UNGA DISEC

The NPT and concerns associated with the same

Note from the Executive Board

Welcome to the simulation of the General Assembly sub-committee meeting of Disarmament and International Security. The agenda item list consists of two agendas mainly comprising of:

The NPT and concerns associated with the same

The role of the Executive Board is to facilitate the debate and be the procedural guidelines of the committee and shall substantially abstain themselves from the debate. The simulation shall be adhering UNA-USA rules of procedure which shall be explained during the first hour of the meeting. However there are certain expectations from the committee which mainly constitutes of diplomatic courtesy and ideal representation of a diplomat during the committee sessions. The diplomats or representatives are expected to debate and deliberate upon the agenda item and come to a consensus on a decisive solution if they deem it necessary.

Lastly the role of a study guide is to be the pillars for your research and its role is limited to be the backbone of your research and the diplomats are expected proceed further and delve deep in the process of their research.

Regards,

Brahadeesh Srinivasan	Krishnakumar Ramachandran	Sai Ram
President, UNGA-DISEC	Vice-President, UNGA-DISEC	Director, UNGA-DISEC

Introduction to the simulation

United Nations General Assembly

The United Nations General Assembly (UNGA, GA, or French: Assemblée Générale "AG") is one of the six principal organs of the United Nations and the only one in which all member nations have equal representation. The General Assembly (GA) is the main deliberative, policymaking and representative organ of the UN. Its powers are to oversee the budget of the United Nations, appoint the non-permanent members to the Security Council, receive reports from other parts of the United Nations and make recommendations in the form of General Assembly Resolutions. It has also established a wide number of subsidiary organs.

The General Assembly meets under its president or Secretary-General in regular yearly sessions the main part of which lasts from September to December and resumed part from January until all issues are addressed (which often is just before the next session's start). It can also reconvene for special and emergency special sessions. Its composition, functions, powers, voting, and procedures are set out in Chapter IV of the United Nations Charter.

Voting in the General Assembly on important questions, namely, recommendations on peace and security, budgetary concerns and the election, admission, suspension or expulsion of members – is by a two-thirds majority of those present and voting. Other questions are decided by a straightforward majority. Each member country has one vote. Apart from approval of budgetary matters, including adoption of a scale of assessment, Assembly resolutions are not binding on the members. The Assembly may make recommendations on any matters within the scope of the UN, except matters of peace and security under Security Council consideration. The one state, one vote power structure potentially allows states comprising just five percent of the world population to pass a resolution by a two-thirds vote.

The Disarmament and International Security

The First Committee deals with disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime.

It considers all disarmament and international security matters within the scope of the Charter or relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of international peace and security, as well as principles governing

disarmament and the regulation of armaments; promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments.

The Committee works in close cooperation with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament. It is the only Main Committee of the General Assembly entitled to verbatim records coverage.

The First Committee sessions are structured into three distinctive stages:

1. General debate
2. Thematic discussions
3. Action on drafts

Working Methods of General Assembly

Over the years, efforts have been made to rationalize the work of the Committee, concentrating on rearranging its agenda and improving its organization of work.

- During the 48th session of the Assembly, in 1993, the item entitled "Rationalization of the work and reform of the agenda of the First Committee" was included in the agenda of the Assembly. Thereafter, the Assembly has focused on improving the effectiveness of the methods of work of the First Committee.

- During the 59th session, in response to a request of the Secretary-General to seek the views of Member States on improving the effectiveness of the methods of work of the First Committee, a report compiling those views was submitted by the Secretariat.

- Since the 60th session, under the item "Revitalization of the work of the General Assembly", the Committee has adopted its programme of work and timetable for the forthcoming session. Please also see the note by the Secretariat.

Sources:

http://www.un.org/en/ga/first/

https://en.wikipedia.org/wiki/United_Nations_General_Assembly

A/01/
001

The NPT and the Concerns associated with the same

1 | Introduction

The Nuclear Non-Proliferation Treaty (NPT) is one of the bed-rocks of modern policy in the United Nations. Its aim is to attempt to reduce proliferation of nuclear weapons technology, and increase the use of nuclear energy for peaceful purposes. It illegalizes nuclear weapons technology transfer, but does not put a halt on peaceful nuclear programmes, or to a large extent, indigenous nuclear programmes. It promotes the disarmament of nuclear weapons, through various direct and indirect methods.

