From *The Economist*, September 5, 2015

Monitoring nuclear weapons

The nuke detectives

Clandestine weapons: New ways to detect covert nuclear weapons are being developed, which could help inspectors monitor Iran’s nuclear deal

Sep 5th 2015 | From the print edition

AS NUCLEAR blasts go, North Korea’s first test in 2006 was small. The detonation of an underground device produced an explosive force well below one kiloton (less than a tenth of the size of the bomb dropped on Hiroshima in 1945). Even so, the vibrations it caused were recorded half a world away in the centre of Africa. Advances in the sensitivity of seismic sensors and monitoring software are now good enough to distinguish between a distant nuclear detonation and, say, a building being demolished with conventional explosives, says Lassina Zerbo, head of the Preparatory Commission for the Comprehensive Test-Ban-Treaty Organisation (CTBTO), the international organisation that seeks to enforce the agreement ratified, so far, by 163 nations.

The CTBTO operates 170 seismic stations worldwide, 11 underwater hydroacoustic centres detecting sound waves in the oceans, 60 listening stations for atmospheric infrasound (low-frequency acoustic waves that can travel long distances) and 96 labs and radionuclide-sampling facilities. More sensors are being installed. Crucially, however, the optimal number for global coverage was recently reached. It is now impossible, reckons Dr Zerbo, to test even a small nuclear weapon in secret anywhere on Earth. And on top of that, the United States Air Force runs a detection network that includes satellites that can spot nuclear-weapons tests.

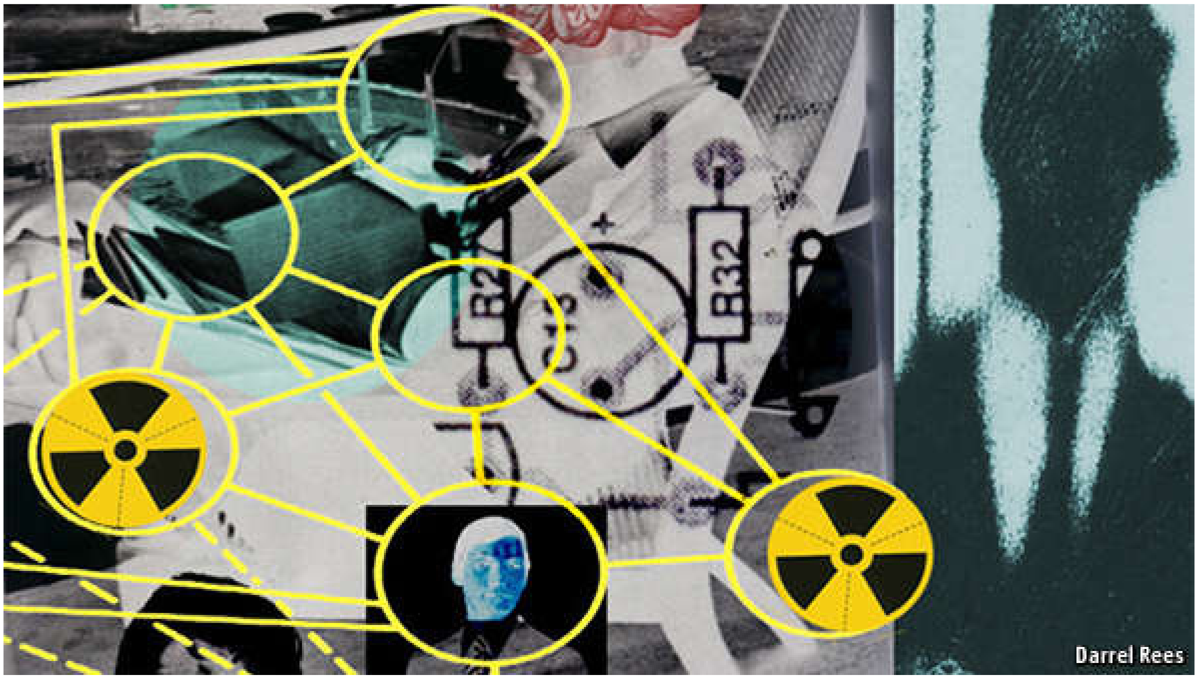
It is better, though, to discover a secret weapons programme before testing. Once a country has a nuclear bomb or two, there is not much other governments can do to stop it from making more, says Ilan Goldenberg, a former head of the Iran team at the Pentagon. Plenty of states want such capabilities. The Defence Science Board, an advisory body to the Pentagon, concluded in a report last year that the number of countries that might seek nuclear weapons is higher now than at any time since the cold war. Those states include Saudi Arabia and other Sunni-Arab rivals of Iran, which in July, after long and tortuous negotiations, signed a nuclear deal with America and other nations to restrict its nuclear activities, and to allow enhanced monitoring and inspection of its facilities.

