standards establish limits for both radiated electromagnetic emissions and susceptibility to electromagnetic radiation with respect to electronic, electrical and electromechanical equipment and subsystems.



Figure 2: (left) EOD helmet tested for electromagnetic compliance (MIL-STD-461 and Def-Stan59-411) in an anechoic chamber (David Florida Laboratory, Canadian Space Agency, Ottawa, Ontario, Canada) (right) RF jammer (Allen-Vanguard) subjected to the same tests.

While there exist commercial electromagnetic compliance standards (e.g. FCC, EC), more stringent military standards are deemed more suitable in the context of EOD environments and the use of life-saving equipment such as bomb suits, often used in military settings. Two military standards are commonly used for this purpose: the MIL-STD-461 standard from the United States Department of Defense and the Def-Stan 59-411 from the UK.

The MIL-STD-461 standard document declares that “the stated interface requirements are considered necessary to provide reasonable confidence that a particular subsystem or equipment complying with these requirements will function within their designated design tolerances when operating in their intended electromagnetic environment (EME)”. This standard was first released in 1967, and multiple revisions have since been generated (Revision G dates back to 2015). The UK-based Def-Stan 59-411 Part 3 document “provides requirements for Ministry of Defence (MOD) Project Officers and Defence Contractors to assist them in the specification and selection of Electromagnetic Compatibility (EMC) Test Methods and Limits for Subsystems to limit the propagation and coupling of unintentional electromagnetic energy whether conducted or radiated.” The original version of that document was first released in 1999, and the latest revision dates back to 2008.

Both sets of tests are to be conducted in an anechoic chamber (Figure 2), with representative and fully functional test samples with associated accessories.

Two main types of tests are conducted for each standard: radiated emissions, and susceptibility, at frequencies up to 20 GHz.





RF jammer devices

RF jammers are engineered to ensure interoperability with various vehicle and manpack systems. The jammers include the ability to customize the waveform technique to minimize interference with friendly collocated systems as well to share reference oscillators, timing indicators, triggers and data communications to allow for constructive synchronization between systems that compete for electromagnetic spectrum resources.

Multiple jammers are often required to target the threat profile. In particular, the ability to collocate multiple jammers in close proximity is a prime consideration in EOD carry forward scenarios (Figure 3). The potential for self-interference between the jamming units themselves, through radiated susceptibility, must be addressed similar to the interoperability scenario between the jammer and EOD helmet. The close proximity of RF jammers necessitates the need for proper RF shielding, validated through MIL-STD-461 radiated susceptibility testing. *Without a suitably RF hardened enclosure, jammers may interfere with each other.*



Figure 3: RF jammers in close proximity (SCORPION, Allen-Vanguard) on a “Dual Carrier” to maximize the jamming response for enhanced operator safety.

Currently, to comply with the MIL-STD-461 Radiated Standard requires a field strength of 50 Volts/meter with no impact to the device. As an added safety measure, the most advanced jammers are routinely qualified to 200 Volts/meter field strength in the majority of the frequency bands to ensure that the probability of adverse effects are significantly further reduced.

MIL-STD-461 standards, in particular the RS103, are just one in a suite of MIL-STD tests that jammer manufacturers utilize to ensure product robustness in harsh operating environments. Other applicable standards include MIL-STD-810, featuring operational hot &





cold, storage hot & cold, humidity, thermal shock, shock and vibration as well a commercial IEC/EN 60529 for IP ratings water and dust ingress rating.

Representative tests against an actual jammer device

While compliance to the requirements of the above standards ensures that EOD Personal Protective Equipment (PPE) is well shielded against RF/ECM threats, it offers no guarantee that an EOD helmet's full functionality would be preserved when exposed to a specific jammer since jammer specifications are secret. However, compliance to the MIL-STD-461 and Def-Stan 59-411 truly minimizes the chances of interferences between EOD PPE and jammers.



Figure 4: Volunteers testing the functionality of different Med-Eng legacy EOD helmets at varying distances from an ECM device.

This being said, compliance of EOD equipment with a specific jammer device can be verified through functionality tests representing actual threat environments to ensure that bomb technicians have the required electronic functionality to accomplish their mission safely. For instance, through the development of the first RF shielded EOD helmet, volunteers tested four different legacy EOD helmets (Figure 4), among which only one was designed towards RF/ECM compliance.



Figure 5: Test setup for the EOD helmet tests against actual jammers. Pylons positioned at 10-meter intervals from two SCORPION ECM devices (Allen-Vanguard jammers).

the test site and the radios and hard-wired system were situated 100 meters away. Pylons were set up at 10-meter intervals from the ECM devices until a distance of 50 meters from the ECM device was reached (Figure 5).

A representative radio communication system and a wired system were both tested in combination with the helmets. Two ECM jammer devices were situated at one end of



The ECM devices were then activated. Each volunteer was asked to operate their helmets' different functions (searchlights, ventilation fans, communications) to determine whether the helmet was being affected by the ECM device and, if so, in which way (i.e. buzzing noise, searchlights would not turn on, etc.). Once each helmet had been tested for its functionality, the volunteers then walked towards the ECM device stopping at each 10-meter interval to repeat the functionality test. If the helmet was determined to be too painful to wear, or its functions were no longer operating, it was removed from the trial. The trial was then repeated for each ECM frequency band.

The results highlighted the benefits associated with RF shielding of the helmet, since all helmets, except the shielded one, introduced loud interference noises when exposed to the jammer, which in some cases became unbearable to the operator. In addition, some helmet functions were negatively affected (e.g., fans and communications) for all helmets, except the intentionally shielded helmet design version. Additional tests were then conducted with the operators hand-carrying the ECM devices. Even in this harsh scenario, only faint sounds were noticed for the shielded helmet, while none of the non-shielded helmets were found to be operable.

These tests thus confirmed the appropriateness of designing EOD helmets, connections, and accessories around the requirements of military electromagnetic compliance standards, to ensure full helmet functionality in the presence of a particular functioning jammer device. While the tests described above involved only one single jammer type, it is suspected that the shielded helmet's performance would remain satisfactory in the presence of other jammers, given its shielding level, so long as frequencies and power emitted were in an acceptable range consistent with the standards.

CONCLUSION / DISCUSSION

As bomb technicians are increasingly exposed to the threat of Radio-Controlled Improvised Explosive Devices, the deployment of advanced Electronic Counter Measure tools has become critical to minimizing the chances of explosive devices being triggered during render-safe missions.

As such, intentional design for shielding the electronic systems of the bomb technician, including their PPE and accessories, against electromagnetic threats is essential to ensure that operator safety and operational functionality of the equipment are not compromised. The tests highlighted above clearly demonstrated the difference between "hardened" systems and ordinary commercial electronics on bomb suit ensembles.

While there is no guarantee that a bomb suit ensemble designed to specific standards, such as MIL-STD-461 and Def-Stan 59-411, will remain fully operational in the presence of all current and future ECM jammer tools, meeting these stringent military requirements provides some safeguarding that a protective system will be functional and safe within an ECM and RCIED environment. To ensure full equipment compatibility, further validation trials should be conducted with the actual jammer ECM equipment of interest and specific PPE worn by the bomb technician, alongside any electronic accessories.

Irrespective of such further validation trials, meeting stringent military requirements for electromagnetic compliance (as opposed to less stringent commercial variants such as FCC and CE) represents a significant enhancement in capability against the most prevalent IED threat being faced by deployed militaries against the most prominent terrorist organizations. The use of electronic equipment that is not suitably shielded and validated in an RCIED render safe mission and/or within the range of ECM radiation may place the bomb technician at undue risk through the possibility of accidental detonation or malfunction of the equipment being used.

Alex Leask holds an Industrial C.E.T for Robotics, Automated Controls, RAB Certified Lead Quality Auditor with over 25 years expertise in compliance testing to Mil-461,810, 1275 as well as UL, CSA, EN, CE, FCC, STANAG, Def-Std., for complex high frequency RF systems, mechanical systems & safety equipment. He is currently the Engineering System Verification and Test Manager at Allen Vanguard.

Dr. Trevor Yensen holds a Ph.D. and M.Eng. in Electrical Engineering. His 17 years of work with Allen-Vanguard, most recently as its Chief Scientist, has established a world-class electronic warfare (EW) program with a focus on jamming systems for radio controlled improvised explosive devices (RCIEDs).

Dr. Aris Makris holds Masters and Ph.D. degrees in Mechanical Engineering, specializing in explosions and protection against blast effects, with over 30 years of related experience. He is VP of Research, Development & Engineering and Chief Technology Officer at Med-Eng, and has led numerous programs to design and develop personal protective systems to protect against IEDs, landmines, and explosive threats.

Dr. Jean-Philippe Dionne holds a Ph.D. in Mechanical Engineering and has over 20 years expertise in the fields of numerical simulations of detonations, blast waves and combustion. As the Director of Engineering at Med-Eng, he has directed numerous blast test programs and significantly contributed to the National Institute of Justice NIJ 0117.01 standard for Public Safety Bomb Suits.

Douglas Wong holds a B. Eng. and has over 30 years of experience in mobile data acquisition systems, robotics, spectrometer development, and optics. As the Med-Eng Director of Electronics Engineering, he holds EOD-related expertise in advanced sensors and signal conditioning methods used to monitor and measure blast events and their effects.





VBIEDs – Screening vehicles with portable X-ray scanners

By Tony Kingham

Source: <https://counteriedreport.com/vbieds-screening-vehicles-with-portable-x-ray-scanners/>

The recent anniversary of 9/11 has raised bitter memories of that terrible day back in 2001, and of course the chain of events that followed; the war on terror, the war in Afghanistan, the war in Iraq and of course the emergence of ISIS.

We have all learnt to live with terrorism and the effects it has had, particularly on travel and the use of public spaces. The spectre of a 'spectacular', as terrorist groups like to call attacks like 9/11, the Madrid train bombing, the Paris and Mumbai shooting attacks and dozens more besides, have gripped the public imagination, especially around air travel. Probably because that is where most of us are directly affected by the resulting additional security measures.

We also have seen the rise of the "lone wolf" attacker, using readily available items to inflict death and misery such as hire cars, knives and even swords, as we sadly witnessed in incidents in Barcelona, Nice and Westminster, and many more.

But the bomb remains the weapon of choice for the terrorist and in particular the Vehicle Borne Improvised Explosive Device or VBIED.

According to Wiki since 9/11 there have been 211 incidents of mass casualty car and truck bombings causing over 11,900 deaths and tens of thousands more maimings and injuries. Of those only 52 were suicide bombs (the vast majority of those in Afghanistan, the Middle East and Africa) and 159 were vehicles left in the target area, to be detonated by timer or remotely.

So, why is the VBIED the weapon of choice?

Well, the answer is simple; it is the most low-tech, low risk and mobile way to deliver a large quantity of explosives to an intended target.

Using a truck or car means the terrorist can use large amounts of readily and cheaply available materials such as ammonium nitrate fertilizer. Combined with fuel and other legal substances this will make a very big bomb, without the risk of attracting the attention of the authorities by having to obtain the equivalent amounts of controlled substances like commercial explosives.

Of course, they will need some high-grade explosives to detonate the bulk of the material but, the amount required is relatively small and therefore, so too is the risk associated with acquiring it, either locally or through smuggling operations.

Once the bomb is ready, it can be driven directly to the target, at a time and place of the terrorist's choosing, without raising suspicion.



It can be detonated either as part of a mobile suicide attack, using a trigger switch or impact trigger, or left covertly at the target and triggered by timer or remotely.

US Marines searching for victims in Beirut eight days after an attack that killed 241 American service members on October 23, 1983. (Source: CNN)

So, what you have is a weapon that is crude, cheap, unsophisticated, stealthy, highly mobile but devastatingly effective!

It should be remembered that terrorists killed more US servicemen and civilians with a truck bomb, driven into their barracks in Beirut in

1983, than they did with the American Airlines Flight 77 that crashed into the Pentagon on September 11, 2001.

So how do you protect public spaces and events against VBIED attacks?

Well, the obvious answer is to prevent movement of vehicles in the immediate vicinity of the venue or event. But maintaining the balance between people's freedom to enjoy normal activities and security considerations, means that simply pushing back the vehicle perimeter is not always practical or desirable in a free society.

So, restricting, slowing, and controlling vehicles in and around event venues are some of the primary ways in which we can protect ourselves against the VBIED.

The trick is to increase our defences without turning our venues and public spaces into fortresses, which, if we did, hands a partial victory to the terrorist.



Discrete, unobtrusive security is the desired effect and there are now numerous products available to help mitigate the threat whilst maintaining a steady movement of traffic.

Pop-up steel barriers have been around for some time and are a tried and tested technology that works for gates and roadways. The



safe, desirable, default position for these barriers would be in the up position, only lowering the barrier once a driver and vehicle have been checked, but clearly this is not practical for most public venues and spaces. For most high threat venues and events, they become the back stop in a layered security approach, including measures like CCTV in combination with Automated Number Plate Recognition (ANPR) facial recognition and traffic slowing measures like speed bumps and chicanes. This gives security staff the opportunity to screen vehicles and drivers before physical checks at vehicle check points.

However, inspecting selected vehicles cannot be avoided and this is where portable x-ray scanning systems are an invaluable tool. Large scale non-intrusive vehicle scanners are simply too expensive to be appropriate for most events. So, portable scanners allow security staff to thoroughly inspect vehicles safely and quickly.

ThreatScan® – portable x-ray system.

Portable x-ray Scanners like the 3DX-RAY ThreatScan offer incredible portability, flexibility, and military grade capability, in a roadside situation.

