ADVANCED AND CYBER WEAPONS SYSTEMS: TECHNOLOGY AND ARMS CONTROL

ANDALO (TRENTO) – ITALY

8-15 JANUARY 2017

Protection of Nuclear Facilities Against Armed Attack including Cyber Attack

By

A.A.Soltanieh

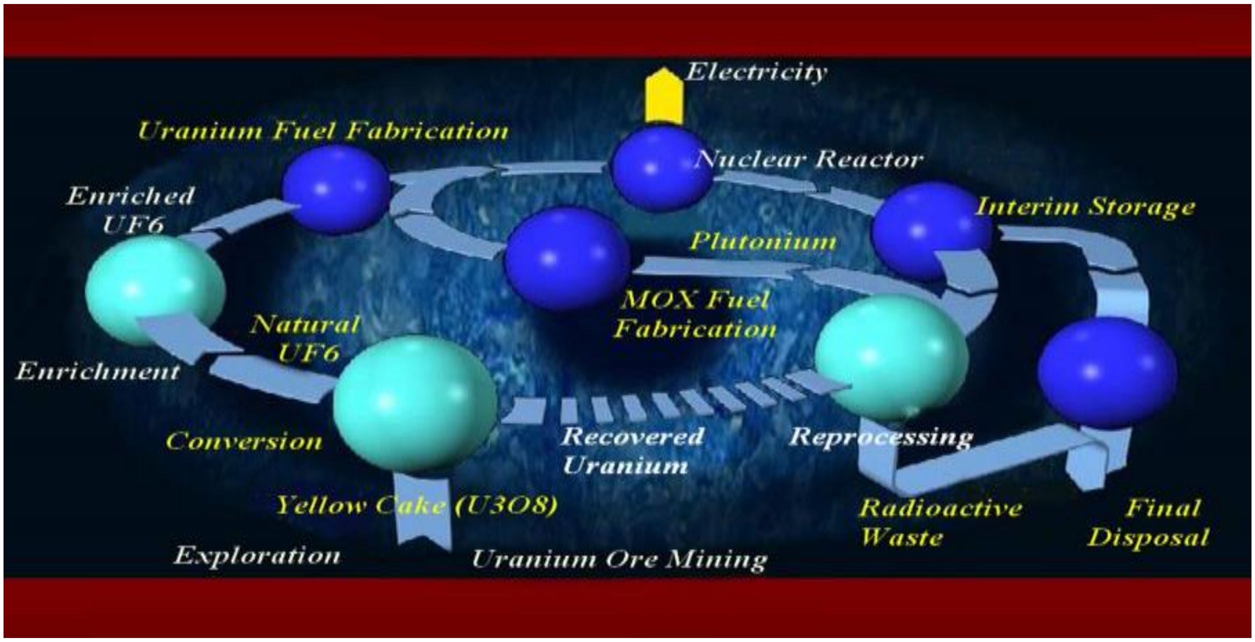
Former Ambassador to the United Nations and Other International Organizations (IAEA & CTBTO) in Vienna

Fast efficient promotion of "Information Technology", expansion of visual space, vast application of internet all over the world have contributed a lot to the "man to man relation", contributing to the sustainable development in the 21st century. However, the instrumental malicious use of such an advanced technology has created a serious global concern.

Serious cyber- attacks occurred in all over world have given warnings to public and decision makers. It seems no one is immune. Thus, it needs collective mobilized efforts to combat such threat.

Among the cyber- attacks, the most serious and worrisome is the attacks against nuclear facilities since it shall have radiological consequences for the mankind and the environment.

Though the security impacts and consequences of armed attack, including cyber-attack, against different part of nuclear fuel cycle are not the same, but radioactive release is common. In chains of the cycle such as uranium conversion, waste management, and reprocessing, in nuclear fuel cycle, where chemical material such as fluorine is also involved, in case of attack, threat to human beings and environment, is much more.