Some wonder how effective such monitoring measures will be—and that is with the benefit of agreed access to Iran's facilities. The West's record on detecting more covert nuclear work is spotty. A large North Korean centrifuge facility for uranium enrichment remained hidden until the regime gave a Stanford University professor a tour in 2010, letting the cat out of the bag. This troubles many. Enrichment is the biggest, trickiest step in bombmaking, so it should create the most evidence. By contrast, a roomful of scientists running mathematics software on offline computers to calculate the best way to detonate enriched uranium can keep a low profile, says Mr Goldenberg. It doesn't help, he adds, that A.Q. Kahn, a metallurgist who made Pakistan's nuclear weapons, circulated his designs.

The latest kit

As the technologies to unearth work on clandestine nuclear weapons become more diverse and more powerful, however, the odds of being detected are improving. Innovation is benefiting detection capabilities, says Ramesh Thakur, a former UN assistant secretary-general. The products under development range from spy software that sifts through electronic communications and financial transactions to new scanners that can detect even heavily shielded nuclear material.

Start with intelligence-gathering. Western spooks were mostly clueless about the network Mr Kahn built to traffic bomb expertise and equipment, until Libya, a Kahn client, surrendered its programme in 2003. No one using the same approach today would get very far, reckons Mr Thakur, now head of the Centre for Nuclear Non-Proliferation & Disarmament at the Australian National University in Canberra. This, he says, is thanks to advances in "network analysis" software.



Darrel Rees

After the September 11th terrorist attacks in 2001 America poured money into developing software for counter-terrorism. When fed with information, such as people's e-mails, schooling, web surfing, phone calls, banking transactions and purchases, the programs try to work out who might be a terrorist. A person could pop up on an intelligence agency's computer screen if, say, he downloads podcasts of a radical Sunni cleric, visits the city where that cleric preaches, and then takes calls from a town held by Islamic State. Now America is making a big effort to adapt this software to sniff out nuclear shenanigans too, says William Tobey, a former head of counter-proliferation strategy on the White House's National Security Council.

Software used for this type of analysis include i2 Analyst's Notebook from IBM, Palantir from a Californian firm of the same name, and ORA, which was developed with Pentagon funds at Carnegie Mellon University in Pennsylvania. ORA has crunched data on more than 30,000 nuclear experts' work and institutional affiliations, research collaborations and academic publications, says Kathleen Carley, who leads the ORA work at Carnegie Mellon. Changes, such as a halt in publishing, can tell stories: scientists recruited into a weapons programme typically cannot publish freely. Greater insights appear when classified or publicly unavailable information is sifted too. Credit-card transactions can reveal that, say, a disproportionate number of doctors specialising in radiation poisoning are moving to the same area.

Who's who in the zoo

The software uses combinatorial mathematics, the analysis of combinations of discrete items, to score individuals on criteria including "centrality" (a person's importance), "between-ness" (their access to others), and "degree" (the number of people they interact with). Network members with high between-ness and low degree tend to be central figures: they have access to lots of people, but like many senior figures may not interact with that many. Their removal messes things up for everybody. Five or more Iranian nuclear scientists assassinated in recent years—by Israel's Mossad, some suspect—were no doubt chosen with help from such software, says Thomas Reed, a former secretary of the United States Air Force and co-author of "The Nuclear Express", a history of proliferation.

Importantly, the software can also evaluate objects that might play a role in a nuclear programme. This is easier than it sounds, says a former analyst (who asked not to be named) at the Pentagon's Central Command in Tampa, Florida. Ingredients for homemade conventional bombs and even biological weapons are available from many sources, but building nukes requires rare kit. The software can reveal a manageable number of "chokepoints" to monitor closely, he says. These include links, for instance, between the few firms that produce special ceramic composites for centrifuges and the handful of companies that process the material.

A number of countries, including Japan and Russia, use network analysis. Japan's intelligence apparatus does so with help from the Ministry of Economy, Trade and Industry, which assists in deciding which "dual use" items that might have both peaceful and military purposes should not be exported. Such work is tricky, says a member of the advisory board (who also asked not to be named) to the security council of the Russian Federation, a body chaired by Vladimir Putin. Individual items might seem innocent enough, he says, and things can be mislabelled.