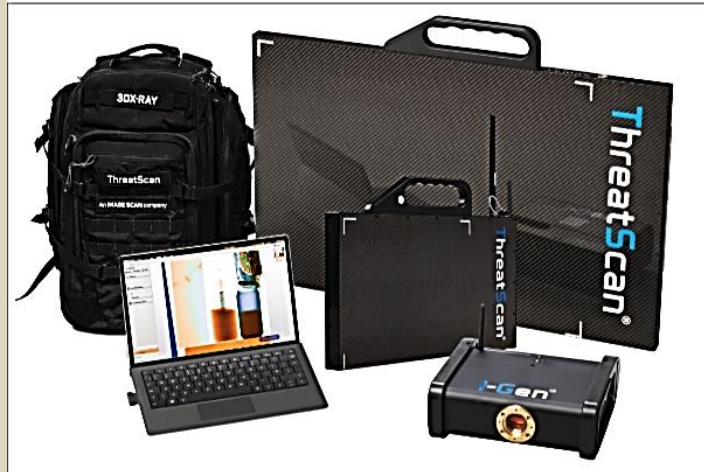
The system can be packed into the boot of a regular vehicle and deployed at any venue, whether it is a city stadium or an outside concert or festival, with no logistical infrastructure required.

However, inspecting selected vehicles cannot be avoided and this is where portable x-ray scanning systems are an invaluable tool. Large scale non-intrusive vehicle scanners are simply too expensive to be appropriate for most events. So, portable scanners allow security staff to thoroughly inspect vehicles safely and quickly.

Portable x-ray Scanners like the 3DX-RAY ThreatScan offer incredible portability, flexibility, and military grade capability, in a roadside situation.

The system can be packed into the boot of a regular vehicle and deployed at any venue, whether it is a city stadium or an outside concert or festival, with no logistical infrastructure required.

ThreatScan with its I-Gen x-ray generator is small and light



enough to place anywhere on a vehicle, and with its specially designed stand can be positioned at any angle for best scanning results.

The large 600mm x 460mm imaging area means that more of the vehicle can be scanned in a single scan. Which means it is now possible to scan top-down as well as through doors, wheels, and tyres.

The ThreatScan also produces colour differentiated scans, (the same technology that we see in airport security scanning systems), which makes it possible to determine the nature of the materials being scanned. For example, orange shows organics, such as explosives, chemicals, and drugs, as well as more innocent items such as foodstuffs. Blue is for metals, such as guns, knives, hand grenades, metal pipe bombs as well as IED components such as the power sources, switches, circuit components and metallic fragmentation. Green is for inorganic materials like black powders and aluminumized homemade explosives and Grey scale is used for recognition of shapes and the form of objects.

Another key factor when selecting a portable ray system is the image quality. What determines the overall image quality is a combination of both the detector panel and the x-



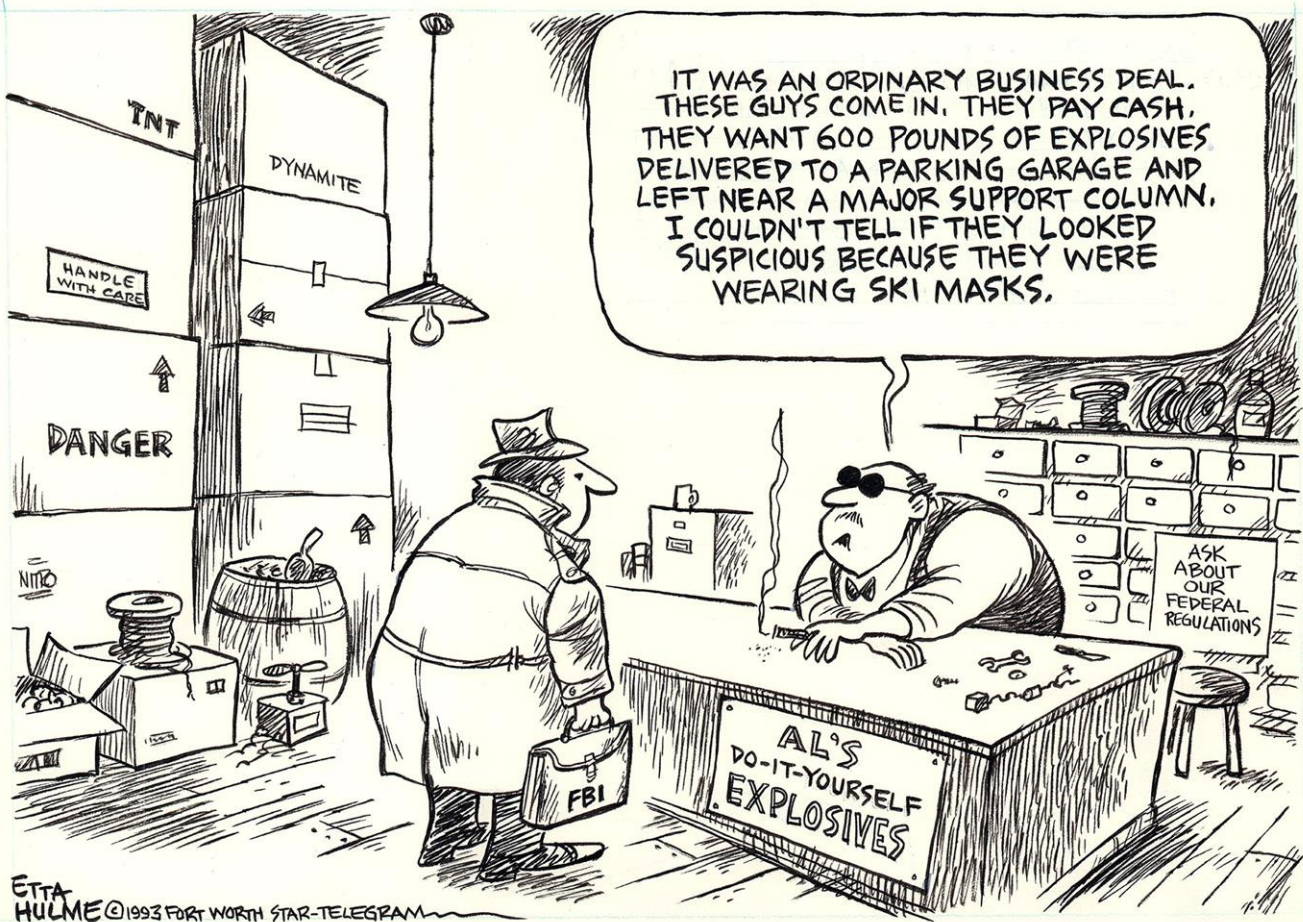
ray generator. Most systems on the market do not use a constant x-ray generator. With these systems the image quality plummets as you move away from the panel significantly. But the ThreatScan I-Gen system uses a constant potential generator, with this generator it actually improves. So, it is important to select a portable x-ray system with a constant potential generator. What is clear is that the threat from VBIEDs is not going to go away anytime soon, and the only way to safeguard the safety and security of our citizens is to ensure that we remain vigilant, have the right procedures and protocols and the right tools to do the job!

Tony Kingham is a journalist and PR consultant specializing in defense and security issues for more than 25 years.

Is RPG-7 still effective?

Read also the related questions column (right)

3 copies of 4613 and 2 copies of 58



THURS MARCH 4, 93



ICI
International
CBRNE
INSTITUTE



HOTZONE
SOLUTIONS
GROUP

CYBER NEWS



After a Year of Silence, Are EU Cyber Sanctions Dead?

By Stephan Soesanto

Source: <https://www.lawfareblog.com/after-year-silence-are-eu-cyber-sanctions-dead>

Oct 26 – One year ago, on Oct. 22, 2020, the Council of the European Union imposed its second, and so far last, EU [cyber sanctions package](#) in response to malicious cyber activities that constitute an external threat to the European Union or its member states. Though these sanctions were [envisioned](#) as a new tool to impose significant costs and bring about a change in policy or behavior from the sanctioned governments and individuals in cyberspace, they have [failed](#) in both substance and volume to achieve their strategic aims.

To date, only eight individuals and four organizations have been sanctioned by the European Union for various campaigns, including WannaCry, NotPetya, and the 2015 Bundestag hack. By comparison, since April 2015, the U.S. Treasury Department has [imposed cyber-related sanctions](#) on a combined 99 individuals and 59 entities, including 13 individuals and 19 entities in [2021 alone](#).

The limited EU response is not for lack of high-profile malicious cyber campaigns uncovered and attributed to foreign government agencies, groups and individuals that targeted EU member states. Instead, the imposition of EU cyber sanctions has been hampered by a lack of coordinated intelligence collection efforts, a focus on voluntary intelligence sharing, and a political process that likely undermines the creation of a common EU threat perception in cyberspace.

A Year of Adversarial Campaigns

Adversarial campaigns by a wide array of foreign state actors targeting EU member states have continued since the last round of sanctions were announced a year ago. On Feb. 17, 2021, the U.S. Department of Justice unsealed a federal indictment against three North Korean military hackers. Jon Chang Hyok, Kim Il and Park Jin Hyok were [charged](#) with “participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks [and] to steal and extort more than \$1.3 billion of money and cryptocurrency from financial institutions and companies.” Among the handful of victims named in the [indictment](#): the Polish Financial Supervision Authority, a Maltese bank and a Slovenian cryptocurrency company.

In March, the Finnish Central Criminal Police (KRP) and the Finnish Security Intelligence Service (SUPO) [attributed the breach](#) of the Finnish Parliament’s internal information technology system in the fall of 2020 to a Chinese threat actor known as APT31. In an effort to call out APT31’s activity in several member states, the EU high representative for foreign and security policy, Josep Borrell, published a [declaration](#) on July 19, which stated that these activities “have been conducted from the territory of China for the purpose of intellectual property theft and espionage.” Two days later, the French cybersecurity agency, ANSSI, [warned](#) that they are “currently handling a large intrusion campaign impacting numerous French entities. Attacks are still ongoing and are led by an intrusion set publicly referred to as APT31.”

In mid-April, Swedish public prosecutor Mats Ljungqvist [announced](#) that “Russian military intelligence, [the] GRU who, via its 85th Center, also known as unit 26165, has planned and carried out the serious breaches of data secrecy against the Swedish Sports Confederation” from December 2017 through May 2018. However, despite the Swedish attribution assessment, Ljungqvist [explained](#) that his office “reached the conclusion that the necessary preconditions for taking legal proceedings abroad or extradition to Sweden are lacking. I have, therefore, today decided to discontinue the investigation.”

The list goes on. The EU Computer Emergency Response Team [noted](#) in April 2021 that at least six EU institutions, bodies and agencies were affected by the supply chain attack against SolarWinds’s Orion platform. The Belgian Ministry of the Interior [stumbled](#) on a previously unknown espionage campaign while securing their systems against Hafnium’s indiscriminate exploitation of vulnerabilities in Microsoft Exchange Server. And the Dutch newspaper de Volkskrant [reported](#) that a Russian intelligence service infiltrated the network of the Dutch police back in 2017, when they were the lead investigator into the Malaysia Airlines flight MH17 incident.

Impediments to EU Cyber Sanctions

Given that there are marked differences between the intelligence type and volume necessary to confidently connect a campaign to a specific individual operator, a government agency or an intrusion set like APT31, it is unsurprising that these cases have broken down or are stuck at different stages in the investigatory process. In the North Korean case, the affected EU countries were likely unable to connect the dots across several national jurisdictions and might have deemed the individual incidents not severe enough to push them up to the EU level. The APT31 case seems to miss crucial intelligence that clearly links APT31 to a Chinese government agency or specific individuals—meaning that either intelligence has not yet been collected by an EU member state or it has been collected but the member state is unwilling to share it with the union’s other 26 governments for operational reasons. Meanwhile, the Swedish case likely ran into the problem that the GRU’s

85th Center and the operators responsible were probably [already sanctioned](#) by the European Union in June and October 2020. Time will tell whether these investigatory hurdles and intelligence blind spots will persist.

The GRU Ghostwriter campaign against Poland and Germany could break the EU's cyber sanction abstinence. On Sept. 24, just two days prior to the German federal election, the EU high representative published a [declaration](#) stating that Ghostwriter's "malicious cyber activities are targeting numerous members of Parliaments, government officials, politicians, and members of the press and civil society in the EU by accessing computer systems and personal accounts and stealing data." The declaration ends with the promise that "the European Union will revert to this issue in upcoming meetings and consider taking further steps." This is suggestive of a potential discussion of EU cyber sanctions, but whether or not they are imposed will depend on whether the EU member states have the intelligence at hand to identify and sanction specific Ghostwriter operators. Another course of action could be to sanction the GRU yet again, hoping that this will somehow create a different outcome. That being said, as of this writing, no EU institutions have picked up discussions on the Ghostwriter issue.

The EU's nonuse of cyber sanctions over the past year, and the challenges of responding to the Ghostwriter campaign in particular, are indicative of a flawed process. First, the intelligence services of the European Union's 27 member states are not streamlined to selectively gather relevant foreign intelligence to underpin the EU cyber sanction process. As a result, classified intelligence sharing on adversarial campaigns occurs only by accident or when one intelligence agency proactively reaches out to others to figure out whether they have relevant information that they are willing to share. Second, intelligence sharing on the EU level is by design voluntary as information has to be declassified to be shareable with the other 26 members. Some member states are likely to outright refuse to engage in this process for operational reasons, while others have run into the problem that the intelligence shared is not compelling enough. Third, the decision to impose cyber sanctions is a political process that likely undermines the creation of a common cyber threat perception within the EU. When the Polish government [raised](#) the issue of Ghostwriter on the EU level back in June, the bloc refused to take any subsequent action. But when the German government brought up the same issue three months later, the EU's high representative released a declaration on Ghostwriter within just nine days. And fourth, at the end of this complicated process, it is unclear whether EU cyber sanctions impose any costs on the sanctioned individuals or entities. In fact, the more EU cyber sanctions are imposed on the same threat actor—such as the GRU—the weaker the EU's argument becomes that sanctions can bring about a change in policy or behavior from the sanctioned individuals and entities.

