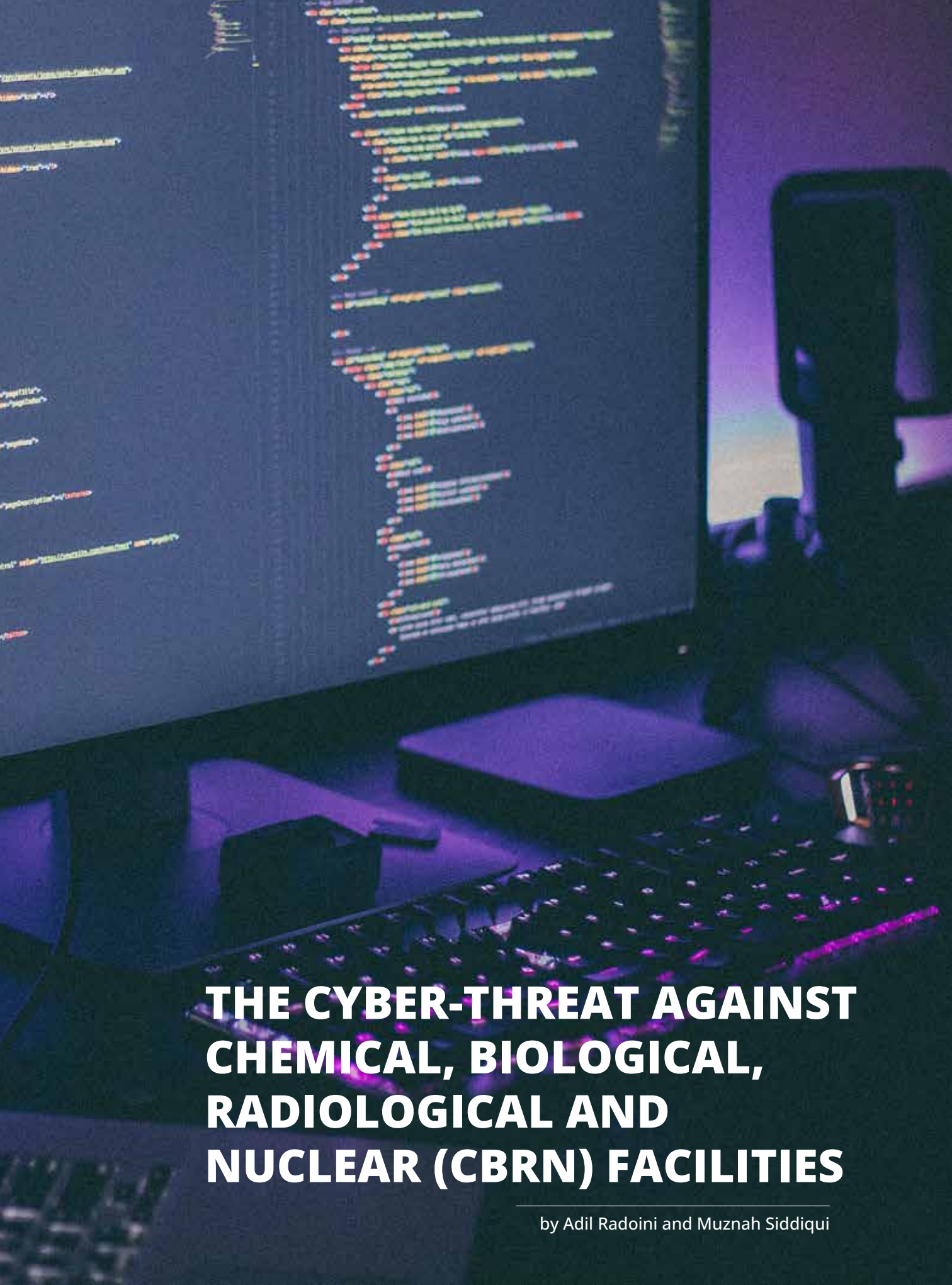
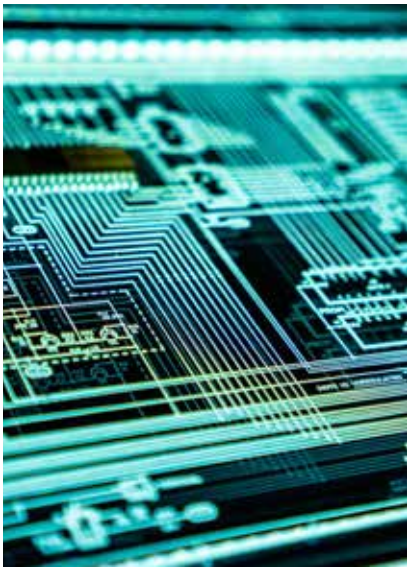