Data sources are diverse, so the work takes time. Intelligence often coalesces after a ship has left port, so foreign authorities are sometimes asked to board and search, says Rose Gottemoeller, undersecretary for arms control at America's State Department. The speed of analysis is increasing, however. Software that converts phone conversations into computer-readable text has been "extremely helpful", says John Carlson, a former head of the Australian foreign ministry's Safeguards and Non-Proliferation Office.

The known unknowns

Network analysis has limitations. Adapting terrorist-identifying software to pick out people in a covert nuclear programme is hard. Proliferators are outnumbered by terrorists, so there is less nuke-specific data to calibrate the software. Beyond this, computers struggle to calculate the astronomical number of potential links in a network. The problem is made worse as analysts realise that new types of data, such as details of metal or chemical imports, prove useful.

North Korea helped to keep its centrifuge facility secret by using mostly black-market or domestically manufactured components

Would-be nuclear states can also reduce their networks. North Korea helped to keep its centrifuge facility secret by using mostly black-market or domestically manufactured components. Iran is also indigenising its nuclear programme, which undermines what network analysis can reveal, says Alexander Montgomery, a political scientist at Reed College in Portland, Oregon. Iran mines uranium domestically and has produced centrifuge rotors with carbon fibre, instead of importing special maraging steel which is usually required.

A big computer system to make sense of all this would help, says Miriam John, vice-chairman of the Pentagon's Threat Reduction Advisory Committee. Which is why the Pentagon is building one, called Constellation. Dr John describes it as a "fusion engine" that merges all sorts of data. For instance, computers can comb through years of satellite photos and infra-red readings of buildings to detect changes that might reveal nuclear facilities. Constellation aims to increase the value of such nuggets of information by joining them with myriad other findings. For example, the whereabouts of nuclear engineers who have stopped teaching before retirement age become more interesting if those people now happen to live within commuting distance of a suspect building.

Yet photographs and temperature readings taken from satellites, even in low Earth orbit, only reveal so much. With help from North Korea, Syria disguised construction of a nuclear reactor by assembling it inside a building in which the floor had been lowered. From the outside the roof line appeared to be too low to house such a facility. To sidestep the need for a cooling tower, water pipes ran underground to a reservoir near a river. The concealment was so good the site was discovered not with remote sensing but only thanks to human intelligence, says Dr Tobey, the former National Security Council official. (Israel bombed the building in 2007 before it could be completed.)

Some chemical emissions, such as traces of hydrofluoric acid and fluorine, can escape from even well-built enrichment facilities and, with certain sensors, have been detectable from space for about a decade, says Mr Carlson, the Australian expert. But detecting signs of enrichment via radiation emissions requires using different sorts of devices and getting much closer to suspected sources.

The "beauty" of neutrons and alpha, beta and gamma radiation, is that the energy levels involved also reveal if the source is fit for a weapon, says Kai Vetter, a physicist at the University of California, Berkeley. But air absorbs enough radiation from uranium and plutonium bomb fuel to render today's detectors mostly useless unless they are placed just a few dozen metres away. (Radiological material for a "dirty bomb" made with conventional explosives is detectable much farther away.) Lead shielding makes detection even harder. Not one of the more than 20 confirmed cases of trafficking in bomb-usable uranium or plutonium has been discovered by a detector's alarm, says Elena Sokova, head of the Vienna Centre for Disarmament and Non-Proliferation, a think-tank.

Ground-based detectors are becoming more sensitive. Some new machines can discover a stash only a fifth of the mass required five years ago at a similar distance, Dr Vetter notes. Better algorithms help identify and disregard naturally occurring background radiation. Detectors are becoming more useful, too, thanks to simpler interfaces, including applications that now run on iPads, says Ann Harrington at the Department of Energy's National Nuclear Security Administration (NNSA) in America. Many field workers would not have been qualified to interpret the readouts from previous equipment.

Range rovers

Such improvements have yet to translate into much greater range, however. Detectors still need to be close to whatever it is they are monitoring, which mostly restricts their use to transport nodes, such as ports and borders. The range the detectors operate over might stretch to about 100 metres in a decade or so, but this depends on uncertain advances in "active interrogation"—the bombardment of an object with high-energy neutrons or protons to produce other particles which are easier to pick up. One problem is that such detectors might harm stowaways hiding in cargo.