There are many smart people working in the EU institutions and agencies on cyber policy, and a serious response to the Ghostwriter campaign would be a vindication of their work. But this seems unlikely. The status quo for the EU cyber sanctions regime will probably persist, because admitting failure is hard and major policy overhauls never come easy.

Stefan Soesanto is a senior researcher in the Cyberdefense Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich. Prior to joining CSS, he was the Cybersecurity & Defense Fellow at the European Council on Foreign Relations (ECFR) and a non-resident James A. Kelly Fellow at Pacific Forum CSIS.

Turkish Army Uses Algorithm to 'Persecute' Gulenists: Report

Source: <https://balkaninsight.com/2021/11/25/turkish-army-uses-algorithm-to-persecute-gulenists-report/>

Nov 25 – A new report published by StateWatch, a UK-based international rights organisation monitoring the state and civil liberties in Europe, says an algorithm used to detect alleged government opponents in the Turkish Armed Forces, TSK, has been used to persecute thousands of people.

The report, "[Algorithmic persecution in Turkey's post-coup crackdown: The FETO-Meter system](#)" says more than 20,000 military personnel have been dismissed since a failed coup attempt in 2016 on the basis of algorithms.

"The report shines a flashlight on the (mis)use of algorithms and other information-based systems by the Turkish government in its ruthless counterterrorism crackdown since the July 2016 events. Thousands of people have been put out of work, detained, and persecuted by reference to 'scores' assigned to them by a tool of persecution, the so-called FETO-Meter," Ali Yildiz, one of the authors of the report and a legal expert, told BIRN.

Yildiz added that "this situation is far from being unique to Turkey: in an increasingly connected world where states make wider recourse to counter-terrorism surveillance tools, the possibility of falling victim to algorithmic persecution is high".

"The report, therefore, serves as a wake-up call to bring more awareness to the devastating effects of algorithmic persecution and oppression not just in Turkey, but also in the entire world," Yildiz added.

The so-called FETO-Meter is based on 97 main criteria and 290 sub-criteria, many of which violate individual privacy.

The name references alleged supporters of exiled cleric Fethullah Gulen whom the government calls FETO, short for Fethullahist Terrorist Organisation. US-based Gulen has always denied any links to terrorism.

Algorithmic persecution in Turkey's post-coup crackdown: The FETÖ-Meter system

Emre Turkut & Ali Yıldız

FACTSHEET

After 2016's botched coup attempt, several algorithms were utilized by Turkish state authorities to profile all active and retired members of Turkish armed forces and determine those who were to be dismissed. The FETÖ-Meter Algorithm was particularly alarming because of its widespread use, unlawful ways of obtaining and processing private data, implicit approval of state authorities and the irrecoverable damage it caused. Statewatch published this report with the hope that understanding development in the array of formal democracies now led by authoritarian leaders will make it clearer why the norms of a pluralistic and open society must be defended continuously.

- **MASS USE:** The FETÖ-Meter is an excel based algorithm, designed by Rear Admiral Cihat Yaycı, to profile and determine the degree of 'terroristness' of all active and retired military officers. At least 810,000 individuals have been subjected to this profiling algorithm.
- **TARGETED A PARTICULAR SOCIAL GROUP:** According to Yaycı, it is a "decision support program" to uncover "crypto" Gülenist soldiers.
- **INSTITUTIONALISED:** A special unit called 'The Office of Judicial Proceedings and Administrative Action' (ATİİİŞ) was responsible for the application of this algorithm.
- **APPROVAL OF AUTHORITIES:** The ATİİİŞ became operational on 11 September 2016. Its personnel who run the FETÖ-Meter algorithm were personally chosen by Yaycı himself. The conclusions of ATİİİŞ that certain personnel should be dismissed as a result of the point he/she scored from of the FETÖ-Meter algorithm were fully endorsed by the government.



A Grotesque Data Privacy Infringement



97
Main Criteria



290
Sub-Criteria

810,000 Individuals screened / subjected to unlawful profiling



16
Government Ministries Provided Data

25

Public Institutions Cooperated with the System

~1 million
GSM Numbers' Record of Phone Calls and Internet Traffic Scrutinized



19 million
Lines of Banking Data Screened

more than 20,000

Personnel Dismissed from the Armed Forces based on the Algorithm

A Fourfold Profiling System

The system collected and processed data on:

1. The Private Life
2. The Professional Life
3. The Social Circle
4. The Relatives of the subjects.

The questions for profiling and scoring individuals include information of their marriages, education, bank accounts, their children's school records, their promotions and references in the army. The questionnaire demands information about people's relatives and also neighbours. It was deployed following the July 2016 coup attempt to root out alleged followers of Gulen who is accused of masterminding the failed coup.

"Hundreds of thousands of people have been profiled and assigned a 'score' by the algorithm, which is operated by a special unit called 'The Office of Judicial Proceedings and Administrative Action', ATİİİŞ, within the Turkish navy," Emre Turkut, another author of the report and an expert on international human rights law from Hertie School Berlin, told BIRN.

Turkut said that the report includes testimonies from several high-ranking former military officers who have since sought asylum in the EU, and highlights that application of the algorithm has been arbitrary and underpinned punitive measures not only against primary suspects but anyone in their social circles, including their family members, colleagues, and neighbours.

However, Cihat Yaycı, a former navy admiral and the architect of the FETÖ-Meter algorithm, has defended it. "FETÖ militants are very successful in hiding their real identities. The FETÖ-Meter gave us very successful results for identifying Gulenists," Cihat Yaycı said in a TV interview in 2020.

Since 2016, 292,000 people have been detained and nearly 598,000 people

investigated over their alleged links with Gulen. According to the Turkish defence and interior ministries, nearly 21,000 members of the armed forces, 31,000 police officers, more than 5,500 gendarmerie officers and 509 coastguards have also lost their jobs over alleged links to Gulen. More than 30,000 people are still in prison because of their alleged ties to the cleric and more than 125,000 public servants have been dismissed.

Massive cyberattack disrupts petrol stations in Iran

Source: <https://www.aljazeera.com/news/2021/10/26/cyberattack-affects-petrol-stations-across-iran>

Oct 27 – A significant cyberattack has hit Iran's online petrol distribution system, affecting fuel stations across the country and causing long lineups.

State television and an outlet close to the country's security apparatus said on Tuesday that the origins of the hack were under investigation.



Thousands of petrol stations went offline starting before noon, but the cause was not confirmed as a cyberattack until later in the day.

After several hours, some petrol stations across the country restarted offering services, but offline and at the open rate that is twice the subsidised rate offered through rationed “smart fuel cards”. Officials said all petrol stations will be back online soon.

Hassan Firouzabadi, the secretary of Iran’s Supreme Council of Cyberspace, told state TV late on Wednesday that the cyberattack was “probably” sponsored by a foreign state, but it is “too early” to name that country.

Iran has suffered several high-profile sabotage attacks recently, including two – blamed on Israel – against [its main nuclear facilities at Natanz](#).

The widespread attack came shortly before the second anniversary of the November 2019 nationwide protests against an overnight petrol price rise.

At the time, petrol prices as much as tripled, sparking the protests that Amnesty International has said led to the deaths of more than 300 people. Internet access was also shut down across the country for almost a week during the protests. Some areas where protests were still continuing experienced weeks of internet disruptions. Social media videos early on Tuesday showed long queues at petrol stations that were out of commission. Several also showed that digital city monitors were hacked, displaying messages such as “Khamenei, where’s our petrol?” addressed to the country’s supreme leader.

Local officials denied the monitors were hacked. Al Jazeera could not independently confirm the veracity of the videos.

The semi-official ISNA news website published a story saying the petrol distribution system and the digital city monitors were hacked, but it later said its website was targeted by a cyberattack and hackers published the story.

Democratizing Harm: Artificial Intelligence in the Hands of Non-State Actors

Source: <https://www.hstoday.us/subject-matter-areas/terrorism-study/democratizing-harm-artificial-intelligence-in-the-hands-of-non-state-actors/>



An ISIS member in Sinai tinkers with a U.S.-made captured Egyptian military drone in 2020. (ISIS photo)

Nov 29 – Advances in artificial intelligence (AI) have lowered the barrier to entry for both its constructive and destructive uses. Just a few years ago, only highly resourced states and state-sponsored groups could develop and deploy AI-empowered drones, cyberattacks, or online information operations. Low-cost, commercial off-the-shelf AI means that a range of nonstate actors can increasingly adopt these technologies.



As the technology evolves and proliferates, democratic societies first need to understand the threat. Then they can formulate effective policy responses. This report helps them do both. It outlines the contours of AI advances by way of highlighting both the accessibility and appeal to nonstate actors such as terrorist, hacking, and drug trafficking groups. Based on the analysis, effective or feasible policy responses are unlikely to Advances in artificial intelligence (AI) have lowered the barrier to entry for both its constructive and destructive uses. As the technology evolves and proliferates, democratic societies first need to understand the threat. outright bans on AI or autonomous vehicles that rely on AI because of questions about enforceability. AI is so diffuse that such bans are not practical and will not be effective. Instead, public-private partnerships will be key in incorporating software restrictions on commercial robotics, for example, which would address the potential consequences of nonstate actors using AI to program the flight and targeting of a drone.

Cultivating a broader and deeper talent pool in the science, technology, engineering, and math (STEM) fields will also help enrich the ability of democratic states to guard against the misuses of AI-enabled technology. Lastly, democratic societies should work together to develop ethical use norms, which may not preclude the misuse by nonstate actors but at least create guardrails that present obstacles to the export of harmful AI technologies from states to non-states and can shape the ways nonstate actors consider using these technologies.

Rules of war need rewriting for the age of AI weapons

Source: <https://www.ft.com/content/d8371144-364b-496d-943c-16f7e0982b6e>

Whoever becomes the leader in artificial intelligence “will become the ruler of the world”, Vladimir Putin said in 2017, predicting future wars would be fought using drones. Even then, for all the Russian leader’s own ambitions, China and the US were the frontrunners in developing the technology. Yet four years later, the vision of autonomous fighting units is becoming a reality, with potentially devastating consequences. The computer scientist Stuart Russell — who will devote a forthcoming Reith Lecture on BBC radio to the subject — met UK defence officials recently to warn that incorporating AI into weapons could wipe out humanity.

AI promises enormous benefits. Yet, like nuclear power, it can be used for good and ill. Its introduction into the military sphere represents the biggest technological leap since the advent of nuclear weapons. While atomic bombs were used on real cities in 1945, however, it took more than two decades before the first arms control treaties were signed.

Nuclear weapons are also difficult and expensive to develop or obtain. By contrast, AI-aided arms — used at scale — could combine the power of weapons of mass destruction with the scope for cheap production of the AK-47. That opens the possibility of their use, even if not in their most sophisticated forms, not just by advanced economies but by “rogue” states and terrorists. And the world is starting to wrestle with how to control them while the technology is still evolving at lightning speed.

The most immediate concern is “lethal autonomous weapons systems” (Laws), often dubbed “**killer robots**”. In fact, the term means any mobile platform — drone, android, self-flying plane — carrying a machine that can perceive its environment, make decisions on tactics and targets, and kill. Rudimentary versions exist today. The UN says Turkish-made Kargu drones incorporating image-processing capabilities were used in Libyan conflicts last year to home in on selected targets.

Academics warn of swarms of cheap miniature drones armed with facial recognition and tiny bombs being used as mass killing machines. Many experts have demanded a ban on developing lethal autonomous weapons. A UN body has drawn up guidelines and worked on a potential embargo. Several military powers oppose a ban, fearing the loss of a chance to gain a military edge or that other would ignore a prohibition that would be near impossible to enforce.

Yet many countries have joined conventions on biological and chemical weapons, though these also offer cheap routes to mass lethality. The scientific community says it has ideas and lessons from other arms control efforts on how to devise and police a Laws ban.

Beyond killer robots, AI could be used to enhance or replace human skills in everything from operating weapons to intelligence gathering and analysis, early warning systems, and command and control. Dialogue is needed not just between the biggest military powers but more broadly on rules of engagement, what sort of wars countries are prepared to countenance in an AI era, and how to impose some transparency and constraints. Agreements are needed to keep humans “in the loop” in all forms of military decision-making.

Establishing such contacts will not be easy; China is reluctant to engage with the US even on nuclear arms. But past leaders agreed on “rules” of war, with at least some limited success, because they saw it as in their mutual interests to do so. It should be more than a naive hope that those rules can be updated for an age when humans are combining awesome destructive force with machines that can calculate faster than they can.

EDITOR’S COMMENT: Rules at war? In the 21st century? Is this a joke or what?

Using Math to Prove Computer Security

Source: <https://www.homelandsecuritynewswire.com/dr20211202-using-math-to-prove-computer-security>

Dec 02 – Eureka prize winner and University of Melbourne Associate Professor Toby Murray thought math was boring, but he now relies on it to secure critical systems like those of the Australian Department of Defense against hackers.

Murray talked with Catriona May, [University of Melbourne](#).

'Secure' computer systems get hacked all the time. We live in a world where very few systems are truly safe, and proving that a system is secure is challenging. It's about understanding the kind of evidence required. I first became interested in how to prove a platform is secure when I was working for Defense in the early 2000s – and I'm still working on it.