Nuclear Fuel Cycle (from Mining to final disposal of nuclear waste)

The cyber- attack against nuclear facilities within the fuel cycle, specifically the enrichment is no more an anticipated probable scenario, but a reality. Cyber- attack using so called Stuxnet, under the “Nito Zeus Plan” against Iranian enrichment facilities was aimed at paralyzing the peaceful activities which are under the full scope safeguards of the International Atomic Energy Agency (IAEA).

Convening international conferences on CIP (Critical Infrastructure Protection) during recent years indicate the fact that the intellectual communities have noticed the importance of the issue. However, the urgency of the matter, as well as the necessity of collective work, is not felt yet. Researches are being performed in different countries in confidential manner without exchange of technological information. We have still long way to go to reach to the point of the convergence of scientific works for such common objective, combating the common threat. Such international conference may increase the awareness of decision maker of the gravity of the threats to the extent that they are convince to compromise the monopoly for the sake of national and internal security.

From the economic point of view, the cyber- crimes direct and direct damage to the world economic is estimated about 400 billion dollars which shall drastically increase in twenty years. According to some reports this include the huge investment that research centers of giant companies have so far invested up to 1.5 billion dollars.

Apart from the economic concerns, the violations of privacy of citizens of the world by cyber – crimes are matter of serious concern.

There is a paradox; while the government of different countries of witnessing the continuous threats and attacks against their countries, specifically their citizen, however some strongly do support the hackers and cyber- criminal, with the assumption that they are serving them to combat against the adversaries. They lose sight of the fact the knowledge could not be contained and the experts of the other side can have the access to, depending on the price, and soon they will use against them.

In cyber-space the identity and the location of the players are kept secret, anonymous names are usually used. This made the legally process against the cyber- criminal very difficult.

Considering the fact that security has three main specificities: Accessibility, Integrity, and Confidentiality, the materialization of "security of cyber space" is very difficult. The cyber is moving so fast. The former head of CIA, during President Bush Administration, confessed that the cyber was moving so fast that we were always a step behind it on the politics.

Cyber Attacks against Iran' Nuclear Facilities

- FLAME was developed in 2007 used in attack in May 2012
- DUQU was developed in 2007 used in attack in September 2011
- STUXNET developed in 2009 used in attack in February 2010

Impact of Stuxnet virus on the strategic nuclear program of Iran

According to the report of the IAEA on 18 February 2010, there were indication of virus in the Iranian nuclear facilities. The IISS, the US institute, known or its close collaboration with intelligence services on Iran's nuclear activities, reported that over 1000 centrifuge machines were effected thus removed and replaced by new ones. However, the same institute confessed that attackers failed in their attempt to destroy all Iranian centrifuges. According to the research made by Symantec Company, the Stuxnet virus attacked the controlling systems of the motors of the centrifuge machines and their speeds.

Nitro Zeus Plot against Iran's Nuclear Activities

According to some news the plan "Nitro Zeus" was design by the US Defense, Pentagon, for cyber- attack against Iranian telecommunication, electricity and air defense as well as nuclear facilities in case the negotiation with failed. The designed and preparation of this plan for a comprehensive cyber- attack was made during 2009-2010, upon the instruction of the US president to General John Allen.

The industrial sabotage providing Iran with conventional equipment used in any industry with prefabricated electronic malfunctions was discovered by Iranian expert at a nuclear site. The author as the representative of Iran to the IAEA raised this irresponsible dangerous industrial sabotage at the General Conference, incorporating in the nuclear security resolution.

Threat is Global!!

This is not merely the concern of Iranian nuclear industry. The South Korea's state-run nuclear operator was also the subject of a cyber- attack in December 2014 which saw the theft of sensitive information, including the blueprints of at least two nuclear reactors and electrical flow charts (Kim and Cho, 2014).

The news "Fears of Belgium for Nuclear Power Plant" with expression of wornness by Belgium and other European Countries, is a clear indication of the dimension of security threat .

Multidimensional Phenomena

There is not a "one-size-fits-all" solution to counter cyber incidents and the older approach is outmoded and not sufficient to deal with today's threats to ICT systems. Therefore:

A mix of technical, organizational, cultural-focused solutions is needed in order to enhance "resilience" of the ICT system and web Inbuilt "security-by-design" through the whole system

Strengthen a "cyber-security culture" at each level of multi-layered complex infrastructure

Security of Cyber Space vis-à-vis Nuclear Security

The term nuclear security covers all security aspects of nuclear facilities or activities. At the same one has to notice that nuclear security is intertwined with nuclear safety and nuclear safeguards. Each of these three, so called 3S, are related to specific international norms, regulations, conventions.

