Cyber Threat to Nuclear Installations

SITAKANTA MISHRA

Critical infrastructures' like power grids, nuclear facilities, satellites, defence networks, governmental informatics have been integrated with computer networks, especially since the 1990s. This has certainly simplified the task of managing important activities remotely and expeditiously. The 'world-wide-web' that denotes the 'cyber space' has further eased all day-to-day activities. However, increasing digitalisation and computerisation has also made everything vulnerable to malicious acts, through the premeditated use of cyber space, termed as 'cyber terrorism.'

Nuclear facilities as sensitive infrastructure have long been feared and proven vulnerable to cyber terrorism. These facilities use both digital and analog computer systems to monitor and operate equipment; and to obtain and store vital information. In addition, many plant computer systems are linked to digital networks that extend across the plant, performing safety, security and emergency functions. The preparedness to protect these critical digital assets and the information they contain from malicious use is called 'cyber security.'

The Stuxnet attack against the Iranian nuclear program, and three other cyber incidents occurred at the US nuclear facilities between 2003 and 2008 – Davis-Besse worm infection, Browns Ferry shutdown, Hatch automatic shutdown (*Strategic Insights*, Spring 2011) – demonstrate the impact that a sophisticated adversary with detailed knowledge of process control systems of a nuclear plant can have on plant operations.

The Stuxnet virus that attacked the industrial control systems at several Iranian nuclear installations between 2009 and 2011 is known to have disrupted Iran's centrifuge program. Stuxnet commanded the programmable logic controllers (PLCs) to speed up and slow down the spinning centrifuges, destroying some of them, while sending false data to plant operators to make it appear the centrifuges were behaving normally. Reportedly, this has destroyed over 1000 centrifuges and pushed Iranian nuclear programme back for several years.

On January 25, 2003, the 'Slammer worm' exploiting vulnerability in Microsoft SQL Server infected 75,000 servers worldwide in ten minutes. It disabled data-entry terminals at 911 call centres in Washington, shutdown 13,000 Bank of America ATMs, and forced Continental Airlines to cancel several flights. The 'Slammer worm' also infected computer systems at the Davis-Besse nuclear power plant in Ohio.

The shutdown of Unit 3 at the Browns Ferry nuclear plant in Alabama on August 19, 2006, demonstrated that critical reactor components, not only computers, could be disrupted and disabled by a cyber attack. Unit 3 was manually shutdown after the failure of both reactor recirculation pumps and the condensate demineraliser controller. Without the recirculation pumps, the power plant could not cool the reactor, making a shutdown necessary to avoid melting the reactor core.

Similarly, on March 7, 2008, Unit-2 of the Hatch nuclear power plant in Georgia got automatically shut down after an engineer applied a software update to a computer on the plant's business network. When the engineer rebooted the computer, the synchronisation programme reset the data on the control network. The control systems interpreted the reset as a sudden drop in the reactor's water reservoirs and initiated an automatic shutdown. This demonstrated that one cyber malfunction may lead to another malfunction that is completely beyond imagination.

The worse fear is the possible reactor core meltdown owing to dis-functioning of safety apparatus affected by a virus. Non-nuclear systems can be completely shutdown in case of a cyber attack, but nuclear reactors run for one to two years once the fuel is installed. Even when the reactor is shutdown, the fuel still produces decay heat and must be cooled, or the reactor core may melt. Therefore, a design basis cyber security system must be embedded to the nuclear plant to address any future premeditated attempt.

However, defending against an evolving threat like cyber terrorism is a complex endeavour. A tiny disk or hard drive is enough to execute a cyber terror

A tiny disk or hard drive is enough to execute a cyber terror plan even if the computer system in a plant is isolated from the internet.

plan even if the computer system in a plant is isolated from the internet. To protect nuclear plants from cyber attacks, the primary objective of any cyber security programme must be to protect the confidentiality, integrity and attributes of electronic data or computer systems and processes in a highly complex and integrated environment. Appropriate measures against cyber attacks targeting the digital ICT systems of nuclear plants, therefore, include detection, response, mitigation, recovery. It is critically important to ensure that computer networks used to operate nuclear power plants are not accessible even by "insiders" who could tamper the cyber systems directly from within the plant. To achieve this capability, countries need to promote a cyber security culture aided by appropriate law enforcement and emergency management systems.

So far, there is no known incident of reactor meltdown and release of radiation owing to cyber attacks on nuclear plants. However, the four incidents mentioned highlight the importance of incorporating computer or cyber security as a fundamental part of the overall security plan for nuclear facilities across the globe as nuclear disasters do not respect national boundaries.

The IAEA, in pursuit of helping nations to build national cyber warfare capabilities, has formulated both legal and technical guidelines. The Office of Nuclear Security was created in 2002 and the *Technical Guidance* on "Computer Security at Nuclear Facilities" (2011) has brought together "the knowledge and experience of specialists, who have applied, tested and reviewed computer security guidance and standards within nuclear facilities". Since safety and security of nuclear facilities are sole responsibilities of sovereign nations, the IAEA and other multilateral initiatives extend only advisory help. The Multinational Statement on Nuclear Information Security during the Seoul Nuclear Security Summit 2012 also recognised "the importance of preventing non-state actors from obtaining information, technology or expertise required to acquire or use nuclear materials for malicious purposes", and advised "to enhance cyber security measures concerning nuclear facilities".

It is alleged that India currently has neither a strong cyber law nor effective cyber security capabilities. Many times in the past, government websites and emails have been hacked. Reportedly, computers at the Rare Materials Plant (RMP), Rattehalli, were possibly infected by malware. Neither there is no official

response in this regard nor there exists any information on India's cyber security strategy for its nuclear infrastructure. Surrounded by unstable nations and non-state actors who could attempt to manipulate its nuclear programme by laying their hand on cyber espionage or sabotage, India must be serious to defend against such a critical threat. The critical infrastructure protection policy of India must protect them on priority basis. It is expected that Indian technocrats are prepared to mitigate a Stuxnet-type threat to its nuclear installations with robust protection. The Global Centre for Nuclear Energy Partnership (GCNEP), under construction at Kheri Jasaur, Haryana, aims to pursue enhanced safety and security studies.

However, considering the evolving and challenging threat environment and negative public perception on anything nuclear, especially after the Fukushima nuclear disaster, any cyber-generated malfunction of nuclear plants could have far-reaching repercussions – on plant safety, material safety, and socio-environmental safety – which in turn could lead to unacceptable societal consequences. Most importantly, it could undermine the 'public acceptance of nuclear power' in general, and our endeavour to ensure energy security through the nuclear route in particular, as the world has no easy options left for meeting its growing energy demand.

Dr **Sitakanta Mishra** is a Research Fellow at the Centre for Air Power Studies, New Delhi.