WELLMAN
BOOTH
SAFE WORKING LOAD 4 TONNES
TRAVELLING BEAM ELECTRIC HOIST
SAFE WORKING LOAD 2 TONNES

A FATAL ERROR HAS OCCURRED

Attacks by computer hackers on the IT (Information Technology) systems of government and commercial organisations have become commonplace, and cybercrime is arguably the fastest growing new crime of the 21st century.

Andy Oppenheimer

Among the most dangerous prospects is a cyberattack on a Nuclear Power Plant (NPP) or nuclear reprocessing plant such as the Sellafield complex in north-west England, due to the possible release of radiation from reactors or spent fuel ponds. According to the director general of the International Atomic Energy Agency (IAEA) Yukiya Amano, in August 2015 "reports of actual or attempted cyber-attacks are now virtually a daily occurrence."

In March and April, further warnings resounded about the possibility of an at-

Sellafield Ltd

This is the first-generation Magnox storage pond at Sellafield reprocessing plant in north-west England. Steps must be taken to ensure such facilities are not vulnerable to cyber attack.

ISIS THREAT

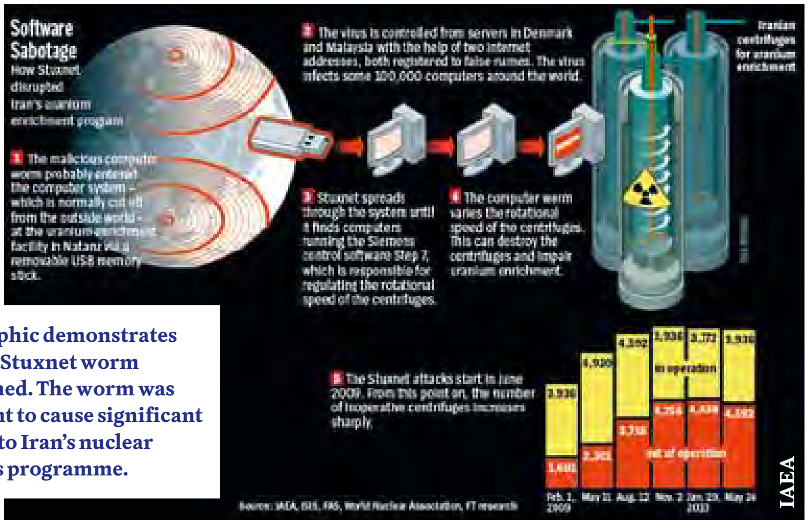
These dangers have resurfaced since the rise of the Islamic State of Iraq and Syria (ISIS), and their occupation of large parts of both these countries, following multiple reports of the use of chemical weapons (CW) on Kurdish and Iraqi forces in Iraq, and focusing on their further potential to launch other CBRN (Chemical, Biological, Radiological, Nuclear) weapons. It is widely feared the most deadly (and well-financed) violent political organisation of recent times is acquiring radioactive materials from which they could construct and emplace Radiological Dispersal Devices (RDDs). In March, ISIS operatives are reported to have seized around 40 kilograms/kgs (90 pounds/lbs) of Low Enriched Uranium (LEU) from Mosul University in northern Iraq. While LEU has limited toxicity, if dispersed by a homemade bomb it would necessitate a specialist CBRN response and clean-up of contaminated areas, buildings and citizens. In October 2015, the FBI (US Federal Bureau of Investigation) working with police in Moldova disrupted a deal hatched in February to supply ISIS with enough caesium to contaminate an urban centre.

Beyond RDDs, however, a physical or cyberattack on an NPP and particularly on a spent fuel pond, which contains the most radioactive materials on earth, could trigger an environmental disaster on this level. A cyberattack on NPP systems and back-ups powering reactor cooling systems could trigger a meltdown incident similar to the disaster witnessed at the Fukushima Nuclear Power Plant, following the earthquake on the east coast of Japan in 2011. With the dawn of digital communications and globalized commerce all countries became inexorably linked and hence, infinitely more vulnerable to cyber infrastructure attack.

NATION-STATE ATTACKS

Cyberattacks are launched by nation-states on a regular basis. In March 2015 the Republic of Korea (RoK) government accused the Democratic People's Republic of Korea (DPRK) of carrying out a cyberattack in December 2014 on the nation's main energy supplier, Korea Hydro and Nuclear Power (KHNP). DPRK hackers reportedly leaked internal documents from KHNP five times by using Internet Protocol addresses in Shenyang, the People's Republic of China (PRC) to access the KHNP network. They published designs, manuals, and other information about RoK reactors on Twitter, along with personal information about workers.