I started my Ph.D. thinking I was going to answer this tough problem and then I moderated my ambitions! Proving security is difficult. But I have continued in the same direction since.

When I was an undergraduate I thought 'the math stuff' in software development was boring and useless. But math became a necessity. What helped convince me were some cases in the 90s and early 2000s where mathematical approaches proved that systems everyone thought were secure actually weren't.

I still don't consider myself a good mathematician, but it's a tool I find very useful for my work. Computer systems are highly complex but we can distil security problems down to the critical details. Once we have the essence of the system, we can describe its constituent parts really elegantly using mathematics and logic.

Back in 2015 we had no mathematics to prove the security of important software systems performing multiple tasks at once. These are known as concurrent systems. We realized there was an opportunity to develop new methods to interrogate and test these kinds of software, so we developed the [COVERN](#) logic.

It's a tool for distilling the logic underpinning the security of software that does different things at different times. It essentially works through a computer program, but like any kind of mathematical proof it still requires some human intelligence.

Our research can be dry and tricky so connecting with something practical was a wonderful opportunity. We developed COVERN to prove the security of a new device for Defense, called the [Cross Domain Desktop Compositor](#) (CDDC). It safeguards sensitive data while allowing instant access to online content.

Working on a real-world project meant we weren't just talking about abstract software fairyland, but actually making sure our research is useful.

Some of my partners on the CDDC project were colleagues back in my Defense days. We worked together twenty years ago, when Wi-Fi was just emerging and iPhones didn't exist. It's been great to work together again on such a successful project.

It was initially very difficult to interrogate and test the security of the CDDC. That was because it is concurrent and dynamic, with users potentially handling top-secret data one minute and using the public Internet the next. When we first started the project in 2015, we had no idea how we could prove its security. It's been very satisfying to deliver a solution.

It might seem like an odd question, but now I'm asking, 'how do I prove my system has a vulnerability?' It's the opposite question to the one I started with, which was 'how do I prove my system is secure?'. But, actually, it is easier to look for evidence of trouble rather than evidence of the absence of trouble. It means we can look more quickly and easily for vulnerabilities we might expect to find in certain kinds of systems.

Our mathematical methods that prove security can also prove systems have vulnerabilities. That's been really interesting to discover. They have some unique advantages over other methods, too. Again, it's all about deconstructing the large system and analyzing its constituent parts.

This means that when we change one part of the system, we only need to re-analyze the parts we changed, so we can search for vulnerabilities incrementally. While it's not as assuring as proving security, proving vulnerability can be a faster and simpler process.

Murray was part of the team that won the 2021 Science and Technology Eureka Prize for [Outstanding Science in Safeguarding Australia](#), along with University of Melbourne colleague [Dr. Robert Sison](#) and colleagues from the University of New South Wales and the Defense, Science and Technology Group at the Department of Defense. Catriona May is a freelance writer.



New Cyber Protections against Stealthy “Logic Bombs”

Source: <https://www.homelandsecuritynewswire.com/dr20211211-new-cyber-protections-against-stealthy-logic-bombs>

Dec 11 – Cybersecurity researchers at [Rutgers University-New Brunswick](#) and the Georgia Institute of Technology have proposed new ways to protect 3D printed objects such as drones, prostheses, and medical devices from stealthy “logic bombs.”

The researchers presented their paper, titled “[Physical Logic Bombs in 3D Printers via Emerging 4D Techniques](#),” at the 2021 Annual Computer Security Applications Conference on December 10, 2021.

Rapid prototyping is the quick fabrication of a part, model or assembly using 3D computer aided design, usually using 3D printing or “additive manufacturing.” Additive manufacturing is increasingly used in a range of industries to produce safety-critical products, but there currently are no trustworthy methods for verifying their integrity against adversarial pre-print design modifications.

“Next-generation, cyber-physical additive manufacturing enables advanced product designs and capabilities, but it increasingly relies on highly networked industrial control systems that present opportunities for cyber-attacks,” said principal investigator Saman Zonouz, an associate professor of electrical and computer engineering in the Rutgers-New Brunswick School of Engineering. “The predominant approach to defending against these threats relies on host-based intrusion detectors that sit within the same target controllers, and hence are often the first target of the controller attacks.”

The researchers looked into Mystique, a new class of attacks on printed objects that leverage emerging 4D printing technology to introduce embedded computer code – or logic bombs — by manipulating the manufacturing process.

Mystique enables visually harmless objects to behave maliciously when a logic bomb is triggered by a stimulus such as changes in temperature, moisture, pH or modifications to the materials used initially, potentially causing catastrophic operational failures when they are used.

The researchers successfully evaluated Mystique on several 3D printing case studies and showed that it can evade prior countermeasures. To address this, they proposed two strategies.

The first solution focuses on designing a sensor that can measure the composition and diameter of raw materials passing through the printer’s extruder to ensure they meet expectations before the object is printed. A dielectric sensor can detect a change of 0.1mm in filament diameters and a change of 10% in concentration composition.

The second solution uses high-resolution computed tomography images to detect residual stresses in printed objects that contrast benign and malicious designs before activation of the attack. This CT detection has an accuracy of 94.6 percent in identifying 4D attacks in a single printing layer.

The research team plans to provide guidelines to tie together resilience solutions in software security, control system design and signal processing, and to incorporate reliable and practical cyber-physical attack detection into real-world manufacturing.

“Our proposal is a novel potential attack vector that needs to be considered and mitigated effectively in additive manufacturing platforms. The idea is to use new physical logic bombs in 3D printed objects, such as industrial gears and personal protective equipment like COVID-19 masks,” Zonouz said. “These logic bombs can later be activated by the adversaries using physical stimulus like moisture or heat whenever suitable for them to make the printed objects malfunction, such as to make a COVID mask lose its protection against the viral infection.”

CSS Analyses in Security Policy

No. 296, December 2021



Regulating Cybersecurity in the Health Care Sector

During the COVID-19 pandemic, awareness about vulnerabilities in the health care sector increased. Experts from governments, civil society, and industry called for more cybersecurity regulation that clarifies responsibilities and expectations. Regulation is one answer, but some issues require other policy solutions, such as further international cooperation.

Nele Achten is Senior Researcher for Cybersecurity Policy in the Swiss and Euro-Atlantic Security Team at the Center for Security Studies (CSS) at ETH Zürich.



How China Could Cyberattack Taiwan

By Ralph Jennings

Source: <https://www.homelandsecuritynewswire.com/dr20211211-how-china-could-cyberattack-taiwan>

Dec 11 – China has the means to launch a disabling cyberattack against political rival Taiwan ahead of any military invasion, experts say, as the technology is already targeting the island's political leadership.

Beijing claims self-ruled Taiwan as its own and has threatened to use force if necessary to unify the two sides. The claim has held since the Chinese civil war of the 1940s, when Chiang Kai-shek's Nationalist government reestablished on the island after losing to Mao Zedong's Communists. Most Taiwanese prefer to maintain the status quo, according to a [National Chengchi University poll](#).

A straight-up military invasion would cost lives and mobilize U.S. forces for Taiwan's defense. Disruptive cyberattacks could sow chaos and soften Taiwan's defenses, potentially making an invasion less costly for Beijing, according to Chen Yi-fan, assistant professor of diplomacy and international relations at Tamkang University in Taiwan.



Attacks Happening Already

Chinese operators are already using the internet to launch an estimated 200 million to 400 million attacks each month, mostly targeting websites run by the government and Taiwan's all-important semiconductor companies, Chen said.

"PLA's [People's Liberation Army] Strategic Support Force and its Network Systems Department may be those behind the scenes to conduct the maneuvers," Chen said. "Successful cyberattacks can disable Taiwan's critical infrastructure and make Taiwan vulnerable to follow-up PLA attacks."

Anonymous mainland Chinese nationals already poke at Taiwan by mobilizing thousands of social media accounts to condemn domestic policies of the island's ruling Democratic Progressive Party (DPP), said Yun Sun, co-director of the East Asia program at the Stimson Center in Washington. The party takes a guarded view of any China-Taiwan unification.

In December 2019, [DPP spokesperson Lee Yen-jong said](#) the "Chinese internet army" had posted a "malicious" video on Facebook about a month ahead of party-backed President Tsai Ing-wen's reelection. The video posed as a campaign commercial in support of the DPP and falsely claimed the party supports China-Taiwan unification under the one-country, two-systems type of rule that Beijing uses to govern Hong Kong.

Attacks today seek to steal intelligence and compile a list for cyberattacks in the "precision strike phase of any future operations," said Taiwan's Ministry of National Defense in a recent report.

During wartime, the report says, cyberattacks can be used to sabotage and destroy "national critical infrastructures and C2 [command and control] systems to cause turbulence and chaos in its society and decimate the internal security kept by the military and law enforcement organs of the nation and its government functions."

The Chinese government does not acknowledge launching any attacks. The Chinese state-backed [Global Times](#) website, however, said this week that a Taiwan-based organization called GreenSpot had launched cyberattacks since 2007 against Chinese government agencies and aerospace and military-related research institutes "to steal high-value data and classified information."

Disable First, Strike Later?

China could disable Taiwanese computer systems that run transport, utilities and defense operations to make a military strike easier, scholars suggest.

"If there is a war, and the Chinese shut down the power grid through a cyberattack, that may not completely shut down Taiwan's defense system, but it's going to have an impact," Sun said.

Successful cyberattacks on financial institutions and other targets would shake people's confidence, said Alexander Huang, chairman of a military strategy research foundation in Taipei. All of Taiwan's "critical infrastructure" is connected by the internet, he added, a linkage that could cause "great difficulties" as well as widespread panic among people.

"If we got a cyberwar, then all these systems are down," Huang said. "If the communication node is broken, then it would be a form of decapitation."

Advanced conventional weapons such as new submarines and aircraft would be of little use during a debilitating cyberattack, he said, adding that it's unclear whether Taiwan's government has taken enough measures to guard against a major cyberattack.



Taiwanese officials first signaled awareness of the threat in 2000. The National Security Council came out with an “information and communication infrastructure security mechanism plan” that year and, in 2001, the government created a related task force, the academic website Taiwaninsight.org says. The government-run Central News Agency said Taiwanese officials began planning in 2018 to set up a cybersecurity academy that would help overcome a talent shortage among civil servants.

A media liaison with the defense ministry did not answer a request for comment on any preparations for wider cyberattacks from China.

Ralph Jennings is a writer covering China.

On the Threat of Deep Fakes to Democracy and Society

Source: https://www.counterextremism.com/sites/default/files/CEP-KAS_Deep%20Fakes_062920.pdf

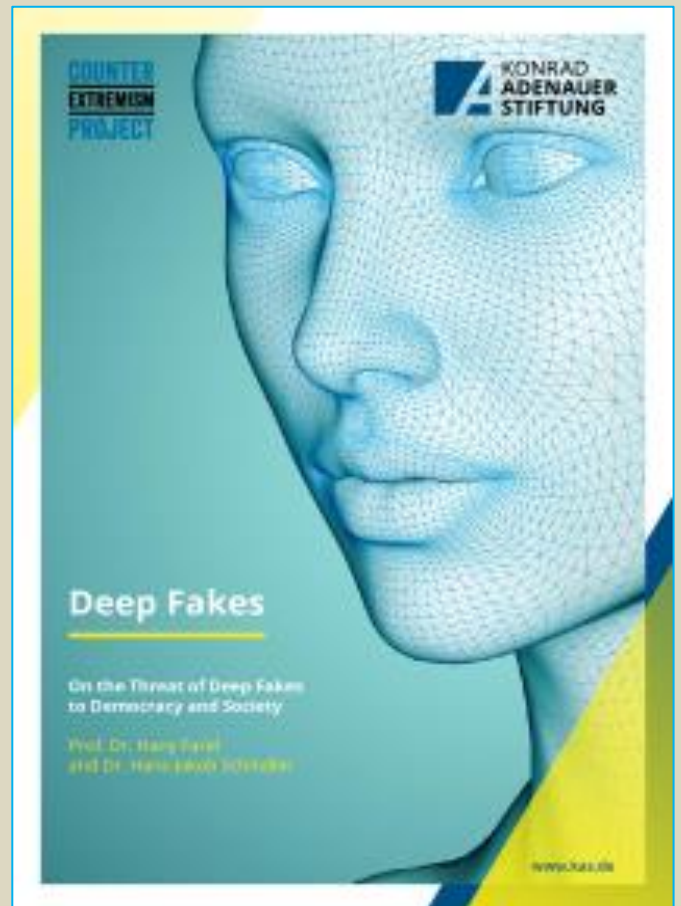
The influence of fake news and the manipulation of public and political perception has been a threat to political systems for years. Today, fake news is often supported by so-called deep fakes—seemingly real but synthesized videos of various kinds. Due to advances in software design, significant technical skills to produce deep fakes are no longer necessary, vastly increasing the risk of their misuse. CEP, in cooperation with the Konrad Adenauer-Stiftung (KAS), released a study, [On the Threat of Deep Fakes to Democracy and Society](#).

The authors, Dr. Schindler and CEP Senior Advisor Dr. Hany Farid, discussed the study and ways to confront the problem during a [CEP webinar](#).

Key messages

The present study is the result of a cooperation between the Konrad-Adenauer-Stiftung and the Counter Extremism Project. The authors, Prof Dr. Hany Farid and Dr. Hans-Jakob Schindler, deal with the destructive potential of so-called deep fakes – videos and images altered by artificial intelligence (AI) misused for political manipulation.