Nuclear security covers, any deliberate acts which endangers the security of a nuclear facility or activities. Therefore, military attack, terrorist attack, cyber-attack by a terrorist or a state, industrial sabotage, and the assassination of nuclear scientist or personnel are related to nuclear security.

Iran’s International Initiative

Pursuant to the military attack by Israeli regime against Iraqi reactor in 1981, followed by military attack against Bushehr Nuclear Power Plant of Iran by Sadam regime, the author proposed on behalf of the Islamic Republic of Iran a draft resolution which was passed in 1990. According to the said resolution, Res/533, any armed attack and threat of attack against a nuclear installation during operation and during construction constitutes violation of the UN Charter, IAEA Statute, and the international law. According to this resolution, the United Nation Security Council has to act immediately in such cases. After almost two decades, when the threat of attack by Israeli regime against Iranian nuclear facilities were augmented, the author, on behalf of the Islamic Republic of Iran proposed a text to with the same content, to the IAEA General Conference in 2009, which was adopted, by consensus, as the Presidential Statement. The following year, 2010, at the NPT Review Conference similar text was proposed by Iran which was also adopted by consensus. Therefore, there is an internationally accepted document in this regards paving the way for next step to turn it to a legally binding instrument.

Considering the fact that the nuclear security is a global concern, the Nuclear Security Summit held in Washington (2010), Seoul (2012), The Hague (2014) , and the last in Washington again (2016) with participation of about 50 selected countries is an exclusive approach which dooms to failure. In order to put things on the right track Iran (the author on behalf) and other like-minded countries proposed in the IAEA to hold high level conference open to all Member States. The first Ministerial Conference was held in 2013.The 2nd was held in December 2016 under auspices of the IAEA.

The issue of cyber-attack was incorporated in the minitrial declaration in 2016:

“ We recognize physical protection as a key element in nuclear security, and support the further development of the IAEA’s assistance in areas of importance to Member States such as nuclear forensics, nuclear security detection architecture and response, information security, transport security, and insider threat mitigation, recognizing the need for appropriate measures to protect sensitive information in achieving this objective. In particular, we support the IAEA’s efforts to assist Member States to strengthen computer security, recognizing the threat of cyber-attacks against nuclear installations”.

H.E. Dr. Salehi, vice president & Head of Atomic Energy Organization of Iran touched upon this issue in his statement at the Ministerial Conference in 2016:

“ In the backdrop of the 2013 platform, the risk that nuclear or other radioactive material could be used in criminal or terrorist acts remains a matter of concern and continues to be regarded as a threat to international security. Ironically, advances in information and communication technologies and the intertwining of industrial infrastructure and cyberspace have caused another security concern. It is clear that cyber-attacks against nuclear facilities and activities– as happened in the case of the deployment of the Stuxnet virus against Iran will amplify the scale and expand the domains of insecurity with transboundary consequences. In this context, while recognizing the real threat of cyber-attacks it is incumbent upon all of us to condemn such attacks and to take every necessary measures to confront them in a comprehensive manner”.

Conclusion:

- Any cyber- attack against nuclear facilities has radiological consequences with the transfer of radioactive material beyond international borders, as happened in the case of nuclear accidents (Chernobyl and Fukushima), therefore is a global threat, thus it requires prompt collective international actions both for prevention and for emergency assistance;
- The interconnection of various institutions such as digital infrastructure organizations, business community, law enforcement, safety regulatory bodies, NGOs all have to collaborate closely in order to effectively combat the cyber-attacks.

Concrete Proposal:

Considering the international developments on protection of nuclear facilities from armed attack, specifically the last provision adopted by consensus, it is the time to initiate negotiation for a legally binding instrument, a convention, on prohibition of any armed attack or threat of attack ,including cyber- attack, against nuclear facilities.