THE CYBER-THREAT AGAINST CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR (CBRN) FACILITIES

by Adil Radoini and Muznah Siddiqui

The increasing digitalization of critical infrastructure sectors and the associated industrial systems, particularly the digitalization of chemical, biological, radiological and nuclear (CBRN) facilities, is changing the nature of cyber-risks. In today's societies, entire ecosystems of key sector have become increasingly digital, decentralized and complex, multiplying opportunities and increasing the level and typology of threats.



A recent major cyber-attack that should serve as a warning to us all about the scope these threats can have is the so-called "*SolarWinds cyber-attack" t*hat went undetected for months before Reuters[1] reported on it in December 2020. By first hacking into the U.S. company SolarWind, the massive hack successfully spread and infiltrated their customers' IT systems. Among them were U.S. Government agencies. SolarWinds is a Texas-based company whose software manages American companies, institutions, and government departments' administrative and security networks. The attack targeted parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury. Other high-profile clients attacked included Fortune 500 companies such as Microsoft, Cisco, Intel, Deloitte, and organizations like the California Department of State Hospitals and the Kent State University.[2] According to high U.S .government officials, the scope of the damage is unprecedented and it could take years before the networks are secure again.[3]

A few weeks later, on 5 February 2021, a U.S. water treatment plant was targeted by a cyber-attack. An operator in Florida's West Coast saw his cursor being moved around on his computer screen, opening various software functions that control the water treatment. The hackers increased by 100 times higher than normal the level of a chemical substance called sodium hydroxide - or lye - in the water supply.

Sodium hydroxide, the main ingredient in liquid drain cleaners, controls water acidity and removes metals from drinking water in treatment plants. Lye poisoning can cause burns, vomiting, severe pain and bleeding.[4]

> **In today's societies, entire ecosystems of key sector have become increasingly digital, decentralized and complex, multiplying opportunities and increasing the level and typology of threats**

1 https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0P-G?edition-redirect=uk

2 https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402?mod=djemalertNEWS

3 https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html?action=click&module=Opinion&pgtype=Homepage

4 https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems

Cyber-sabotage could affect the normal operations of a CBRN facility or significantly damage equipment and processes

More recently, in May 2021, another major cyber-attack targeted the U.S. Oil and Gas pipeline, disrupting the supply of almost half of the East Coast's fuel. According to the World Economic Forum, the attack caused an increase of oil prices and it is considered as one of the most expensive attacks to an economy.[5]

The recent attacks targeted objectives in the United States, which is one of the most advanced countries in terms of cyber-security policies and preparedness in this area. All of this calls attention to the vulnerability of critical infrastructures to cyber-attacks across the world, as it poses a serious threat to the very functioning of entire sectors of our societies. Indeed, IBM, in a 2020 report, noted a 2000% increase in cyber-security incidents targeting the operational technologies employed in Critical National Infrastructures (CNI) since 2019.[6] The complexity of the interconnection of information systems in CNI is compounded by the COVID-19 pandemic, as it forced an abrupt shift for facilities and companies towards working from home. Consequently, the cyber-threat level has dramatically increased as production control networks have, for the most part, become remotely accessible.