While we could spend a lot of time explaining what the NPT is and does, any delegate can access that. What this guide shall attempt to do is provide auxillary data and direction to the whole thought-process behind the approach on delegating under such an agenda.

The key cruxes of understanding the NPT, and how to improve it, is not through understanding how it operates, but through analysing how it fails under circumstances. The treaty itself is about 50 years old; it was first signed in July 1968. Technology and geopolitics have since drastically changed – in fact, one of the most important parties to the treaty, the Soviet Union, underwent dissolution. For more than a decade and a half after its introduction, the world saw massive upsurge in the amount of nuclear firepower – it was three times the size of the world's arsenal today. And do not be quick to declare that the NPT has been successful in reducing the arsenal to a third of the then level – it was more because of the economics of manufacturing and maintaining nukes than it was about efforts towards disarmament.

Towards understanding its flaws, we shall look at two scenarios – the Iran situation, and the DPRK situation. After that, we shall look at other flaws, and then close with possible scenarios the NPT has not spoken much about, while elaborating just one of them.

Like said before, do not expect fact-based guidance here, mere direction. There are other scenarios worth exploring in committee, which we do expect you to do in committee.

2 | The Iran Situation

To understand the Iranian situation with respect to the NPT, one must understand the history of their nuclear programme:

1957: The United States and Iran (under the Shah) signed a civil nuclear cooperation agreement as part of the **Atoms for**

Peace program. The agreement provided technical assistance, uranium to Iran and research cooperation on peaceful nuclear energy.

1967: The Tehran Nuclear Research Center, supplied by the United States, opened with a 5MW enriched uranium research reactor - Tehran Research Reactor (TRR).

1968: July – Iran signed the Nuclear Non-Proliferation Treaty (NPT) and ratified it in February 1970.

1974: May 15 – Iran signed the **NPT's Safeguards Agreement** with the IAEA which allowed inspections for verifying that nuclear enrichment for peaceful nuclear energy is not diverted to nuclear weapons or other nuclear explosive devices.

1979: **The Iranian Revolution happened. The Islamic Republic of Iran discards the NPT in itself.**

After the revolution, the United States stopped supplying highly enriched uranium for the Tehran Research Reactor.

1984: Iran opened the Isfahan Research Nuclear Centre – China supplied a training reactor.

1987: Argentina concluded a $5.5 million deal to supply a new core for the Tehran Research Reactor, so as to operate with 20% enriched uranium, instead of 90%, and deliver the 20% EU to fuel the reactor.

1992: Russia and Iran signed a **Cooperation Agreement on the Civil Use of Nuclear Energy**.

1995: Russia agrees to build a light water reactor at Bushehr, Natanz under IAEA safeguards within 55 months. The project's completion was delayed until August 2010.

1997: May – The IAEA expanded the Safeguards Agreement by adopting the **Additional Protocol**, whereby inspectors would be allowed to conduct short notice inspections. Iran signed the it in 2003, but has not ratified.

1999: Iran and Saudi Arabia issued a joint statement supported turning the Middle East into a **WMD-Free Zone**, to counter Israel's alleged nuclear programme.

2000: President Clinton signed the **Iran Non-proliferation Act**, empowering the US to sanction those providing aid to Iran's nuclear, chemical, biological and ballistic missile weapons programs.

2002: The National Council of Resistance of Iran, an exiled opposition group, revealed that Iran was building two secret nuclear sites at Natanz and Arak. President Khatami acknowledged the existence of Natanz and other facilities on Iran's state-run television and **invited the International Atomic Energy Agency** to visit them.

2005: IAEA inspectors were only allowed partial access. **Under the NPT, Iran was not required to allow inspectors into its military bases**.

August – Britain, France and Germany (a.k.a., the EU-3) proposed the *'Framework for a Long-term Agreement'* to Iran, offering aid in developing peaceful nuclear energy; in exchange Iran should not pursue anything but light water power and research reactors. It also called for a on the heavy water research reactor at Arak. Iran **rejected the proposal**.

November – Iran's parliament approved a bill to **stop voluntary implementation** of the Additional Protocol, if Iran were referred to the Security Council. The parliament did **not** move to **block normal inspections**.

2006: **Iran Freedom Support Act** imposed economic sanctions on nations and companies that aided Iran's nuclear program.