- ❖ Manipulated images and videos have already been posing major challenges to journalism, science, jurisdiction and politics in the past. New technology, however, has made the production of deep fakes widely available to the public – we are experiencing a democratization of deep fakes. Deep fakes used in disinformation campaigns can cause social cohesion and thus be a threat to democracy.
- ❖ Social media play an increasingly central role in informing the public and have become the main distribution platform of fake news. These platforms are operating unregulated and with different standards, presenting a particular challenge in the fight against disinformation campaigns.
- ❖ Germany is at an early stage of this new challenge. There is still enough time to develop an effective defense mechanism against the threat of deep fakes.
- ❖ The fight against this complex challenge requires a multipronged approach which combines technical solutions with legal and public education measures.



*Prof. Dr. Hany Farid, Professor, University of California, Berkeley; Senior Advisor, Counter Extremism Project
Dr. Hans-Jakob Schindler, Senior Director, Counter Extremism Project*



ICI
International
CBRNE
INSTITUTE



HOTZONE
SOLUTIONS
GROUP



C²BRNE
DIARY

DRONE NEWS



Iran's Growing UAV Capabilities Unveiled

Source: <https://i-hls.com/archives/111800>

Nov 25 – Iran has been using unmanned aerial vehicles for launching attacks and smuggling weapons. Isarel Defense Minister Benny Gantz said that Iran has launched maritime attacks with unmanned aerial vehicles from bases in the country's south.

"One of the key tools is UAVs and precision weapons, which can reach strategic targets within thousands of kilometers, and thus this capability is already endangering Sunni countries, international troops in the Middle East, and also countries in Europe and Africa," he said, according to [jerusalempost.com](https://www.jerusalempost.com).

Tehran also attempted to send explosives to Palestinian terrorists in the West Bank from Syria using unmanned aerial vehicles, Gantz said. "Iran is not only using unmanned aerial vehicles to attack but also to transfer weapons to its proxies." In February 2018, Iran carried out an attempt to smuggle TNT explosives using the **Shahed m141 UAV**. The advanced Iranian drone took off from the



T-4 airbase in Syria and crossed into Israeli territory via Jordanian airspace, according to Gantz. The drone was spotted and intercepted in Israel near Beit She'an by an Apache attack helicopter.

►► Read also: [The Oryx Handbook of Iranian Drones](#)

A cascading catastrophe: The drone threat to critical infrastructure

By Zachary Kallenborn

Source: <https://thebulletin.org/2021/11/a-cascading-catastrophe-the-drone-threat-to-critical-infrastructure>

Nov 26 – The FBI recently revealed an [attempted drone attack](#) on the American electric grid, via an electrical substation in Pennsylvania. Someone or some group modified a drone to dangle a length of copper that, if it hit high-voltage equipment below, would have caused a short circuit. While the drone crashed into the ground without causing any harm, in theory a successful attack could have caused broader power outages and much bigger problems.

The 2020 attack failed, but a blueprint for trouble remains.

Risks to critical infrastructure are growing as terrorists increasingly adopt drones as an attack vehicle. Commercial drone producers are not only making larger drones available at lower cost, they are making increasingly sophisticated systems that incorporate capabilities like autonomy. But drones have numerous legal and popular uses— from taking glam real-estate





photos to checking on pipelines—the United States and global governments face a balancing act in trying to reduce the risks drones could pose.



Italian soldiers carry a counter-drone system. Credit: Italian Army. CC BY 2.5.

More drone terrorism

After failing as a political force in Japan, Aum Shinrikyo, the infamous doomsday cult that once boasted tens of thousands of members, believed it would prevail in a [World War III-style](#) battle by arming itself with chemical, biological, and [nuclear](#) weapons; it even sought [earthquake-generating machines](#). Aum also appears to be the first terrorist organization to pursue [drone warfare](#), acquiring, a Russian helicopter and two remote controlled drones in order to [deliver](#) biological weapons, according to a Stimson Center report.

The Japanese government largely brought down Aum after the 1995 sarin gas attacks on the Tokyo subway system. But other terrorist groups have since followed Aum's lead in pursuing drones.

[Trends](#) in terrorist drone use had been steady and upward until ISIS, which at one point had captured vast swaths of Iraq and Syria for its caliphate, took things to a whole new level in the early 2010s. The group flew [frequent](#) drone operations, hundreds in one month in 2017 alone. ISIS showed it could “strike with a small munition with surprising accuracy with near complete surprise into areas that are believed to be safe,” a military analyst told *Vice's Motherboard* at the time.

Growing terrorist use of drones is no surprise. After the September 11th attacks, most counter-terrorism measures assumed a ground-based attack: suicide bombers, car bombs, and the like. Aerial drones allow terrorists to skip over the ground-based defenses, like fences and bollards, are easy to buy or [even make](#), and can be launched from safe (for the terrorist) distances. Avoiding all that folderol on the ground is clearly an advantage for a terrorist. The next terrorist attack in the United States won't necessarily be a drone attack, of course. Cheap drones with [small payloads](#) might not be worth it for an attacker. Larger drones that can reach a [thousand or more pounds](#), while available on the commercial market, are expensive. Drones are also new, and terrorists might not want to risk a botched attack. They might just buy a gun and shoot up a mall, or drive a truck through a crowd. But as Middle East experience shows, the threat of terrorist drone use is real.

Critical infrastructure at risk

Terrorist organizations can be expected to increasingly target critical infrastructure. The energy grid, water ducts, transportation infrastructure, and other critical systems are necessary for society to function. Disrupting those systems allow terrorists to create large-scale effects with relatively minimal capability.



The risk of [cascading consequences](#)—that is, when damage to one area of critical infrastructure cascades to others—is particularly concerning. In 2019, during [a five-day blackout in](#) Venezuela, hospitals lost power, patients died of treatable conditions, food spoiled, residents went to rivers to drink, and transport stalled. The Venezuelan government has blamed sabotage and terrorists for blackouts, but others say the outages in that oil-rich country simply reflect its poor track record of investment in energy infrastructure.

Drones have [already been](#) used by non-state groups to halt critical infrastructure operations. In December 2018, unknown operators flew two drones around London's [Gatwick airport](#), causing the airport to shut down for days and grounding thousands of flights. Then in 2019 either Iran or Houthi rebels from Yemen used drones to attack [Saudi oil facilities](#). (Whether the Houthi rebels or Iranian forces were responsible is unclear, though the Houthis have [previously](#) launched sophisticated drone attacks with Iranian support.)

The small payloads carried by many drones place an upper bound on how much damage any given drone can cause. So the question is: Can relatively small payloads of explosives cause significant damage, by, for instance, targeting areas of a facility that can cause [larger chain-reactions](#)? Facilities should assess for themselves the potential [vulnerabilities](#) of critical components within their facilities, and develop response plans.

Drones do not need to be used in direct attacks to be effective terror tools.

Drones provide terrorists with a platform to collect intelligence information to plan an attack. Standard hobbyist drones come with cameras attached. Terrorists could monitor security patrol patterns, inspect a facility parameter, and identify specific points of attack. For example, in the attack on two mosques in Christchurch, New Zealand, that killed 51 people, the attacker used a [drone](#) to scout the target.

Long-term trends

Drones are becoming increasingly autonomous. Commercial off-the-shelf drones are capable of basic [waypoint autonomy](#). That means they can be programmed to fly to particular points without a person moving the joystick. That would allow terrorists to create a crude “fire-and-forget” weapon; they could launch an attack, then run away before the first bomb explodes. Autonomy also poses a grand challenge for counter-drone systems, because most counter-drone systems rely on jamming the signal between operator and drone. If the drone needs no signal, then those defenses are obsolete.

Cheaper, more available, and more autonomous drones likely mean that terrorists will be more readily able to acquire drones and use more of them in a single attack. Technology also is increasingly enabling the use of true [drone swarms](#)—drones that communicate and collaborate on the basis of artificial intelligence. Such advances necessarily require greater capability on the part of the terrorist organization, to include the programming and algorithmic skills to design the system. But that's far from impossible: MIT students designed the [Pardix drone](#), one of the Department of Defense's leading swarming drones.

Reducing the threat

Depending on specifications, drones can be cheap—some quite capable models cost no more than \$100—and still theoretically useful in a crude attack on critical infrastructure. Of course, would-be terrorists could acquire much more capable and expensive drones, as well. Controlling the sale of popular and useful tools is difficult. What should the US government, or others, do to reign in the threat drone terror could pose to utilities or other critical infrastructure?

Within the United States, only [federal authorities](#) can operate counter-drone systems. The Department of Homeland Security's 2019 *Counter Unmanned Systems Technology Guide*, a 33-page booklet about drones and ways to detect and disable them, contains four warnings, in case anyone mistakes the guide's description of the counter-drone systems for permission to build or acquire them. Counter-drone systems create their own risk to surrounding systems. A drone-jammer does not just jam the signal to the drone, but any signal operating on the [same frequency](#). That could include air traffic control radio, and other critical signals.

But a federal monopoly on these important defenses raises questions about how effective they can be in an emergency.

If a critical infrastructure owner or operator has to call the FBI when they fear a drone attack, any response will mean little, unless counter-drone operators are already on site. A [racing drone](#) flying over 100 miles per hour will outrun a federal SUV every time, especially when the drone has a significant head-start.

The [Department of Homeland Security](#) has legal authority to protect “covered” facilities and assets, though exactly what types of facilities are protected is unclear from open sources. (And realistically, that information should not be publicly available, because it would provide a clear guide for adversaries on what facilities are unprotected.) Unless the department protects every covered facility, there will be vulnerabilities, because correctly anticipating every terrorist target is impossible/

Growing technology may create opportunities to avoid making tough value trade-offs. The same technology that allows drones to operate remotely or autonomously may be applied to counter-drone systems. A [network](#) of remotely-operated or autonomous counter-drone systems stationed at critical infrastructure sites would allow federal authorities to maintain control, while also allowing far more rapid response to drone events. Authorities could manage numerous counter-drone systems dispersed over a whole region from a central location.



Critical infrastructure faces growing risks from drone terrorism. As the stories of Aum, ISIS, and other terror groups show, non-state actors have been using and experimenting with drones since the mid-1990s. At least back then, to obtain them they had to do more than a quick search on Amazon.


***Zachary Kallenborn** is a research affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a policy fellow at the Schar School of Policy and Government, a US Army Training and Doctrine Command “Mad Scientist,” and national security consultant. His work has been published in a wide range of peer-reviewed, trade, and popular outlets, including Foreign Policy, Slate, War on the Rocks, and the Nonproliferation Review. Journalists have written about and shared that research in outlets including Forbes, Popular Mechanics, Wired, The Federalist, Yahoo News!, and the National Interest.*

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY FEDERAL PAGES
DHS

STAY CONNECTED

The Threat from Drones and How You Can Prepare

Security professionals should incorporate drone-related security into their planning regardless of their location, status, or posture.

 By Sarah Jacob November 24, 2021



- Advertisement -

Sign Up

to receive HS Today
Newsletters.

Sign Up for FREE

As drone popularity increases, feds look to rein in bad behavior

Source: <https://www.washingtonpost.com/transportation/2021/12/03/drones-flying-prosecutions/>

Dec 03 – The firefighters were standing outside on a summer day when a drone — its blades whirling in a high-pitched whine — headed right for them, sending them scurrying, authorities said.

Then it came again.

“They had to dive out of the way to avoid being struck,” said Christopher Kavanaugh, U.S. attorney for the Western District of Virginia. Some city police officers also were sent scrambling.

The harassment outside the Salem, Va., firehouse — located feet from a monument of steel beams retrieved from the wreckage of the World Trade Center’s North Tower — continued until the first responders retreated into the station. The drone then followed them into the garage, investigators with the U.S. Department of Transportation said.

As the popularity of drones has grown in recent years, so has their misuse. The proliferation of small aircraft involved in untoward actions has led federal investigators to try to rein in some of the most egregious behavior.

The Virginia case is among a handful of drone-related prosecutions that have led to recent convictions.

Ultimately, the drone smashed into a pole, and no one was injured. James Russell Weeks III, of Salem, pleaded guilty recently in connection with the July 2019 incident.

Under a broad provision in federal law, Weeks was charged with flying an unregistered aircraft, which covers drones that weigh more than 0.55 pounds. Prosecutors say that catchall charge and other similar provisions offer straightforward tools for dealing with a range of crimes using drones.

In June, a Georgia man who was jailed for armed robbery was sentenced to 12 months for allowing someone else to use, or try to use, his unregistered aircraft. Federal prosecutors said the man and his brother had plotted to smuggle cellphones and tobacco into Telfair State Prison, but his brother and an accomplice were stymied by sheriff’s deputies in nearby woods.

Last year, a Bangor, Pa., man was sentenced to five years in prison after pleading guilty to operating an unregistered aircraft, as well as firearms charges. Federal prosecutors said the man, who had been subject to a domestic violence protective order, dropped small homemade bombs from a drone to scare his ex-girlfriend and “terrorized an entire community.”

The Salem investigation was led by the U.S. Department of Transportation’s inspector general’s office. Given the proliferation of drones, the office “is committed to doing all that



we can to help ensure that unmanned aircraft systems are operated legally, especially where public safety and the operations of first responders is concerned,” the office said in a statement.

The Federal Aviation Administration, which has responsibility for the safety of U.S. airspace, said a regulation finalized earlier this year will require drone operators to broadcast identification information and their aircraft's location. That will aid law enforcement trying to connect unauthorized drones with people flying them, the agency said. Operators must comply by September 2023.

“Remote identification will help law enforcement determine if a drone poses an actual threat that needs to be mitigated, or if it's an errant drone that got away from someone but means no harm,” the FAA said in a statement.

