American Model United Nations
International Atomic Energy Agency

IAEA/II/1

SUBJECT OF RESOLUTION: Nuclear security

SUBMITTED TO: The International Atomic Energy Agency

The International Atomic Energy Agency,

Alarmed by past nuclear terrorism incidents such as those committed by Aum Shinrikyo, Al Qaeda, the North Caucasus terrorists, the Islamic State, and the smuggling of nuclear material from the Kinshasa research reactor,

Noting with concern recent insider and cyberattacks at nuclear production facilities such as the Doel-4 nuclear power plant in 2014,

Seeking to prevent future acts of terrorism involving nuclear technology and material acquired through a breach in the secure transit or storage of nuclear resources,

Recalling the 1979 Convention on the Physical Protection of Nuclear Material and the 2005 Convention for the Suppression of Acts of Nuclear Terrorism, passed by the General Assembly to address nuclear terrorism,

Further affirming that terrorism related to nuclear technology and materials must be prevented to maintain a stable global order and prevent a major nuclear disaster,

Acknowledging the increase in prevalence of cyber-related attacks on companies, government agencies, and other organizations worldwide,

Anticipating the danger of cyberattacks increasing as more technology is integrated into nuclear facilities,

Affirming the role of the International Atomic Energy Agency (IAEA) in preventing breaches of security at nuclear sites and noting the ability of non-State actors to launch cyberattacks from outside the targeted country,

Noting previous efforts by the IAEA to provide expertise and guidance at all stages of the development of information and computer security programs,

Convinced that collaboration between IAEA Member Nations will serve to further solidify a global counter front to those engaging in nuclear and cyberterrorism,

1. *Calls for* the IAEA to collaborate with the United Nations Counter-Terrorism Centre and develop strategies for combating nuclear terrorism with a focus on:

    (a) The security and integrity of civilian facilities utilizing nuclear technology and fissile materials;

    (b) Defense and safety measures in the face of threats or attacks;

    (c) The tracking of terrorist groups operating in regions with nuclear programs or those with ambition to commit an act of nuclear terrorism;

    (d) This report shall only be disclosed to the IAEA representitives every two years to provide transparency to the strategies the IAEA is using to combat cybersecurity and threats of nuclear terrorism;

2. *Requests* that the existing definition of offenses by non-state terrorist actors, defined in the "Convention on the Physical Protection of Nuclear Material" to specifically include the following:

    (a) Attacks rendered, either physically or through the use of malicious software or other computer-related programs, on nuclear facilities, including but not limited to nuclear power plants, enrichment facilities, nuclear weapon stockpile facilities, or other physical sites involving radiological material;

    (b) Any attempt, threat of attempt, or success in an attack on a nuclear facility or transport, shall be considered an illegal act of terror punishable by the state wherein the attack occurred;

3. *Recommends* Member Nations place additional emphasis on the domestic protection of fissile materials in transit including items such as but not limited to:

(a) All vehicles used for the transportation of fissile material used in atomic energy shall be accompanied by armored/protected personnel transporting this material and following standardization guidelines set forth by the IAEA;

(b) Advanced surveillance methods to be used to track said vehicles throughout transit;

4. *Further recommends* Member Nations send security personnel to seek training from the IAEA Nuclear Security Training and Demonstration Centre on issues that pertain to nuclear terrorism, prevention of nuclear terrorism, intercepting cyber security attempts, and creating stronger cyber infrastructure, specifically related to the preparation of information technology personnel;

5. *Further calls for* Member Nations with nuclear facilities to appoint at least one staff member specifically trained in nuclear security and continually educated on the threats to and management of cybersecurity and the mitigation of potential cyberattacks by:

(a) Having Member Nations annually send a report to the IAEA board of directors to show that their nuclear security faculty is well trained in the issues of nuclear security;

(b) Allowing Member Nations that require assistance in the education or training of cyber security request training from the IAEA Nuclear Security Training and Demonstration Centre;

(c) Ensuring Member Nations who show additional financial needs for the adoption/modernization of infrastructure or nuclear education may submit a request to the board of directors on a need basis;

6. *Suggests* that the IAEA offer training for Member Nations' civilian nuclear security officers in order to learn the protections stated in this resolution through:

(a) Utilizing the new Nuclear Security Training and Demonstration Centre in Austria upon its completion;

(b) Providing training resources to local security forces and institutions to conduct the same level of training as the Nuclear Security Training and Demonstration Centre in order to promote self-sustaining local leadership;

7. *Encourages* the usage of existing information sharing mechanisms to include the following items, noting that participation in this information sharing is voluntary, but highly encouraged:

(a) Usage of existing current counter-terrorism intelligence programs via the Office of Counter-Terrorism, for all consenting nations to voluntarily share information with the IAEA and fellow member participants to follow all potential terrorist actors to prevent theft;

(b) Member States shall receive financial, educational, and/or infrastructural benefits as the Nuclear Security Training and Demonstration Centre (for training and infrastructural concerns) and the board of directors (for financial concerns) see best fit;

8. *Emphasizes* the importance of Member Nations' adherence to the recommendations set forth in the report, "Computer Security Techniques for Nuclear Facilities," authored by the IAEA:

(a) This report provides guidelines outlining why and how nuclear facilities should protect digital assets;

(b) The publication provides a risk-management approach to protect Sensitive Digital Assets (SDAs);

(c) The document also establishes revisions and enhancements to current policies, procedures, and programs of nuclear facilities;

9. *Encourages* the utilization of modernized cybersecurity systems and standards for nuclear sites worldwide, while emphasizing the importance of diversity in specific methodologies, as in a local to regional to global approach, used to protect computer systems at these facilities:

(a) Every nuclear site shall be recommended to adopt continually changing or updating strategies or changing their cybersecurity every six months, as reviewed by cybersecurity experts;

(b) The IAEA shall facilitate the collaboration between Member Nations and the expansion of cyber infrastructure;

(c) The IAEA will adopt measures to further address and elaborate on these standards in their 2022-2026 strategy plan;

(d) The IAEA shall employ cybersecurity teams to test the current cybersecurity systems of nuclear facilities as a means to assess their competencies and shortcomings for beneficial feedback;

10. *Suggests* the compilation of voluntarily provided data, with the collaboration of The United Nations Office of Counter-Terrorism (UNOCT), for the sharing of information on malicious software for the use of the security agencies of respective Member States, for the purpose of probing computer systems to establish benchmarks of resilience:

(a) Allows for the voluntary sharing of intelligence information to the United Nations Security Council in the event of a terrorist group acquiring fissile material as this institution would be best suited for dealing with the negotiation and aftermath of such an act;

(b) Promotes collaboration and transparency among both Member Nations and United Nations institutions to further the values set out in the UN Charter and ensure a safer global society;

11. *Requests* that the United Nations Security Council intervene in the case of such terrorist acquisitions:

(a) Recommends that the Security Council assesses the feasibility of intervention in the defined situation;

(b) Advises Member Nations to continue sharing information with the IAEA and other participants of the program during such a crisis so that respective parties remain aware of any possible additional threats.

Passed by consensus, with 0 abstentions