December – The UNSC Resolution 1737 sanctioned Iran for failure to comply with Resolution 1696 and halt uranium enrichment, and banned sale of nuclear-technology and froze the assets of key players. This started the charade of sanction after sanction, which followed up with more in 2006 (EU), 2007 (The UNSC Resolution 1747), 2010 (The UNSC Resolution 1929), 2011, 2012 and 2016.
June – The **Stuxnet computer virus** was reportedly detected in staff computers at the Bushehr nuclear plant.

2012: January 1 – Iran's nuclear agency reported that Iranian scientists have produced their first nuclear fuel rod.

February –President Ahmadinejad unveiled Iran's first domestically produced batch of 20% enriched nuclear uranium for TRR; IAEA inspectors left Iran after being **denied access**.

2016: January – Iran and the P5+1 Implementation Day to start implementation of the **Iranian Civil Nuclear Deal**. The US, EU, and UN lifted some sanctions. Iran also regained

access to the international financial system, repatriated billions of dollars in frozen assets abroad, and returned to the oil market.

September – Iran began construction on its second nuclear power plant with Russian help, which will go online in 10 years.

Stuxnet

The Stuxnet Worm first emerged during the summer of 2010. It is a 500kb worm that infiltrated numerous computer systems. It operates by targeting Windows networks, infiltrating them, and replicating itself, and finally, gaining access to the Program Logic Controllers.

After getting access to the industrial program logic controllers, the creators of the virus will have access to crucial industrial information as well as giving them the ability to operate various machinery at the individual industrial sites.

Stuxnet Effect on Iran

Over fifteen Iranian facilities were attacked and infiltrated by the Stuxnet worm. It is believed that this attack was initiated by a random worker's USB drive. One of the affected industrial facilities was the Natanz nuclear facility. The first signs that an issue existed in the nuclear facility's computer system in 2010. Inspectors from the International Atomic Energy Agency visited the Natanz facility and observed that a strange number of uranium enriching centrifuges were breaking. The cause of these failures was unknown at the time. Later in 2010, Iran technicians contracted computer security specialists in Belarus to examine their computer systems. This security firm eventually discovered multiple malicious files on the Iranian computer systems. It has subsequently revealed that these malicious files were the Stuxnet worm. Although Iran has not released specific details regarding the effects of the attack, it is currently estimated that the Stuxnet worm destroyed 984 uranium enriching centrifuges. By current estimations this constituted a 30% decrease in enrichment efficiency.

Assessment

By all measures, the Iranian Revolution placed a regime that was more authoritarian, more trigger-happy, and more hostile (by Western Standards) to the cause of Non-Proliferation, stemming from their general distrust in Israel and the 'Western Hagemonies'.

Iran's case though made one issue with the NPT very clear – the NPT does not allow proliferation, but it does not place any

restrictions on development of indigenous nuclear programmes, regardless of whether they are for peaceful purposes, or destructive purpose. The issue though lies in that peaceful technology can easily be repurposed for destructive purposes. An even broader, overarching question, though, is whether the point of the treaty is to restrict that at all – after all, it is called the Non-***Proliferation*** Treaty, not the Non-Nuclear Treaty.

3 | DPRK Situation

The DPRK situation has been volatile for years. The Democratic People's Republic of Korea is considered a 'rogue' nuclear power by many. Information that the IAEA has about DPRK can probably be fit into one slightly oversized file. Often associated with Pakistan, the Korean Nuclear Programme, said to have been kick-started in the late 1980s, was guided and aided by a senior Pakistani atomic research scientist Dr. A.Q. Khan. DPRK has tested rockets and missiles since 1993, and graduated to nuclear warheads in 2006. The estimates of stockpiled weapons are put at around 12-27 nuclear weapons. It was party to the NPT from 1985 till 2003 and was member of the IAEA till 1994 - it has now withdrawn from both regimes. DPRK and other concerned parties are bound by the following nuclear treaties and agreements now:

- North-South Joint Declaration of the Denuclearization of the Korean Peninsula
- IAEA-DPRK Safeguards Agreement
- USA-DPRK Agreed Framework

DPRK is not a signatory to the Limited Test Ban Treaty, and has withdrawn from the NPT. It takes a stance that it is no longer obligatory for it to comply with the Safeguards Agreement and the Agreed Framework. Its history as a "fully fledged nuclear power" is as recent as 2009; the then IAEA Chief Dr. Mohamed ElBaradei opined so after reports surfaced that the DPRK has fully functional ICBMs, miniaturized warheads for medium-range missiles, etc. On the other hand, DPRK has been harvesting nuclear energy for civilian purposes since 1965, when the research reactor IRT-2000 at Yongbyon Nuclear Scientific Research Centre, built with Soviet aid, became fully operational. In 1979, DPRK constructed an indigenous second research reactor, along with ancillary facilities.