In this case the hackers were trying to paralyse the RoK's NPP system, but other attacks could go a step further and trigger tack on the world's nuclear power facilities. In the UK, the Office for Nuclear Regulation, the official organization regulating the country's nuclear industry, pointed to the growing threat of attack on Britain's 15 operational reactors, which account for nearly a fifth of the country's electricity. Its 2016-20 strategic plan states: "The capabilities of potential adversaries to operate in cyberspace will continue to grow" and warned against "failure to protect the confidentiality, integrity and availability of sensitive information and assets from both known and emerging security threats to the UK nuclear infrastructure."


Software Sabotage
How Stuxnet disrupted Iran's uranium enrichment program
1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.
2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.
3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.
4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.
Iranian centrifuges for uranium enrichment
5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.
3,936
1,601
4,920
2,301
4,592
3,716
3,936
4,756
3,772
4,428
3,936
4,592
in operation
out of operation
Feb. 1, 2009
May 11
Aug. 12
Nov. 2
Jan. 29, 2010
May 24
Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

IAEA

This graphic demonstrates how the Stuxnet worm functioned. The worm was sufficient to cause significant damage to Iran's nuclear weapons programme.

This photo was taken on 15 March 2011 just after the Fukushima Daiichi disaster. It shows the catastrophic damage to the plant.

TEPCO

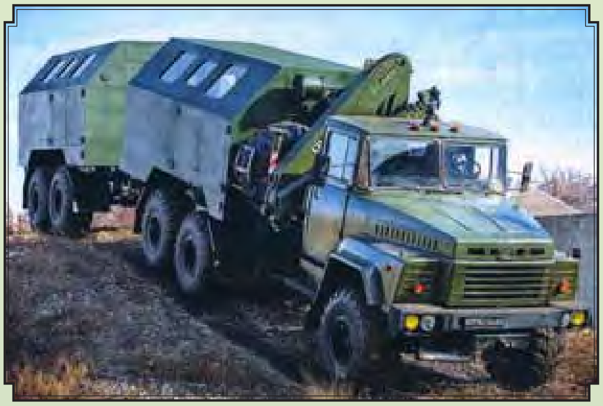
an accident. Of great concern to the RoK was that its national security system and investigation process on cyberattacks was found to be wanting. A far more successful state-launched attack was the Stuxnet worm (a malicious programme inserted into a computer system), which did not set out to blow up a plant or fulfill a similar ISIS-style apocalyptic goal, but managed to set back Iran's nuclear programme in 2009 by instructing 1000 centrifuges at the Natanz Nuclear Facility in the centre of the country to self-destruct. It was only discovered five months later, after a seemingly unrelated incident in Belarus, where a computer security firm was called in to deal with computers in Iran that were crashing and rebooting repeatedly. When they found malicious files on one of the systems, the world's first digital weapon was uncovered, and is known to have spread elsewhere. Stuxnet caused damage by wreaking physical destruction on equipment controlled by computers, in Iran's case the centrifuges, rather than simply hijacking computers or stealing data from them.

In February, a report in *The New York Times* outlined a plan to attack Iran's nuclear facilities with further destructive cyber attacks had the diplomatic effort to limit its nuclear programme failed and a military conflict ensued. Based on statements made in a documentary featuring military and intelligence officials, the operation, codenamed NITRO ZEUS, was intended to disable Iran's air defences, communications systems and electricity grid. To crash its nuclear effort, the initiative was aimed at disabling the controversial mountain-deep Fordo nuclear enrichment site near Qum, northern Iran.

NO IMMUNITY

In October 2015 a report entitled *Cyber*

UKRSPECEXPORT



TECHNICAL SUPPORT MACHINE MTP-72

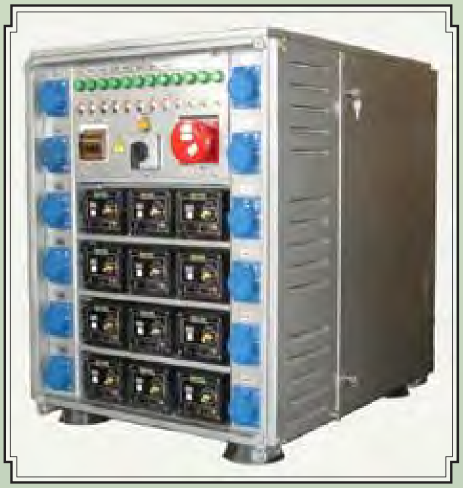
PURPOSE

Technical Support Machine MTP72 is designed for the most labor intensive maintenance and current repairs of tank T-72 in the field.

The structure of the machine includes a trailer with equipment and racks with niches and special boxes for transport and storage of spare parts and consumables for the repair of the tank.