Among all the critical infrastructures, special attention should be dedicated to the chemical, biological, radiological and nuclear facilities, considering the lethality, the pollution potential and the psychological impact that an attack involving CBRN material can provoke. Cyber threats can be engineered by various actors with differing intentions, including for instance

5 https://www.weforum.org/agenda/2021/05/cyber-attack-on-the-us-major-oil-and-gas-pipeline-what-it-means-for-cybersecurity/

6 https://securityintelligence.com/posts/what-the-explosive-growth-in-ics-infrastructure-targeting-means-for-security-leaders/

the physical sabotage and destruction of infrastructures and processes by creating deliberate malfunctions. In the case of CBRN facilities, the consequences could be life-threatening. Furthermore, computer hackers may seek to disclose critical information, render information systems unavailable to authorized users or prevent the proper update of information. The objectives of the criminal actors involved in these operations may include the wish to build access points in facilities for further uses, spreading fear among the public and undermining the credibility of governments.

A cyber-attack against a CBRN facility can disable the IT system and allow the theft of sensitive data. But the breach can also serve as a stepping stone to prepare other types of attacks involving CBRN materials. In addition, cyber-sabotage could affect the normal operations of a CBRN facility or significantly damage equipment and processes. The attacks themselves can occur by injecting malware or viruses into systems, thereby posing a considerable threat to the supply chain management cycles. Finally, cyber espionage refers to retrieving confidential information for malicious purposes. This form of threat is more common, as it requires a lower level of technical expertise, several tools are also freely available on the Internet, such as spyware systems.

The types of malicious actors range from terrorists, covert agents and disgruntled employees to state/non-state hackers, militant opponents, or recreational hackers. In the case of the former, several terrorist groups have begun using social media to recruit hackers and radicalize CBRN facility employees who could enormously facilitate the effort of obtaining sensitive information on the IT system of the facilities. For instance, ISIL successfully radicalized an employee of the Doel nuclear power plant in Belgium, who eventually left the country to partake in terrorist activities.[7] Moreover, the FBI highlights the additional concern that terrorists may hire hackers to conduct cyber-attacks in conjunction with conventional attacks.

A cyber-attack against a nuclear facility could potentially corrupt nuclear command and control systems whilst potentially allowing for the release or theft of radioactive material. The Nuclear Threat Initiative documented 16 cases of cyber-attacks against nuclear facilities across the world. Among the targeted countries there were Lithuania, the UK, the U.S, Japan, Syria, Iran, South Korea and Germany (see table below).

The urgency for a cyber-chemical security framework is compounded by the fact that virtually all chemical plants have some type of computer-based automated control systems and also because the communication networks are replaced or complemented with wireless networks, and to point-to-point communications. In most cases, the chemical industry self-regulates, and whilst they invest in their cyber-security, national governments ought to step in and create standardized norms and regulations.[8]

A recent study that researched the opinion of international field leaders in biotechnology and cybersecurity concluded that "the issue of cyber-bio-security is not well-known or understood, even among biotechnology and cybersecurity experts." Accordingly, the issue of cyber security in the field of biology have not been effectively fleshed out in a practical manner, thereby creating vulnerabilities at the apex of

7 https://www.washingtonpost.com/world/europe/brussels-attacks-stoke-fears-about-security-of-belgian-nuclear-facilities/2016/03/25/7e370148-f295-11e5-a61f-e9c95c06edca_story.html

8 https://www.aiche.org/academy/videos/conference-presentations/detection-cyber-attacks-and-resilient-operation-nonlinear-processes-under-economic-model-predictive

life and medical sciences and infrastructure systems.[9] The increased reliance on Internet connections of facilities containing sensitive bio-data that could be used maliciously to create or modify bio-agents and pathogens should be considered as a severe threat globally.

UNICRI is currently identifying assessment methodologies, tools and good practices that can be made available to the United Nations Member States to improve the governance of cyber-threats against CBRN facilities. The various types of threats and malicious actors involved highlight the need to develop a set of standardized good practices to prevent attacks against CBRN facilities. These practices can be divulged through general awareness-raising and training activities addressed to decision-makers, managers and operators. Such activities can provide the relevant stakeholders with the tools needed to identify potential emerging threats. Facilities can use various methods, including simulations and tests, to enhance knowledge among staff. This will prepare them to identify potential vulnerabilities; evaluate the impact of attacks; recognize the need for constant vigilance; establish protection mechanisms during attacks; develop cyber-resilience and ascertaining the importance of cyber-security instruments. Through embedding awareness of the risks of cyber-threats across operational, managerial and decision-making levels, the most exploited vulnerabilities of CBRN facilities can be consequently considerably reduced.