DPRK's non-compliance with the IAEA has been famously documented. DPRK refused to comply with IAEA obligations till 1992. In 1993, the IAEA released evidence of DPRK's incomplete compliance to its original declaration

and commitments. DPRK, in response, demanded special inspections under conditions specified by its officials - which was not agreed to by the IAEA. The IAEA also reported its concerns to the UNSC. As a result, the DPRK issued a notice announcing withdrawal from the NPT, though the notice was suspended before withdrawal took effect. But ongoing tension between DPRK and the IAEA resulted in its withdrawal from the IAEA. Ever since, the relationship between the IAEA and DPRK has been minimal. After many attempts at making DPRK comply with its obligations, the Board of Governors in 2003 expressed their concern about DPRK's non-compliance through a resolution; this time, DPRK did withdraw from the NPT.

As stressed quite often by IAEA chief Yukiyo Amano, DPRK's programme remains one of the IAEA's biggest areas of concern. In many of his speeches about the situation in DPRK, he has called upon it to allow unbiased IAEA inspections, to no avail. DPRK, under Kim Jong-un seems disinterested in cooperation with the IAEA.

On January 10, 2003, the Democratic People's Republic of Korea announces its withdrawal from the NPT, effective January 11. Although Article X of the NPT requires that a country give three months' notice in advance of withdrawing, DPRK argued that it had satisfied that requirement because it originally announced its decision to withdraw March 12, 1993, and suspended the decision one day before it was to become legally binding. DPRK's stated reasons for withdrawing from the NPT were that the United States was threatening its security by its hostile policy toward DPRK. According to DPRK, the United States had singled it out as a target of a pre-emptive nuclear attack and had threatened it with a blockade and military punishment. The question regarding DPRK's right to withdraw from the NPT under Article X, above, is not whether DPRK's allegations regarding the United States' intent or policies are true in any objective sense. Instead, Article X allows each party to make its own decision as to whether extraordinary events, related to the subject matter of the NPT, have jeopardized its supreme interests.

Arguably, customary international law would impose a good faith requirement on the party deciding that extraordinary events have jeopardized its supreme interests, but the NPT does not establish any mechanism for making a determination as to whether a party has acted in good faith.

On July 4, 2006, DPRK test fires seven ballistic missiles, including its longest-range missile, the Taepo Dong-2. The other six tests include a combination of short- and medium-range Scud-C and Nodong ballistic missiles,

launched from the Kittaraeyong test site. Although the tests of the six short-range missiles appear to be successful, the Taepo Dong-2 fails less than a minute after launch. The launch if the missiles violated DPRK's voluntary moratorium on flight-testing longer-range missiles, which Pyongyang had observed since September 1999.

The UN Security Council adopts Resolution 1695 condemning DPRK's missile launches. The resolution calls on Pyongyang to return to the six-party talks and "demands" that the country suspend its ballistic-missile activities and re-establish its flight-testing moratorium.

Sanctions against DPRK have been imposed by a number of countries and international bodies. The United Nations has itself imposed a lot of sanctions in DPRK after the nuclear test performed in 2006, which include ones in 2006 (Resolution 1718), 2009 (Resolution 1874), 2013 (Resolution 2087 and Resolution 2094), 2016 (Resolution 2270 and Resolution 2321), 2017 (Resolution 2371), and 2017 (Resolution 2375)

Also in February 2017, China announced it would ban all imports of coal for the rest of the year. Other countries like the USA, South Korea, Japan, Australia and bodies like European Union have also imposed sanctions on DPRK.

Assessment

DPRK's concerns about the lack of transparency, setting aside its rogue mentality, may have a basis in truth – 'hagemonic' powers have made it easier for themselves to sustain large arsenals, while limiting newer powers from gaining the deterrence needed to keep the balance of power.

4 | Other Flaws in the NTP

The NPT, by design, isn't legally binding in entirety – only the Article VI is. Article VI states that:

> *Each of the Parties to the Treaty undertakes 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, and on a treaty on general and complete disarmament under strict and effective international control.*

But, as one can understand, every treaty which asks nations to undertake measures in

good faith is incapable of handling transgressions.

This is evidenced in that the NPT does not espouse any measures or provisions of penalties for missing deadlines, or having transgression.