SPECIFICATIONS

Chassis	KrAZ-632207
Trailer type	
Body type	Full metal, welded
Crew	3 (driver - crane operator, locksmith - mechanic, electrician - welder)
Workshop overall dimensions, mm:	
Length	14720
Width	2760
Height	3640
Total weight of a workshop, kg	22750
Maximum speed, km/h	80
Fuel consumption, l/100 km	48
Maximum grade ascending ability, angle degree	25
Fordable depth, m	1,2
Zar-system voltage, V	24, 220, 380



STATIONARY CHARGING STATION SZS-U

PURPOSE

Stationary charging station SZS-U is intended for a charge of acid accumulator batteries, and also alkaline batteries with the rated voltage of 12 and 24 V, with the capacity from 7 to 200 A·h, what is applied in automobile and armored vehicles (personal armored vehicles or tanks)

The station represents the stationary boxing of frame type, it is divided into two compartments.

There is the chargers block in the front compartment, it's consisting of twelve independent charging modules.

There are niches for laying of 12 charging cables sets and 1 powering cables set (220 V and 380 V) in the rear compartment.

Charging modules provide a high long-term charging rate with low fluctuations at the exit, they are interfering to premature wear of accumulator battery's plates, and also are capable to determine the rated voltage of the charged battery automatically.

SPECIFICATIONS

Type	Stationary, power supply from external network
Output voltage, V	12, 24
Station voltage, V	220, 380
Number of at the same time charged accumula- tor batteries	12
Time necessary for station expansion, no more, min.	5
Outline dimensions, mm	
length	1000
width	800
height	1000
Weight, kg:	100

The storage pond at the Thermal Oxide Reprocessing Plant, or 'THORP' at Sellafield contains some of the most radioactive materials on Earth.

Sellafield Ltd

Security at Civil Nuclear Facilities: Understanding the Risks, published by the Royal Institute for International Affairs (RIIA) in London based on an 18-month study on cyber defences in NPPs, stated that UK's plants and associated infrastructure "were not well protected or prepared because the industry had converted to digital systems relatively recently." The researchers interviewed senior nuclear officials in Canada, France, Germany, Japan, the UK, Ukraine and the US and found that risks were compounded by increased digitisation and the industry's growing reliance on commercial software. The report exposed a "pervading myth" in the industry that because computer systems in NPPs were isolated from the Internet at large, they were therefore immune to the level of cyberattacks affecting other industries. At many nuclear plants, engineers and officials thought that because their systems were not connected to the Internet, it would be very hard to compromise them.

The report also found that the 'air gap' between the public Internet and nuclear systems was easy to breach with "nothing more than a flash drive". This occurred with a second Stuxnet attack on Iran's nuclear facilities, when a new version of the malware was unleashed on the Natanz enrichment plant just as its systems had been restored. The malware was designed to manipulate computer systems that control and monitor the speed of the centrifuges by bypassing computers that were 'air-gapped' (unable to be accessed remotely) from the Internet, by infecting them via infected USB (Universal Serial Bus) flash drives.

The RIIA report also found that many plants lacked preparedness for large-scale attacks outside office hours and there were communications difficulties between operational NPP technology engineers and cyber security personnel, many of whom were located off site. Organization directors were not familiar with virtual networks and other links to the public Internet on nuclear infrastructure networks. Search engines that sought out critical infrastructure had indexed these links, making it easy for attackers to find ways into networks and control systems. The report's author, Caroline Baylon, who is a research associate in science, technology and cyber security, at the RIIA, said, "Cyber security is still new to many in the nuclear industry. They are really good at safety and, after (the 11 September attacks in New York and Washington DC) they've got really good at physical security. But they have barely grappled with cyber." According to the RIIA's research director of international security, Dr. Patricia Lewis, "The nuclear industry is beginning, but struggling, to come to grips with this new, insidious threat." She added, "It would be extremely difficult to cause a meltdown at a plant or compromise one... but it would be possible for a state actor to do, certainly. The point is that risk is probability-times-consequence. And even though the probability might be low, the consequence of a cyber incident at a nuclear plant is extremely high."

PAST DISRUPTION

Past instances of accidental disruption include a 48-hour emergency shutdown in March 2008 in the Hatch NPP near Baxley, Georgia, United States after an engineer installed a software update on a computer designed to synchronize data. In a report filed with the Nuclear Regulatory Commission, the updated computer reset the data on the control system when it was rebooted, causing safety systems to incorrectly interpret the lack of data as a drop in the water reservoirs that cool the plant's highly radioactive nuclear fuel rods. As a result, automated safety systems at the plant triggered a shutdown.