Furthermore, robust and effective legislation is a prerequisite for developing effective cyber-security frameworks to secure CBRN critical infrastructures. Accordingly, relevant legislative bodies may authorize national cyber-security programs which address the CBRN risk whilst incorporating adequate deterrent and enforcement measures. In addition, an appropriate legislation should address emerging forms of cyber-threats and vulnerabilities whilst potentially establishing voluntary standards in partnership with the private sector. Consequently, an important element of a risk mitigation strategy should envisage the involvement of experts in cyber-physical security, science, intelligence, law enforcement, state communication departments etc., in a collaborative process. This holistic and multi-stakeholder approach will ensure the full breadth of issues are covered. Finally, relevant legislation and regulations could establish clear consequences for non-compliance, particularly given the magnitude of the potential risks. Other forms of governance measures could include education and training for personnel, the establishment of ad-hoc policies, structures and processes (such as regular assessments and inter-agency coordination), alongside the allocation of resources towards investing in cyber-security infrastructures, in particular for CBRN facilities.

UN Member States have engaged in important efforts to protect their societies from CBRN threats. It is now time for them to get prepared and prevent CBRN risks coming from the cyber-dimension.

9 https://www.sciencedirect.com/science/article/pii/S2590053620301129#bb0040

Chronology of cyber-attacks to nuclear facilities[10]

#	MONTH/YEAR	NAME	COUNTRY	DESCRIPTION	CATEGORY
1	February 1992	Ignalina Nuclear Power Plant	Lithuania	Employee attempted sabotage	Intentional
2	June 1999	Bradwell Nuclear Power Plant	United Kingdom	Employee altered/destroyed data	Intentional
3	March, 2002	Davis-Besse Nuclear Power Station	United States	Worm	Intentional
4	June 2005	Japanese Nuclear Power Plants	Japan	Data release	Unknown
5	December 2006	Syrian Nuclear Program	Syria	Espionage	Intentional
6	March 2009	Energy Future Holdings	United States	Employee attempted sabotage	Intentional
7	June 2010	Natanz Nuclear Facility	Iran	Stuxnet virus used to destroy centrifuges	Intentional
8	April 2011	Oak Ridge National Laboratory	United States	Data theft via spear-phishing	Intentional
9	October 2011*	Natanz Nuclear Facility	Iran	Duqu virus used to conduct espionage	Intentional
10	May 2012	Natanz Nuclear Facility	Iran	Flame virus used to conduct espionage	Intentional
11	January 2014	Monju Nuclear Power Plant	Japan	Data release	Unknown
12	December 2014	Korea Hydro and Nuclear Power Company	South Korea	Data theft and release	Intentional
13	February 2015	Japanese nuclear material control center	Japan	Nuclear facility used as relay point in cyberattack	Unknown
14	February 2016*	Nuclear Regulatory Commission/U.S. Department of Energy	United States	An employee attempted to infect government computers with viruses distributed via spear-phishing emails	Intentional
15	April 2016	Gundremmingen Nuclear Power Plant	Germany	Two viruses entered the plant's fuel rod monitoring system	Unknown
16	June 2016	University of Toyama, Hydrogen Isotope Research Center	Japan	Data theft via spear-phishing	Intentional

THE AUTHORS

Adil Radoini is the United Nations Interregional Crime and Justice Research Institute (UNICRI) Regional Coordinator for the Middle East and Gulf Cooperation Countries. He works for the Chemical, Biological, Radiological and Nuclear (CBRN) and Security Governance Programme. He previously worked as a journalist for the Italian press and television sectors. In 2009, together with other international experts, he published "Un Hussein alla casa Bianca", a perspective of the Arab world on the 2008 U.S. elections. He graduated from the University of Bologna with a Master's degree in International Relations focusing on Middle Eastern politics, carrying out a research thesis led in Cairo and at the Institut d'Etudes Politiques in Paris.

Muznah Siddiqui is a graduate from the University of Cambridge, and has completed her Master's in International Relations and Politics. She is currently working as an intern at the United Nations Office of Counter-Terrorism, and her research interests include the protection of human rights, cyber-security and countering violent extremism.

10 NTI, 2016