Another clash-point is that as in the Iran and DPRK scenario, the NPT creates two sides – the haves and the have-nots, i.e., the ones with nuclear programmes, who have a lot of power, and are very insulated, and the ones without, who either cannot afford one, or want to acquire one and are being 'unfairly' oppressed and stalled from their own right to Self-Defense. This idea is extended by the fact that there is no active deterrent from secession. Therefore, the NPT cannot really enforce itself onto countries.

Another issue rose with the DPRK scenario – when DPRK seceded from the NPT the first time around, and then re-subscribed to the NPT, there was no accountability system in place to discuss or question any transgressions in this period in between. The NPT also ties in with the CTBT, which itself does not have complete subscribership.

5 | Evolving Scenario - Nuclear Digital Security

The internet - the world's biggest battleground. In 2015, there were more than 3.2 billion users across the globe. With the advent of higher generations of internet fidelity, and the introduction of optic fibres as a means of communication, the security of every individual user, government and industry in the world is becoming a rather large question mark, if not a conspicuous joke. In 2009, a FBI report stated that "Cybergeddon" was the second biggest threat to the United States after a nuclear holocaust. In 2010, the secretary general of the International Telecommunication Union (specialized agency of the UN since 1947) suggested the implementation of an international treaty on cyber-security, focusing on three major points of the struggle against cyber-terrorism: global financing to protect citizens of the world, shared information on cyber-terrorists and a ban on state-to-state cyber-attacks. The IAEA director, Mr Yukiya Amano, stated:

"Reports of actual or attempted cyber-attacks are now virtually a daily occurrence. The nuclear industry has not been immune."

Nuclear facilities are now fully computerized and are subject to a numerous number of cyber-attacks. As long back as in 1992, a Lithuanian nuclear power plant was

infected with a virus by one of their technicians, and this lead to huge concerns about the security of the plant. In 2003, a worm software, called the 'Slammer' worm, infected the Davis-Besse Nuclear Plant in Ohio, United States, rendering the sensors of the nuclear core unavailable for five hours. In 2010, another worm, named 'Stuxnet' destroyed over a thousand uranium centrifuges in the Natanz nuclear facility in Iran. It is important to note that these facilities were 'air-gapped', or separated from the public internet. Stuxnet, according to Eugene Kaspersky, Founder and CEO of Kaspersky Internet Security, is US-government engineered worm to target the Iranian nuclear program, and was also responsible for contamination of Russian nuclear power plant too. The United Nations, through the help of agencies like the International Atomic Energy Agency, works closely with nuclear energy providers. Yet, the struggle continues, to prevent cyber-attacks and more importantly, to train nuclear plant employees to recognize such attacks. In fact, cyber-attacks could initiate very dangerous operations, ranging from simple ones such as removal of radioactive material, to more serious ones, such as sabotage of nuclear facilities and/or theft of nuclear sensitive information, or even the gravest of situations – complete meltdowns.

While it is hard for us youngsters to imagine a nuclear plant run without digital systems, original facilities were built without digitization, which, while making the job highly tedious, ensured that they were impossible to sabotage from remote locations. This is not the case anymore, as digitization of the nuclear industry allows cyber-attacks to come from anywhere in the world, including a computer in some obscure basement. Moreover, this type of attack can be utilised by numerous actors or groups: one notorious example is that of anti-nuclear power "hacktivists", who could try (and indeed have tried) to disrupt a facilities, release confidential information, or even corrupt systems, in order to add credence to their agenda of demonstrating the danger of a nuclear incident. Though this type of cyber-attack would be the least dangerous, other groups, such as skilled cyber-criminal groups, such as criminal groups, who can potentially attack nuclear plant, steal confidential information or even could indulge their more vicious motive. This scenario has already happened: in 2014, a cyber-criminal group stole data from Korea Hydro, a group that operates 23 nuclear reactors in the Republic of Korea. Blueprints were leaked on the internet and the group threatened to release more information unless the group paid an exorbitant ransom. If one is a follower of popular culture, then the fire-sale, in Die Hard would be a fitting example of the capability of such groups.

Evidently, States are a central part of the development of cyber-attacks: they purport

infiltration units and structures in other countries, to fuel espionage missions. As of now, such technology has been used to gain intelligence, and thankfully, not to attack the facilities. But escalation into conflict is a possibility that can usher in the rise of cyber-attacks as a means of warfare.