Precedent for actual physical attack on a NPP is rare, but a hallmark plot was uncovered in November 2005 to carry out an attack on the Lucas Heights NPP, on the outskirts of Sydney, Australia by a group of Melbourne- and Sydney-based jihadists. The group had stockpiled weapons, including Australian Army rocket launchers, explosives, and other bomb-making materials, and had scoped out other high-profile Australian targets as well as Lucas Heights. Five men were convicted of political violence charges in October 2009.

COUNTERING THREATS

The RoK government made a decision in March 2015 to set up a security control tower inside the National Security Office to deal with cyberattacks from the DPRK. Japan is to hold field exercises to counter cyberattacks on the control system of its nuclear facilities, in combination with physical attacks. The RoK has conducted regular cybersecurity inspections and reviews since 2015, and with the IAEA, hosted a Regional Workshop on Computer Security for Nuclear Facilities.

The IAEA has issued guidance to NPP operators. Earlier this year, the UK and the US announced plans to cooperate on improving the resilience of nuclear infrastructure to attack. Later in 2016 both countries will stage a war game simulation of a cyberattack on a NPP to test the readiness of the government and of utility companies. In the wake of the March ISIS attacks in Brussels the Belgians have established a Cyber Security Centre and expanded the scope of nuclear facility 'stress tests' to include cyberattack. Meanwhile, the UK government has committed funds to improve the security of civil nuclear infrastructure worldwide. In mid-April the UK secretary of state for defence Michael Fallon announced a $56 million endowment to create a new Cyber Security Operations Centre (CSOC) for the Ministry of Defence (MoD). This forms part of an even larger $2.6 billion to be invested in the UK's cybersecurity over the next five years. The funds were called for in the November 2015 Strategic Defence and Security Review (SDSR), which sets out the UK government's strategic and defence procurement priorities and, according to the MoD, will "transform the MoD's operational cybersecurity capabilities."

NIGHTMARE SCENARIO

In late 2014 a confidential report was published with a stark warning: Britain's 16 NPPs are at risk from attack by Unmanned Aerial Vehicles (UAVs), which could result in tens of thousands of casualties. The report, by leading British nuclear expert John Large of consulting engineers Large and Associates, and commissioned by Greenpeace, an environmental non-government organisation, warned that the authorities were "burying their heads in the sand."

The Large report followed several unexplained, but apparently co-ordinated, flights of tiny versions of UAVs over 13 of France's 19 nuclear power plants between early October and late November 2014. In January a UAV was spotted over the Elysée Palace, home to the French President, and in February they were seen flying around five other Paris landmarks. In giving evidence to the French parliament, Mr. Large posited various modes of UAV attack against the defences of a standard NPP, including precisely-targeted home-made bombs or dropping equipment to aid an insider saboteur. The report modelling showed that the "flexible access and manoeuvrability of the (UAVs)" means that they were able to fly over and twist around physical barriers that "belonged to a different age." Even small, battery-powered UAVs can lift at least ten kilograms (22lbs).

Ms. Baylon adds that "because UAVs are so small, conventional radar cannot detect them. There's a huge vulnerability there." She wrote in *Newsweek* in December 2014 that UAVs could also provide air support for an actual ground-based attack, drop explosives to damage power or communications networks, and be used to bomb spent-fuel pools which are less well protected than reactor cores.

In 2014 Britain's 16 operational reactors suffered 37 security breaches, including by at least one small UAV, the highest number since twelve breaches in 2011. The Large report recommended a major exercise to test the resilience of the UK's power stations against acts of political violence. Following the ISIS attacks in Paris which occurred in November 2015, in January France tasked its National Research Agency with investigating ways to improve the detection and interception of small, low-flying UAVs and announced that it plans to share its findings with other European countries.

However, Mr. Large has said regarding the threat of UAV attacks on NPPs the problem is that the UK plants were designed in the 1950s and 1960s and that those designs did not factor in such dangers. "(Political violence can be) an intentional, intelligent event that seeks out the vulnerabilities of the plant ... but an accident, which they are designed to guard against, is an unintelligent event. Nuclear plants are primarily built on an accident basis. But this (admission) does make the regulator more accountable." Mr. Large added that existing NPPs are not designed to counter the threat of "near-cyborg technology... In each of the four... attack scenarios that I examined, the plant fared very badly indeed. If these scenarios had been for real, there would have been the potential for a major radioactive release."

In this age of multiple threats not just from world franchises of jihadists but also from other extremist groups that are hell bent on destruction, no industry or institution can afford not to take whatever precautions are available. To do this many cultures will have to adapt and change.