That risk has now been solved, claims Decision Sciences, a Californian company spun out of the Los Alamos National Laboratory in America. It uses 16,000 aluminium tubes containing a secret gas to record the trajectory of muons. These are charged particles created naturally in the atmosphere and which pass harmlessly through people and anything else in their path. However, materials deflect their path in different ways. By measuring their change in trajectory, a computer can identify, in just 90 seconds, plutonium and uranium as well as "drugs, tobacco, explosives, alcohol, people, fill in the blank", says Jay Cohen, the company's chief operating officer and a former chief of research for the United States Navy. The ability to unearth common contraband will make the machine's $5m price tag more palatable for border officials. A prototype is being tested in Freeport, Bahamas.

Other groups are also working on muon detectors, some using technology developed for particle physics experiments at the Large Hadron Collider in Switzerland. Another approach involves detecting neutrinos, which are produced by the sun and nuclear reactors, and seeing how they interact with other forms of matter. The

NNSA and other organisations are backing the construction of a prototype device called WATCHMAN in an old salt mine (to shield it from cosmic rays and other interference) in Painesville, Ohio. It will be used to detect neutrinos from limited plutonium production at a nuclear power station 13km away. Such a system might have a 1,000km range, eventually. But even that means it would require a friendly neighbour to house such a facility on the borders of a country being monitored.

Once nuclear facilities have been discovered, declared or made available for inspection as part of a deal, like that signed with Iran, the job of checking what is going on falls to experts from the UN's International Atomic Energy Agency (IAEA). The equipment available to them is improving, too. The Canadian Nuclear Safety Commission has built a prototype hand-held spectrometer for determining if traces of uranium collected on a cotton swab and blasted with a laser emit a spectral signature that reveals enrichment beyond that allowed for generating electricity. Within three years it will provide an unprecedented ability to assess enrichment without shipping samples back to a lab, says Raoul Awad, director-general of security and safeguards at the commission.

Laser scanning can also reveal other signs of enrichment. A decade ago inspectors began scanning intricate centrifuge piping with surveying lasers. A change between visits can reveal any reconfiguration of the sort necessary for the higher levels of enrichment needed for bombmaking. Secret underground facilities might also be found by wheeling around new versions of ground-penetrating radar.

The remote monitoring of sites made available to inspectors is also getting better. Cameras used to record on videotape, which was prone to breaking—sometimes after less than three months' use, says Julian Whichello, a former head of the IAEA's surveillance unit. Today's digital cameras last longer and they can be programmed to take additional pictures if any movement is detected or certain equipment is touched. Images are encrypted and stamped with sequential codes. If technicians at a monitored facility delete any pictures, the trickery will be noticed by software and the inspectors informed.

Such technology, however, only goes so far. The IAEA cannot inspect computers and countries can veto the use of some equipment. It does seem that inspectors sent to Iran will get access to Parchin, a site near Tehran where intelligence agencies say tests related to nuclear-weapons making took place. (Iran denies it has a military programme.) But even the best tech wizardry can only reveal so much when buildings have been demolished and earth moved, as in Parchin.

The big question

Could nuclear weapons be built in secret today? Riaz Mohammad Khan, a former foreign secretary of Pakistan, says not. A senior American State Department counter-proliferation official (whose asked to remain anonymous), however, says that it is not impossible. Others agree. Australia's Mr Carlson suggests one danger is that spies can end up hunting for the wrong clues. Iraq's use of a process called electromagnetic isotope separation, to enrich uranium for bombs before the 1991 Gulf war, remained undetected for years. That is because, says Mr Carlson, analysts were not looking for signs of an inefficient 1940s process that was so low-tech it did not require any telltale imports.

And processes are changing. Companies, including a General Electric consortium, are making progress enriching uranium with lasers (see article). If this becomes practical, some worry that it might be possible to make the fuel for a nuclear bomb in smaller facilities with less fancy kit than centrifuges. It is telling that the authors of the Defence Science Board report—which warned that the number of states which might seek nuclear weapons is higher than since the end of the cold war—were less optimistic upon finishing their research last year than when they began in 2010, says Dr John, its co-chair. That is also the year Iran boasted about advances in enriching uranium with lasers. If the new deal with Iran is to work, and other would-be bombmakers are to be spotted, then the technology available to the world's nuke detectives needs to keep improving, too.