And lastly, the biggest concern for all nuclear powers today is from terrorist groups. They have proven their ability to use social media and the deep Web to carry out messages and information, just as the ISIL could, has demonstrated time and again. Furthermore, in countries like Pakistan, where rising uncontrolled nuclear proliferation grows parallel to the frightening threat of an Afghanistan-esque scenario due to the nefarious activities of various terrorist groups like the Al Qaeda and the Tehrik-e-Taliban Pakistan, it is important that the United Nations can work towards increasing the security of nuclear systems, before a potentially cataclysmic incident shocks the world into whatever action it can take.

Significance of Cyber-Attacks

It is critical to understand that attacks targeting the control systems of facilities would be much more harmful: the loss of power (induced by shutdown of nuclear power facilities) would impair the power grid of many countries significantly, especially if the attack is coordinated to other facilities. Such is the fear, that countries like Germany and Japan, considered by many as technologically advanced nations, have decided to reduce their dependence on nuclear power, with Germany attempting to slash its 30% dependence to about 1-6%.

Another kind of infection could also result in the release of radiation: attacks on the main power generators and disabling of safety features, such as safety neutron control rods, (all possible under a cyber-control) could result in the cascading of the chain reaction, inducing a meltdown of the core of a nuclear plant, which would lead to huge physical, medical and environmental issues in the vicinity of the plant. This has led many Nations to implement nuclear systems that aim to reduce the chances of remote hacking. Some methods are given below.

Protection by antiquity

Most nuclear facilities were built in the 1970's - 80's, when hardware was considered advanced and more trustworthy than the software available of this period. Thus, some nuclear facilities still rely on what is called systems of 'protection by antiquity', where the functioning is controlled by hardware, and not written into code, which protects the system from any kind of cyber-attack. Thus, in order to 'hack' the plant, one requires physical access to the actual control circuits. Given the tight

security around such facilities, unless one can claim to be destiny himself, (or Ethan Hunt, which is still the same), one cannot hack into such nuclear facilities.

But any such system has its own problems - as this equipment reaches the end of its working possibilities, it has to gradually be replaced by other hardware that comprises digital features. Microprocessors are preferred today, being considerably more sensitive and flexible than hardwired circuits, and it is the set of these very properties that make them easier subjects to hacking. Thus, digitalization has also reduced the number of actual fail-safes currently existing in nuclear facilities as they are incorporated to microprocessors. Hacking such new microprocessors now allows attack on the system and also serves to neutralize the failsafe-system instrumented for this particular equipment.

Air-gapping

The most important concern in the digitalization of nuclear facilities is that an increasing number of them now require to be connected to the public internet, which was impossible, and completely unnecessary, a few years ago. Nuclear facilities used to be 'air-gapped', that is, there was a physical disconnection between the network used in the facility and the public internet. The growing use of company networks, both due to the needs of newer software for frequent updates and due to attempts to promote internet-based products, and such, makes this separation increasingly impractical. But this connectivity to the public internet leaves facilities prone to attack. For example, employees of Areva, a French multinational nuclear power group, have access to nuclear facilities in other locations, as well as from subcontractors for this company, due to the use of public internet systems. This system, though, multiplies the risk of a cyber-attack as an increasing number of individuals have the knowledge, prowess and resources to access these facilities. Another problem is the constant use of Wi-Fi networks in facilities, for employees. This gives new avenues for hackers to operate without easy detection. Online monitoring is slowly becoming a major part of the nuclear industry: carelessness when using such methods could be a pathway for viruses and intrusive malwares.

Even when the nuclear plant is "air-gapped", simple USB drives can be used to carry harmful malware. This is probably how the Iranian plant at Natanz was infected, despite being separated from the Internet. A similar case was that in the Lithuanian plant discussed above. Introducing a USB device into a nuclear control computers could lead to the hacking of systems with malware and even to the shutdown of the plant as a best case scenario. In Canada, wherein employees are free to use WiFi and

Mobile Data inside their facilities. This exposes the area to dangerous infection-risks. The risks are often considerably higher when employees of the facility deliberately act in a manner that could endanger the plant – the phrase 'insider threat' had been regularly used during the Cold War. Examples are of Ukrainian, Belarussian and Kazakh employees in nuclear facilities, whose low wages and sometimes Russian or former-Soviet loyalties make ideal extractors of information.