[Drones kept entering no-fly zones over Washington, raising security concerns](#)

The case in Salem, a city of 25,000 near Roanoke in western Virginia, left many residents mystified. Was it more threat or nuisance? An ill-considered prank or lapse in judgment?

Randy V. Cargill, an assistant federal public defender representing Weeks, declined to say what might have been behind his client's actions, citing a policy against commenting on pending cases. Asked if Weeks intended to harm anyone, he noted that “no assault charges or anything akin to such were filed.”

Kavanaugh said Weeks had “used his drone to harass public servants,” and that he flew it in protected airspace around a local airport, warranting federal charges. In court filings, Weeks admitted to facts in the case as part of a plea deal, including flying the drone at the fire station.

“On July 25, 2019, firefighters at Salem's main fire station were ‘buzzed’ by a drone aircraft that darted at them a number of times,” according to a filing signed by Weeks, his lawyer and an assistant U.S. attorney.

Later that day, Weeks appeared at the Salem police station to ask for the return of his incapacitated drone.

As part of the plea agreement on the felony charge, prosecutors agreed not to pursue prison time. There was no agreement on probation or financial penalties. A sentencing date has not been set.

Salem deputy police chief Derek Weeks (no relation to James Weeks) said it did not surprise him that someone would misuse a drone in that way, but he balked at the notion that James Weeks's actions were a threat.

“I don't think it came across that way,” the deputy chief said, though he noted he wasn't there during the incident.

Added fire chief John W. Prillaman: “They were surprised, but they never felt endangered.”

About a block from the spot where Weeks dived his drone at firefighters and police sits the headquarters of a prominent Salem drone firm, Autonomous Flight Technologies. Salem city spokesman Mike Stevens found irony in that coincidence. The company's work with filmmakers, farmers, mining operators and others underscores what advocates say are the upsides of drones.

“To us, this was an isolated incident,” Stevens said. “There had not been any such buzzing occurrences before, and we have not experienced any since.” Police did not return Weeks's drone.

Flying UAV Laboratory

Source: http://cbrnintl.com/Flying_UAV_Lab.html

The "Flying Laboratory" is a pioneering UAV-based product with full CBRN monitoring capabilities, installed in a Penguin B high-performance unmanned platform. This complete, off-the-shelf system includes a second-generation ion mobility spectrometer (IMS), a UV particle fluorometer, a gamma spectrometer, and two Geiger counters. Options for video and IR also available.

The Flying Laboratory can detect up to 20 airborne chemical warfare agents and toxic industrial gases, unusually high biological aerosol levels, nuclear materials, and abnormal radiation levels.

Why airborne? Just one sensor-equipped UAV can perform the same level of surveillance as 12 to 24 fixed location sensors, and with greatly increased flexibility.

Product Features

- Second generation IMS toxic gas detection
- Identify nuclear materials
- Biological or radiological sampling





- Video monitoring
- UAV can be controlled manually or programmed for fully autonomous operation
- Flight time of up to 15 hours

▶▶ [Operational details](#)

Towards Paris Olympics – Europe’s First Vertiport Under Development

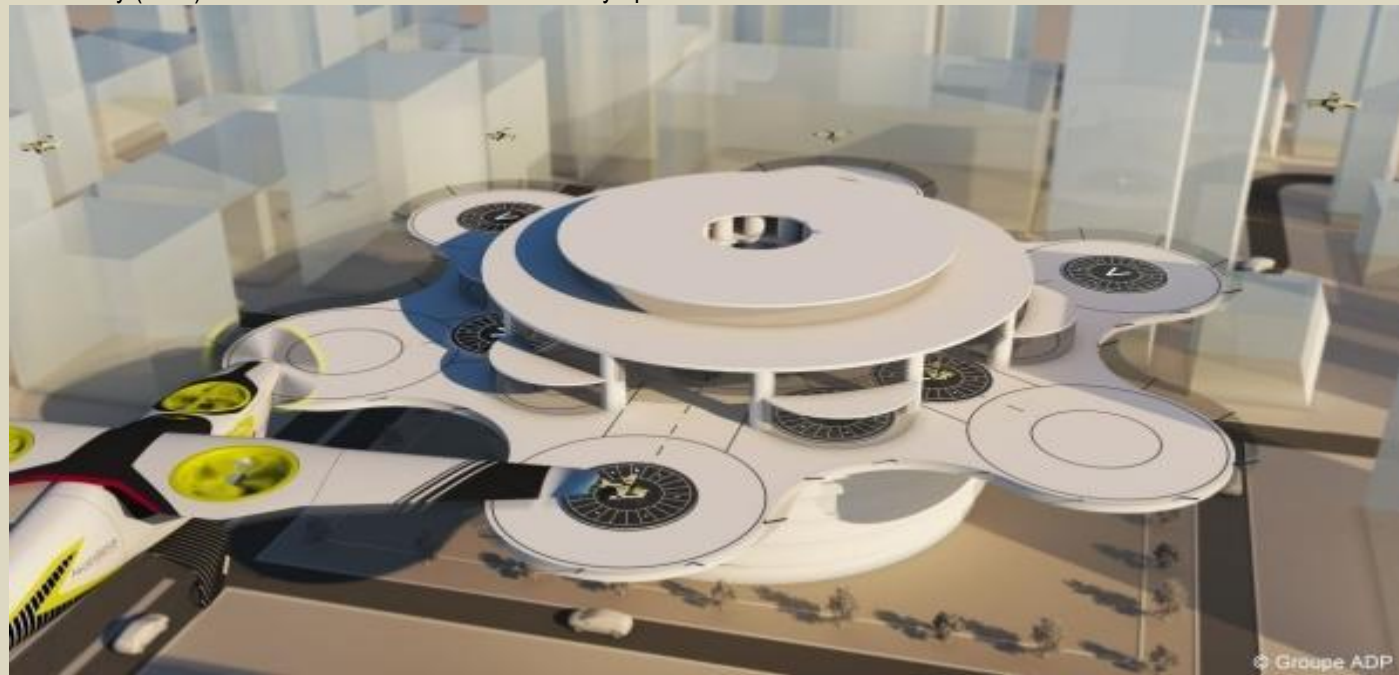
Source [+video]: <https://i-hls.com/archives/111980>



PARIS 2024



Dec 05 – Vertiports, landing sites for eVTOL aircraft, are one of the enablers required for regular air mobility. Europe’s first test vertiport is currently being developed in France, as a significant step towards launching commercial Advanced Air Mobility (AAM) services in time for the 2024 Paris Olympics.



The vertiport will be designed, built, and operated by Skyports at Cergy-Pontoise Airfield in Paris, initially serving as a technology testbed to provide a safe and realistic environment for Skyports and members of the initiative to integrate and test the critical technologies required to enable AAM in Europe.

The program is part of the Re.Invent Air Mobility initiative led by French airport operator Groupe ADP, global mobility company RATP Group and Choose Paris Region, a French agency for business and innovation.

The project is supported by DGAC, the French Civil Aviation Authority and EASA, the European Union Aviation Safety Agency.

The integration of a vertiport within an existing airport site is challenging and complex. Europe’s first trial platform will function as a concrete experiment to explore the field of possibilities of decarbonized and innovative aviation, and to develop the low altitude aviation market (below 300 meters).



All the components of Urban Air Mobility will be explored. The test vertiport will be equipped with a suite of technologies including biometric identity management, re-charging equipment,





situational awareness capabilities and weather stations. The data collected during the testing phase will be essential for the development of AAM regulatory frameworks.

The operational testbed will be used by leading eVTOL vehicle manufacturers to conduct test flights and demonstrations over the next three years in the run-up to the 2024 Olympics.

The site will be constructed using modular technology so that it can easily be relocated to a new location at the end of the program, serving as the first commercial vertiport in France, according to Skyports.

Kamikaze drones: A new weapon brings power and peril to the U.S. military

Source: <https://www.nbcnews.com/news/military/kamikaze-drones-new-weapon-brings-power-peril-u-s-military-n1285415>

Dec 06 — The killer drone whooshed out of its launch tube, spreading its carbon wings and shooting into the sky. Flying too fast for the naked eye to track, the battery-powered robot circled the Utah desert, hunting for the target it had been programmed to strike. Moments later, it sailed through the driver's side window of an empty pickup truck and exploded in a fireball. "Good hit," exclaimed an operator from AeroVironment, the company that produces the drone and sells it to the U.S. military. NBC News traveled to a military testing center for exclusive access to the first public demonstration of the Switchblade 300, a small, low-cost "kamikaze" drone made by AeroVironment, which sources said the U.S. military has used quietly for years in targeted killing operations in Afghanistan, Iraq and Syria. The demonstration told a story of promise and peril.



Americans have become accustomed to images of [Hellfire missiles](#) raining down from Predator and Reaper drones to hit terrorist targets in Pakistan or Yemen. But that was yesterday's drone war. A revolution in unmanned aerial vehicles is unfolding, and the U.S. has lost its monopoly on the technology.

An AeroVironment operator prepares to launch the Switchblade drone at Utah's Dugway Proving Ground. NBC News

A fighting edge

The Switchblade drone is an anti-personnel weapon that allows infantry to attack enemies concealed behind ridges or in other hidden positions.

Wingspan: About 2 feet
Length: Less than 2 feet
Weight: 5.5 pounds
Firing time: Under five min.
Crew: One-man operation
Speed: Up to 98 mph

Electric motor spins propeller
Drone gets its name from the way its wings deploy after launch
Explosives
Sensors include color and infrared video cameras

Strike from the sky
The Switchblade can be carried in a rucksack and enables troops to attack the enemy up to 12 miles away without calling for help such as air support.

Launch and arm

- Launched from a mortar-like tube
- Drone typically flies below 500 feet
- Soldier uses hand-held screen to find target
- Weapon armed after launch

Seek and destroy

- Can loiter for 10 minutes during search
- Will follow moving target, await command to destroy
- Guided by user to identify and lock on to target
- Flight can be aborted and reengaged

Source: AeroVironment Inc. Graphics reporting by TOM REINKEN
DOUG STEVENS Los Angeles Times

Some experts believe the spread of the semi-autonomous weapons will change ground warfare as profoundly as the machine gun did.

They can leapfrog traditional defenses to strike infantry troops anywhere on the battlefield, and they cost just \$6,000 apiece, compared to \$150,000 for the Hellfire missile typically fired by Predator or Reaper drones.

That capability could help save the lives of U.S. troops, but it could also put them — and Americans at home — in great danger from terrorists or nation-states that haven't previously had access to such lethal and affordable technology.

"I think this is going to be the new IED," or improvised explosive device, said [Shaan Shaikh](#), a missile expert at the Center for Strategic and



International Studies. “It’s something that we can see that is going to be a problem, and we have some defenses, but not enough.” Dubbed kamikaze, suicide or killer drones, these unmanned aircraft don’t fire missiles — they are the missiles. But unlike typical missiles, they can circle above a target, wait for the ideal moment and strike with incredible precision.

The U.S. military couldn’t have fought the way it did in Iraq or Afghanistan if the enemy had had killer drones. The next battlefield opponent is likely to have them. And terrorists will eventually get them, too — a possibility that has homeland security officials scrambling to find a solution, given that there is no surefire defense against them.

“There are over 100 countries and nonstate groups that have drones today, and the technology is widely proliferating,” said Paul Scharre, a former Army Ranger who is a scholar at the Center for a New American Security and the author of “Army of None,” a book about autonomous weapons. “It levels the playing field between the U.S. and terrorist groups or rebel groups in a way that’s certainly not good for the United States.”

Today’s small lethal drones are difficult to detect on radar, and they can even be programmed to hit targets without human intervention, based on facial recognition or some other computer wizardry. And while the Pentagon and the Department of Homeland Security are spending billions of dollars to come up with “counter drone” technology, experts say there is, as yet, no foolproof version of it.

Weighing just 5½ pounds, including its small warhead, the Switchblade can be taken into battle in a backpack and fly up to 7 miles to hit a target. The 300 model is designed to kill individuals, while a larger version, the 600, can destroy armored vehicles. AeroVironment isn’t yet allowed to show the bigger one to the public.

They are called “Switchblade” because their bladelike wings spring out on launch.

“It allows our warfighter to have a battlefield superiority, which our enemies can’t see, can’t hear, can’t tell it’s coming, and really precisely achieve a specific mission effect,” said Wahid Nawabi, AeroVironment’s Afghan-born CEO.

Nawabi said he has been told that the Taliban and others who have been on the receiving end refer to it as an angry bird or a buzzing bee.

Public procurement data show that the Switchblade 300 costs a small fraction of a Hellfire missile’s price tag, let alone the total cost of keeping Reaper drones in the air, flown by pilots in Nevada.

The Switchblade has a feature that allows the operator to adjust the blast radius, so it can kill the driver of a vehicle but not a passenger, for example. The weapon can be “waved off” up to two seconds before impact, AeroVironment says, in the event of a mistake or a risk to civilians.

That wave-off capability is notable in light of the [catastrophe in September](#) when the military killed 10 civilians, seven of them children, in a drone strike in Afghanistan that officials now say was a tragic mistake. A Pentagon review found that the strike team was unaware of the presence of children when it decided to fire. Officials said that a child was observed through a video feed of the target area after the launch but that by then the Hellfire missile couldn’t be recalled.

The Switchblade has cameras that show a target seconds before impact. But for a better view of the battlefield, it’s often used in conjunction with a small surveillance drone.

For the NBC News demonstration, AeroVironment used the Puma, which is launched by hand like a large model airplane and provides high-resolution color imagery of the ground. The images beamed back from the Puma’s cameras made it clear that an operator could see the expression on the face of a target in the seconds before the Switchblade struck.