Annex-1

Pertinent Remark by Dr. Hans Blix, Former Director General of the IAEA:

“Dear Ali,   4 October 2014 15:09

I took a very active part in the drafting of what became art.56 of the Protocol Additional to the Geneva Conventions of 12 August 1949. The article has regard to the protection of works and installations containing dangerous forces and protects ’nuclear electrical generating stations against attack, if the attack may cause the release of dangerous forces and consequent severe losses among the civilian population.’ I have also great appreciation for the resolutions adopted by the General Conference of the IAEA on measures to strengthen international co-operation in matters relating to nuclear safety and radiological protection.

Certainly, the protection of civilians is the most important rationale for the provisions of these documents. I think any belligerent action against objects that could release radioactive material may stand as seriously condemned as an attack with nuclear weapons. Any such attacks could also put the whole nuclear industry in the world in jeopardy.

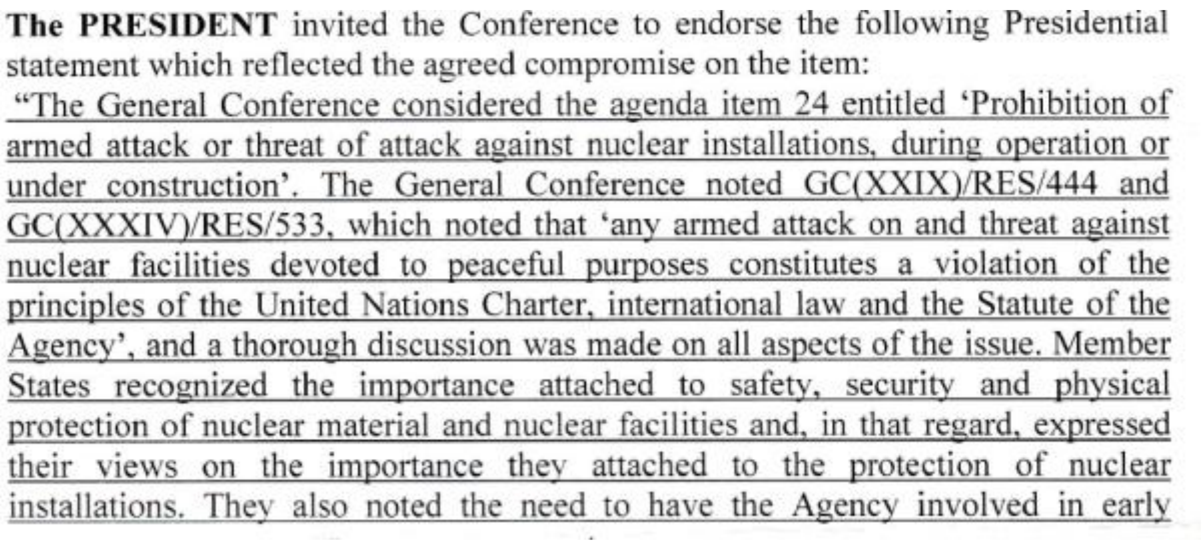
You are free to quote the above.

With warm personal regards,

Hans Blix”

Annex-2

Unanimous Decision of the IAEA General Conference 2009:

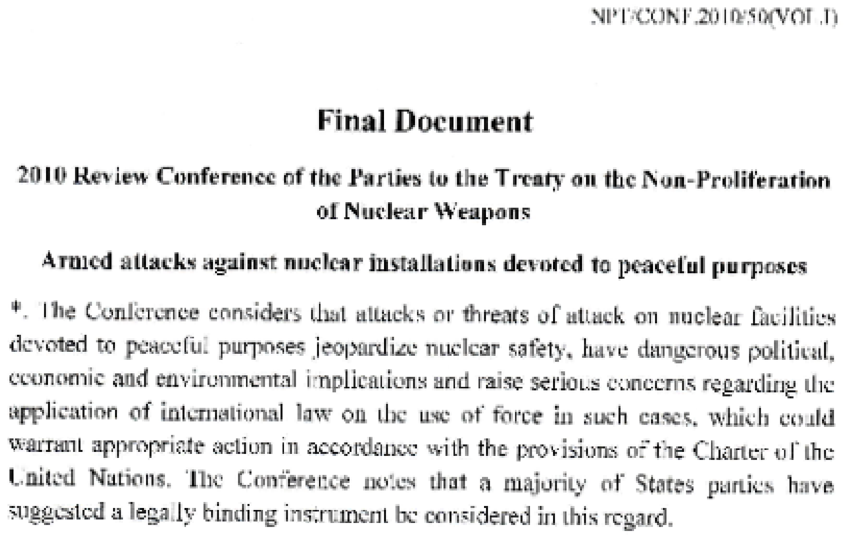


The PRESIDENT invited the Conference to endorse the following Presidential statement which reflected the agreed compromise on the item:

"The General Conference considered the agenda item 24 entitled 'Prohibition of armed attack or threat of attack against nuclear installations, during operation or under construction'. The General Conference noted GC(XXIX)/RES/444 and GC(XXXIV)/RES/533, which noted that 'any armed attack on and threat against nuclear facilities devoted to peaceful purposes constitutes a violation of the principles of the United Nations Charter, international law and the Statute of the Agency', and a thorough discussion was made on all aspects of the issue. Member States recognized the importance attached to safety, security and physical protection of nuclear material and nuclear facilities and, in that regard, expressed their views on the importance they attached to the protection of nuclear installations. They also noted the need to have the Agency involved in early

Annex-3

Unanimous Decision of the NPT Review Conference 2010:



NPT/CONF.2010/50(VOL.I)

Final Document

2010 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons

Armed attacks against nuclear installations devoted to peaceful purposes

*. The Conference considers that attacks or threats of attack on nuclear facilities devoted to peaceful purposes jeopardize nuclear safety, have dangerous political, economic and environmental implications and raise serious concerns regarding the application of international law on the use of force in such cases, which could warrant appropriate action in accordance with the provisions of the Charter of the United Nations. The Conference notes that a majority of States parties have suggested a legally binding instrument be considered in this regard.

Annex-4

Reference:

1. Papers delivered at the "International Conference on Computer Security in the Nuclear World" held on 1-5 Jun 2015, IAEA, Vienna;
2. Keister & Associates, 2016, Internet attack against "Nuclear Power Plant";
3. Computer Security of Nuclear Facilities, 2013, IAEA Security Guideline;
4. Ian Baraclough ,2013,The IAEA's nuclear security Guidance;
5. Cyber Security at Civil Nuclear Facilities; Understanding the Risks, 2016, Chatham House Report, United Kingdom;
6. Caroline Baylon, Roger Brunt, and David Livingstone, September 2015;
7. Maurizio Martellini, 2015, the "Protection of complex infrastructures against cyber-attacks", the High Level Event on Nuclear Security, Bologna, Italy;
8. The Role of Training and Support Centers, and Centers of Excellence, the Nuclear Security Summit 2016 and Beyond ,Bologna, Italy – 7/8 May 2015;
9. Ambassador A.A. Soltanieh, 1-5 July 2013, International Ministerial Conference on Nuclear Security: Enhancing Global Efforts, IAEA, Vienna;
10. Enhancing Global Efforts, 1 July 2013, European Union, International Ministerial Conference on Nuclear Security, IAEA, Vienna;
11. Enhancing Global Efforts, Ministerial Declaration, 2015, International Ministerial Conference on Nuclear Security, IAEA, Vienna;
12. Conducting Cyber Threat Assessments at Nuclear Facilities, 09-12 February 2016, Technical Meeting, IAEA, Vienna;
13. Allissa J. Rubin and Milan Schreur, March 25, 2016, Belgium Fears Nuclear Plants Are Vulnerable;
14. Bring Cyber warfare further out of the shadows, 1 August 2016, The Post's View;

15. EU efforts to strengthen nuclear security, 13 March 2014, joint staff working Document –SWD (2014) 107 final report;
16. Computer Security Techniques for Nuclear Facilities, 2016, IAEA Guideline.
17. International Conference on Nuclear Security, IAEA, Vienna, 5-9 December 2017