While these methods increase or decrease the chances of infection, there are many problems that the nuclear world is riddled with, stemming from the highly secret nature of such advanced technologies. A few problems have been explored here.

Secrecy

Traditionally, it has been a trend that physical nuclear safety has always been given preference over cyber-safety. Even in recent years, wherein cyber-security has been a growing concern, the physical security threat is still considered the most important issue. The issues arise if and when a nuclear system is subject to cyber-attacks - breaches in security, such as that which lead to the decommissioning of the Fessenheim plant in France, aren't usually publicized, as they could possibly reveal chinks in the virtual armour, called the 'firewall', the breached plant, or in facilities running on similar protocols and systems. In fact, in most cases, there is a complete lack of communication between countries: if one attacked plant rectifies the flaw in its system, this information is often suppressed and other countries running on similar systems are not notified, and hence, may not have a chance to correct it. Nuclear operators are reluctant to share information with other facilities, even though the same systems are used in various industries. Moreover, governments are not willing to share information regarding the possible flaws in the systems of their facilities, which renders the tracing of attackers even more difficult. In some cases, nuclear facilities may deal with systemic malfunctions, without realizing or being able to trace out that it has been perpetrated by cyber-attackers.

Commercial Problems

Yet another limitation of cyber-defence in nuclear facilities is that these cyber-amenities come against the existing operation. For example, if a patch needs to be installed in a nuclear facility, the resulting maintenance may require a shutdown of the plant or a military facility for even a couple of days, which is unacceptable, especially for civil contractors and operators. Thus, such updates are often delayed in order to maintain round-the-clock operation of the facility. The divide between nuclear scientists, nuclear engineers and software

engineers often creates tensions when changes or test have to be made.

Further problems arise when the patches that are installed fail. The complexity of these systems still pose the risk of an unforeseen malfunction, as one 'driver' being incompatible with the patch could result in the complete shutdown of the plant. The lack of operational standards in hardware and software with respect to cyber-security around the world, and the incompatibility of local standards (for example in the United States) with international requirements, seem to indicate insufficient effort or will towards complete cyber-security system.

Financial Problems

A rather new issue is that in developing countries, cyber-security is still very expensive and hence very limited, as they do not have the resources yet to obtain cyber-security systems, or create and enforce regulation for the safety of digitalized systems. While some governments and operators have been actively seeking to invest into cyber-security in this field is not as commercially attractive as for information technology industries.

So, what has the world done about this?

As noted earlier, cyber-attacks have become increasingly common, as a tool of intelligence gathering, from other countries or corporate, for profit, or for doing massive damage easily.

In 2001, the Budapest Convention on Cyber-Crime, the first international treaty in the field, was signed and by 2016, 50 countries had ratified it. While attempting to harmonize most national laws, it also helps by defining illegal access or interferences in systems, and by giving legal boundaries for prosecutive action to be taken against cyber-criminals.

In March 2006, the Additional Protocol to the Convention on Cyber-Crime was added to the treaty, and while it addressed racist and xenophobic material, it did not stress on further nuclear safety. No other international treaty has been signed since, even if the many platforms of the United Nations have often recommended the same.

In 2015, the G20 leaders issued a statement that State-sponsored cyber-attacks would be unlawful by norms. While the same has been discussed often, the G20 States and other major powers have often indulged in cross-espionage and cyber-attacks. Tensions have risen to unseen levels between the United States of America and the People's Republic of China after the Google, in 2014, denounced daily attacks, which they claim, were traced to China. In this situation, many countries and their major companies, such as software giants from India,

providing cyber-security services, have thrived in the current market.

Meanwhile, France, have been funding developers of software to completely clean portable devices and ensure the safe transfer of data over networks. In 2005, the European Union instituted the 'European Union Agency for Network and Information Security Agency' (formerly the 'European Network and Information Security Agency', or 'ENISA'). A separation of responsibilities had been decided towards the fight against cyber-terrorism, cyber-crime and prevention of a cyber-crisis between different branches of the government.

In South Korea, the Korea Institute of Nuclear Safety (KINS) has developed a regulatory guide on cyber-security of digitalized I&C (Instrumentalisation and Control) systems that aims at preventing, detecting and responding to malicious acts involving nuclear and other radioactive materials and associated facilities. The guidance covers technical and managerial controls for the computer security of safety I&C systems.

The world is used to reacting to such attacks, not preventing them; the implementation of measures has been carried out only after the damage has been done, and even then, not effectively. Hence, working towards prevention is key in this matter.