Portable drones provide air support to small ground force units even when overhead assets — fighter jets, helicopters, larger drones — aren’t available, Scharre said.

“The ability to have something that’s small and tube-launched that’s in your backpack, that the squad leader has access to, that they don’t have to get on the radio and call in close air support ... that is a real game changer from a military capability standpoint,” he said.

It’s a game changer not just for the U.S.

The Switchblade may be the most advanced of the genre, but Russia, China, Israel, Iran and Turkey all have some version of a killer drone. Iranian-backed militias have [used small drones](#) in 10 attacks this year on U.S. bases in Iraq, the military says. No U.S. personnel have been hurt or killed, but it is only the beginning.

The tiny country of Azerbaijan used small Turkish-made drones to devastating effect against the Armenian military last year, bringing a decisive end to a stalemate over a disputed enclave that had gone on for years.

[Video released by Azerbaijan](#) shows the drones pummeling artillery, tank and troop emplacements surrounded by trenches that offered no protection whatsoever from the fiery death raining down from above.

Russia and Ukraine have used armed drones in [fighting over a disputed region](#), and Iranian-backed Houthi rebels [used them to blow up Saudi oil facilities](#) in 2019.

Drones, Scharre and other experts say, may usher in the largest transformation of ground war tactics since the [advent of the machine gun](#) at the turn of the 20th century, which quickly put an end to sending large formations of troops marching into gunfire.





Drones “are making the battlefield a much more dangerous place for ground troops,” Scharre said. “Now, hiding behind a wall, hiding in a trench line, is not enough to protect you from the enemy.”



An AeroVironment operator prepares to launch the Puma surveillance drone. NBC News

U.S. troops in Iraq are experiencing that danger firsthand. Iranian-backed militias have used small drones in nine attacks on U.S. facilities in Iraq this year, a U.S. military spokesman said. No one has been hurt or killed, but it’s only a matter of time.

A suicide drone attack on an oil tanker linked to an Israeli billionaire killed two crew members off Oman in the Arabian Sea on July 29.

“We have found that every time we come up with some way to defend ourselves against [drones], the technology rapidly advances to the point where it defeats our defensive capabilities,” said Michael Patrick “Mick” Mulroy, a retired Marine and former CIA officer who was deputy assistant secretary of defense for the Middle East from 2017 to 2019.

Mulroy, an ABC News analyst, said that drone defenses include electronic jamming and various methods to shoot them down but that there are technologies and tactics to bypass every possible defense.

The military, for example, can sometimes shoot high-powered weapons at incoming drones on a battlefield. Inside populated areas, however, small, explosives-laden unmanned aerial vehicles pose a more vexing problem.

In a war zone, “you could do more things with electronic warfare ... with using high-powered microwaves that might be very disruptive in a domestic context,” Scharre said. “You could shoot bullets on the sky in a war zone, and you might be less concerned about where they’re going land out in the desert than in a major American city.”

Meanwhile, all the barriers put up in cities to keep truck bombs away from buildings are useless against drones. So far, no terrorist group is known to have used a suicide drone. But experts believe it’s only a matter of time. The Islamic State terrorist group put explosives on [hobbyist drones](#) and used them to harass and occasionally injure coalition forces in Iraq and Syria. The specter of a swarm of explosives-packed drones buzzing toward a crowded U.S. sports arena keeps homeland security officials up at night.

But the government has been slow to react. It was only in 2018 that Congress granted the Department of Homeland Security and other law enforcement agencies the authority to take down drones deemed to be threats inside the U.S.

Since then, DHS has been contracting with outside companies and testing technologies to defeat the drone threat.

A spokesman declined to comment when asked for an update from DHS’ Science and Technology Directorate on the state of domestic counter-drone programs.

In an [article](#) on DHS’ website in July, the agency discusses some of its counter-drone efforts and notes that tests have been conducted. But the article doesn’t say whether the tests showed that any of the technology works consistently.

In 2018, the head of DHS’ intelligence division at the time told Congress that drones posed a major threat.

“Commercially available drones can be employed by terrorists and criminals to deliver explosives or harmful substances, conduct surveillance both domestically and internationally against U.S. citizens, interests and assets,” said the official, David Glawe. “This threat is significant, and it’s imminent, and it’s upon us.”

Swarm Talk: Understanding Drone Typology

By Zachary Kallenborn

Source: <https://mwi.usma.edu/swarm-talk-understanding-drone-typology/>

Dec 12 – In May 2021, during its conflict with Hamas, the [Israel Defense Forces](#) became the first military to use a drone swarm in combat. Not much is known about the event, other than that Israel used the drone swarm to strike “dozens” of targets in concert with other missiles





and munitions. Often media outlets use the phrase “drone swarm” to just mean many drones used at once. But this was a true drone swarm, meaning the drones communicated and collaborated in making collective decisions.

The event is just the beginning. Numerous states from [South Africa](#) to [South Korea](#) are developing or acquiring drone swarms intended to operate across land, sea, air, and potentially even [space](#). Drone swarms may operate in multiple domains at once, incorporating different types of weapons payloads and sensors. To manage this complexity, militaries need a basic typology for sorting different types of drones.



A swarm of drones scans the Cassidy Range Complex at Fort Campbell in a scenario conducted November 16 during the final field experiment for DARPA’s OFFensive Swarm Enabled Tactics, or OFFSET, program. (Credit: Jerry Woller, US Army / Fort Campbell Public Affairs Office)

The most intuitive—and useful—such typology would categorize drones within a drone swarm based on the role they play within the swarm. These categories would not necessarily be discrete, because a single drone could play multiple roles in theory. Likewise, drone swarms may have different combinations of drone types based on the mission. A swarm of undersea drones meant to create a distributed sensor network for submarine searches will look very different than an aerial swarm to suppress enemy air defenses. Ideally, a drone swarm should also be [flexible](#) to allow mission commanders to adjust the swarm composition based on mission parameters, perhaps incorporating different types of attack or sensor drones. With those facts in mind, a set of five categories takes shape: attack, sensor, communication, decoy, and mothership drones.

Attack (and other Effects)

Attack drones carry weapons payloads to strike enemy targets. This can be any sort of weapons payload from guns and bombs to missiles, electronic attack, and chemical weapons. Drones may also have other types of effects, such as chemical weapons disinfectants or mine countermeasures. The type of payload will, of course, be limited by the carry-weight of the drone. A tiny quadcopter is not carrying a Hellfire missile. But a [large unmanned surface vessel](#) might carry a Tomahawk missile.

Different types of attack drones may be used for combined arms tactics. They could also mix conventional weapons with other effects—for states flouting legal bans, this could even mean [chemical weapons](#)—within a swarm to create dilemmas for defenders: Do they don protective gear or dodge the hail of bullets? Of course, such a drone swarm would violate the Chemical Weapons Convention; however, the United States and others may face it on the battlefield. Likewise, multiple payloads create options for responding to different types of defenders and targets. One drone may carry an [antitank missile](#), while others carry bombs or guns.





The American Mojave (top) drone can carry 16 Hellfire ATGMs, which is close to the Apache level, but the Gray Eagle (bottom) drone can also have 20 attack opportunities.



Sensor

Sensor drones capture information about the environment. That information can be used for the swarm to identify targets and to avoid defenders and hazards. Information collected may be shared with the broader swarm to help guide movement, carry out strikes, or make simple decisions on swarm behavior. Typical sensors include electro-optical, infrared, and LIDAR (light detection and ranging). Specialized sensors for chemical, biological, or radiological material may be incorporated as well. Sensors may be on the drone itself, or the drone may distribute the sensors throughout a real or potential battlefield.

Sensor drones enable a particularly useful behavior of drone swarms: the ability to create dispersed sensor networks. Drones with different sensor types can spread broadly over an area to collect intelligence, identify targets, or watch for incoming attacks. When a drone identifies an object of interest, it can share that with the broader swarm, perhaps drawing in more sensor drones to search the area for similar objects or confirmation. That is especially useful for identifying mobile targets that are often more difficult to find and fix.

Sensor drones may be integrated with other drone types. For example, [Russia](#) claims to be testing a swarm with integrated aerial sensor and ground attack drones in which the aerial drones feed information to the ground drones to guide its fires. Likewise, sensor drones may recognize the presence of a defender system and share that information with decoy drones to confound and disrupt that system.

Communication

Electronic warfare is a crucial vulnerability for drone swarms. The key characteristic of a drone swarm is communication between the drones. So disrupting or manipulating that



communication is an obvious way to disrupt or manipulate the entire drone swarm. Electronic attack could target either the communication between the drones or the signals from any ground control station and the drones. This approach is quite common for drones generally, as a [strong majority](#) of counterdrone systems are some form of signal jammer.

Communication drones help ensure the drone swarm maintains its integrity. The drones may serve as relay nodes for communications from external sources, provide an alternative route for interswarm communication, serve as a signal boost in the event of adversary jamming, or provide emergency retreat orders on unjammed frequencies. The design and behavior of such a drone also would need to accommodate the role. As primarily a support or backup function, the communication drone would need to avoid being caught in enemy fire. Likely, it would also need to devote more power output to ensuring any broadcasted signal stays strong.

Decoy

Decoys do not do all that much. Mostly they get in the way. But that can be useful. [Mass](#) is one major advantage of drone swarms. More and more drones can be thrown at a target until it is overwhelmed and destroyed. The swarm may lose a few drones in the process, but if enough get through, there can still be victory at relatively low cost. Decoy drones increase that mass at low cost, because they do not require any integrated weapons, sensors, or other payloads. They are mostly there to absorb defender fires and protect the more valuable drones.

Of course, decoys can be made more sophisticated. They may be designed to give off signatures to trick defenders into believing they are actually manned aircraft. For example, during the [1973 October War](#), Israel used drones to trick Egyptian air defenses into turning on their radar and firing against the wrong targets. This wasted Egyptian ammunition, but more significantly it helped Israel identify the location of the defenses. Israel did the same during the [1983 conflict](#) with Syria over the Bekaa valley. Alternatively, decoy drones may be used to convince defenders that the bulk of the swarm is in another location, which would complicate response to an already [omnidirectional attack](#).

Motherships

[Mothership drones](#) contain other drones. In some cases—what has been evocatively described as a “[turducken of lethality](#)”—one mothership drone contains another mothership drone. Mothership drones help transport the drone swarm to and from the battlefield, and may also provide support for recharging, rearming, or general maintenance. Because mothership drones must necessarily be significantly larger than all the drones they contain (and consequently, require significantly more power), motherships drones may also support broader swarm communication and integration. Of course, mothership drones also create vulnerabilities, because they can be targeted to destroy the whole swarm in a single strike.

Implications

When it comes to drone swarms, complexity is the name of the game. A drone swarm may contain all sorts of drones of different shapes, sizes, and roles. Preparing to use and defend against a drone swarm requires simplifying that complexity to figure out what really works and what does not. That’s where a properly defined typology proves its worth.

Militaries should experiment with different combinations of drones. What combination of attack, sensor, communication, decoy, and mothership drones are most effective in various circumstances? That should include not only ratios of the different types of drone, but the combinations within specific classes. For example, should a counterswarm swarm include more electronic or kinetic attack drones? The answer will also likely vary based on the domain(s) of use and the other types of deployed weapon systems and platforms. Figuring that out may require modeling and simulation, exercises, and wargaming using both real and synthetic environments.

Battlefield commanders should also consider how drone swarm characteristics mesh up with operational details. A commander may flex the number and type of drones based on collected intelligence about likely threats. The commander may want to add more communication drones to prepare for possible electronic attack, or add specific types of attack drones designed to target, say, tanks or infantry formations.

The era of the drone swarm has just begun. Israel’s use of a drone swarm in combat earlier this year might have been the first such instance, but it will not be the last. That means that militaries need to make a concentrated effort to think carefully about how to design and build optimal drone swarms to achieve mission objectives.

Zachary Kallenborn is a policy fellow at the Schar School of Policy and Government, a research affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism, an officially proclaimed US Army “Mad Scientist,” and national security consultant. His research on autonomous weapons, drone swarms,





and weapons of mass destruction has been published in a wide range of peer-reviewed, wonky, and popular outlets, including the Brookings Institution, Foreign Policy, Slate, War on the Rocks, and the Nonproliferation Review. Journalists have written about and shared that research in the New York Times, NPR, Forbes, the New Scientist, and Newsweek, among dozens of others.

MIT Professor Warns That Cartels Could Use “Slaughterbots” to Evade Justice

Source: <https://futurism.com/mit-professor-warns-cartels-could-use-slaughterbots>



Image by Getty Images

Dec 13 – Cheap, lightweight killer robots are just around the corner — and major military powers, including the US, are doing very little to stop them.

In [an interview with TheNextWeb](#), MIT artificial intelligence and weapons researcher Max Tegmark warned that the kind of “slaughterbots” that militaries are already working hard on may soon be in the hands of civilians as well.

“They’ll be small, cheap and light like smartphones, and incredibly versatile and powerful,” he told the site. “It’s clearly not in the national security interest of these countries to legalize super-powerful weapons of mass destruction.”

The greater context is even more chilling. The US, Russia, and China have all signaled that they are against an outright global ban on these so-called “legal autonomous weapons” (LAWs) ahead of a United Nations debate and resolution vote this week.

An unnamed diplomat [told Reuters](#) that there is “not enough support to launch a treaty at this stage,” though they’re hopeful for some sort of “principles” countries will agree to on a nation-by-nation basis.

While such stopgaps may work for Geneva, researchers and activists like Tegmark and Claire Conboy of the Stop Killer Robots coalition think it’s far from enough, and Conboy told *Reuters* that “the pace of technology is really beginning to outpace the rate of diplomatic talks.”

Tegmark’s Future of Life Institute (FLI) at MIT recently released a film about the dangers of this terrifying technology, and the doomsday-esque near future the institute imagines is as horrific as you’d expect: facial recognition drones, robots being used for robberies, and politically-motivated mass executions.

The FLI co-founder told *TNW* that these slaughterbots would be of particular use to cartels.

“If you can buy slaughterbots for the same price as an AK-47,” he said, “that’s much preferable for drug cartels, because you’re not going to get caught anymore when you kill someone.”



“Even if a judge has lots of bodyguards, you can fly in through a bedroom window while they’re sleeping and kill them,” he continued. “And it’s going to go far beyond that. Because pretty soon anyone who wants to knock off anyone for any reason will be able to do this.”

Naturally, this technology already exists and has already been used on battlefields.

Indeed, [NPR reported](#) earlier this year that autonomous drones — that is, killer drones that do not have human operators — were used in a skirmish between dueling Libyan military factions in March 2020, though researchers noted that it doesn’t appear as if anyone was killed by the drones. Israel also [reportedly used](#) an AI-assisted robotic sniper rifle to assassinate an Iranian nuclear scientist last year.

The US, notably, is going through the motions of [asking Congress for permission to build autonomous weapons](#), though it seems like just a matter of time before they get Terminators on their wish list. That fact, paired with signals that the American UN delegation is going to debate and ultimately vote against a treaty against LAWS, is especially telling.

While it’s obviously terrifying to consider a not-so-distant future in which any civilian can buy and program a drone to kill someone else, we can’t forget that human-operated drones already exist and have already killed scores of people in the hands of militaries, with [the US being chief among them](#).

With the [automation craze](#) sweeping every industry from [agriculture](#) to [weapons manufacturing](#), it was only a matter of time before someone decided to take the human element out of drone-striking. Making “slaughterbots” available to the public, as such, is the logical endpoint.

A UN conference this week can alleviate the fears. In [a Geneva meeting](#) that starts today, delegates will debate banning weapons that target people without “meaningful human control.”

Activists, however, are pessimistic about the outcome. While [some countries](#) have endorsed new laws, the world’s leading military powers don’t appear enthusiastic.

The US, for instance, has rebuffed calls to regulate lethal autonomous weapons (LAWS). Instead, American officials [have proposed](#) developing “a non-binding code of conduct.” This may outline some principles of use, but there would be no legal obligations to abide by them.

China and Russia have also shown little appetite for a global treaty. As the UN meeting requires a unanimous agreement on any new rules, the prospects of meaningful restrictions look bleak.

Ultimately, the opposition to new rules may prove self-destructive.

The Impact of Drone Warfare on World Order

By Kathy Hovis

Source: <https://www.homelandsecuritynewswire.com/dr20211216-the-impact-of-drone-warfare-on-world-order>

Dec 16 – An upcoming book by a Cornell doctoral student explores a new field of study related to the use of Unmanned Aerial Vehicles, typically referred to as drones, in warfare.

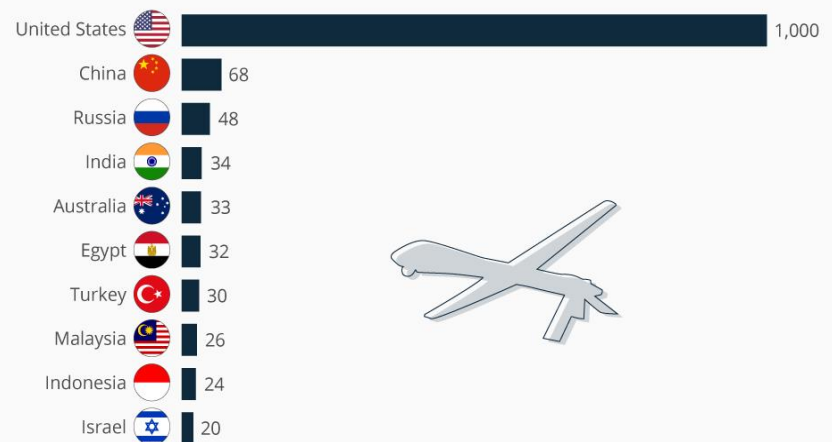
[Drones and Global Order: Implications of Remote Warfare for International Society](#) (Routledge, 2021) edited by Paul Lushenko, Srinjoy Bose and William Maley, will be released 29 December.

Much of the current literature on armed drones focuses on their proliferation across countries, effectiveness against terrorists, and the legal, moral, and ethical impacts of their use, said Lushenko, a U.S. Army Lieutenant Colonel and doctoral student in International Relations. His work “fills the gap by contributing to a ‘fourth wave’ of literature concerned with the trade-offs imposed by drone warfare for global order.”

The book includes chapters by 15 authors, including both academic and military experts, covering issues ranging from the impacts of armed drones on sovereignty to the implications for international law.

The Countries Set To Dominate Drone Warfare

Total forecast purchases of weaponized military drones up to 2028



CC BY ND
@StatistaCharts

Source: Jane's Markets Forecast via The Guardian

statista



“There’s a pattern of relations that govern how states interact with each other and we don’t yet understand the implications of drone warfare on those interactions,” he said. “Drones also have implications for international law and for humanitarian intervention. While the implications are broadly negative, in some cases they can be helpful.” Lushenko is at Cornell as part of the U.S. Army’s Advanced Strategic Planning and Policy Program, which prepares officers for service as strategic planners and leaders through a combination of practical experience, professional military education and a university doctorate. “This program allows officers to reconcile a passion for critical thinking with a desire to lead men and women operationally,” he said. Along with this book, Lushenko’s work was recently featured on a [West Point podcast](#) and he’s written several articles on the topic, including [this recent Washington Post piece](#) with co-author Sarah Kreps, the John L. Wetherill Professor of government and an expert on drone warfare. “I’m an analytical person, so I’ve always been interested in deeply understanding issues, coming up with hypotheses and testing them,” he said. “At key gates in my career, I’ve attempted to bridge my operational experiences and expertise with an academic appreciation and study of emerging trends in warfare.”

Kathy Hovis is a writer for Cornell’s College of Arts and Sciences.

Turkey is Testing a New Laser Drone

Source: <https://i-hls.com/archives/112168>



Dec 16 – A new laser-equipped drone was tested by the Turkish military. The bomb disposal drone is capable of penetrating a carbon steel plate using a high-powered laser beam. According to the state-run Anadolu Agency, the **“Eren” drone** fired a laser from 100 to 500 meters (328 to 1,640 feet) away, burning a hole in three millimeters of steel in 90 seconds. Developed by Asisguard and Tubitak, the laser-equipped drone is designed to destroy explosive devices and has a maximum flight altitude of 3,000 meters (9,842 feet). The drone will be transferred to the Turkish armed forces after completing testing.

New policing system will send drones to the source of gunshots

Source: <https://newatlas.com/drones/shotspotter-airobotics-drones-gunshots/>

Dec 21 – If you hear gunshots in an urban setting, it’s important to get the police to their source as quickly as possible. A new system is being developed to help, by combining autonomous drones with an existing shot-locating technology.

Already in use in over 120 cities in the US, South Africa and the Caribbean, the American ShotSpotter system utilizes a network of microphones within a neighborhood to detect “loud, impulsive sounds.”

Whenever such a sound is detected, its geographical originating point can be triangulated by analyzing the millisecond differences in the times at which it was picked up by the different microphones – the closer a mic was to the gun, the earlier it will have detected the sound of that gun firing. That said, a combination of AI software and human staff (at a control center) is used to determine if the sound *is* indeed gunfire.

In the existing version of the system, police are quickly dispatched to the location. If they’re using ground transportation, however, it may take a while for them to get there. And even *if*





the police department has a helicopter, performing pre-flight checks, etc will still take some time – assuming the aircraft isn't already in the air on patrol, that is.



[An Airobotics drone approaches its docking station \(Airobotics\)](#)

With these potential limitations in mind, Israeli drone manufacturer [Airobotics](#) has teamed up with ShotSpotter to add autonomous drones to the mix. In the new version of the setup, police will still be dispatched, but so will the closest system-specific drone. That aircraft will be in the air within seconds, immediately flying to the source of the gunshots. By analyzing the live video from its onboard camera, police officers can then gain a better sense of the situation they're heading into.

Each drone will be based out of its own covered docking station, where its batteries will be charged when it's not in flight. A robotic arm will pull out the aircraft's existing battery and replace it with one that's fully charged, so the drone is ready to fly at a moment's notice. Plans call for the service to be utilized in urban areas throughout Israel.



International
CBRNE
INSTITUTE



C²BRNE
DIARY



HOTZONE
SOLUTIONS
GROUP

EMERGENCY RESPONSE





The Dangers of Not Protecting The “3Ps” During Events

By Kole (KC) Campbell

On 5 November 2021, an apparent crowd crush at the Astroworld music festival in Houston, Texas resulted in ten deaths and untold injuries. While the criminal investigation is in its early stages at the time of this article, the music festival undoubtedly represents some failures of safety and security planning and execution. The death count and reported injuries are too high to be the normal cost of holding events. Disturbing videos from the event, in addition to statements from concert goers and first responders, belie assertions that initial observations by subject matter experts are impossible until the completion of the investigation. The events at Astroworld are a reminder of the need to “protect the 3Ps” at concerts and special events, and the fact that these activities must be balanced.



Gathering storm – The industrial infrastructure catastrophe looming over America’s Gulf Coast

By Tristan Baurick

Source: <https://thebulletin.org/2021/12/gathering-storm-the-industrial-infrastructure-catastrophe-looming-over-americas-gulf-coast/>



Dec 09 – Jim Blackburn likes to drive out-of-town visitors across the high arch of the Fred Hartman Bridge for the best view of the Houston Ship Channel, a 52-mile-long waterway crowded with the continent’s largest collection of petrochemical plants and oil refineries. Sprawling over what had been low coastal marshland is a jumble of pipelines, smokestacks, storage tanks and cargo ships. For the full impact, the environmental lawyer sometimes brings guests after sunset.

“You come over this bridge at night, and you see all the lights and steam and the flares going off all over the place,” he said as his car crested the span. “One time, I had an Episcopal priest from Seattle with me. She looks down at all this and says, ‘This is what hell looks like.’”

Blackburn let out a sour chuckle. The ship channel’s transformation into a true hellscape, he said, is yet to come. “Throw a real hurricane at this and it’ll be the largest environmental disaster in US history,” he said.

Blackburn, who teaches at Rice University, has been prophesying this calamity for more than a decade. What might have seemed a grim fantasy a few years ago looks increasingly likely with each storm that rakes across the industrial corridors of Texas and Louisiana.

His end-times vision begins with a mild-mannered tropical storm taking shape somewhere in the mid-Atlantic.

As it gathers strength in the warm waters of the Gulf of Mexico, the storm builds into a hurricane hundreds of miles wide with winds topping 130 mph. Instead of striking just east of Houston, as Hurricane Ike did 2008, or veering over to Louisiana, as Laura did last year, this storm plows straight into the heart of Galveston Bay, pushing it into a nearly 30-foot-high



Read.



bulge and dropping it on the bay's heavily developed west side, an area that's home to more than 800,000 people. Thousands may die from the initial burst of wind and water, but the real terror begins when the storm surge squeezes into the Houston Ship Channel. The surge, he said, will break ships off their moorings, cleave oil pipelines, and pummel thousands of storage tanks holding the raw material for everything from paint thinners to jet fuel. This toxic stew of oil, chemicals, and debris will flood urban bayous, spill into neighborhoods, and eventually wash back into the bay.

"This is what hell looks like."

Blackburn's bleak prediction, developed with computer modeling by Rice's Severe Storm Prediction, Education and Evacuation from Disaster (SSPEED) Center, loses doubters with each passing storm.

"The storms and types of weather we're having are more extreme," said MaryJane Mudd, executive director of East Harris County Manufacturers Association, an alliance of chemical producers along the ship channel. "We are having to prepare for things we've never considered before."

Despite the risks, the industry has been slow to adapt. Companies are not building bigger floodwalls, altering facility designs, or shifting development inland. Federal and state governments are doing little to push industries. Regulations remain frozen as the climate warms, increasing the likelihood of stronger and more frequent storms.

Industry leaders and regulators are instead banking on a nearly \$30 billion storm protection project known as the Ike Dike. Named for the hurricane, the vast system of walls, gates, and levees would make Galveston Bay a veritable fortress that could be sealed up when hurricanes threaten.

It's ambitious and expensive, but Blackburn says it will be too little, too late. Likely to take the better part of two decades to build, the Ike Dike won't hold up to the worst hurricanes. "Look, it needs to be built," he said. "But it needs to be built for the bigger storms to come. It will be way outdated once it's constructed."

►► [Read the full article at the source's URL.](#)

Tristan Baurick is an environment reporter with The Times-Picayune / New Orleans Advocate. His work has appeared in ProPublica, The New York Times and Aububon magazine.



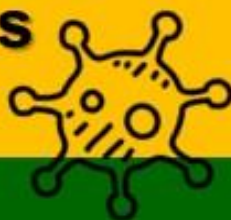
- Detection
- Monitoring
- Sampling & Analysis
- Protection
- Decontamination
- Destruction & Waste Management
- Scene Management Training
- Instructional Equipment
- Live Agent Testing & Validation



HOTZONE
SOLUTIONS
GROUP



**The world's most practice oriented
provider of Hazardous Substances
Management Solutions**



hotzonesolutions.org/