Panel II Presentation:

*Interim Measures to reduce and eliminate risk of accidental, mistaken, unauthorized or intentional nuclear weapons detonations*

**25 February 2016**

**Dr Beyza Unal, Nuclear Weapons Policy Research Fellow Chatham House**

Thank you Mr. Chairman,

I appreciate the opportunity to speak at the panel on measures to reduce and eliminate the risk of accidental, mistaken, unauthorized or intentional nuclear weapon detonations.

I would like to first start by defining risk in the current international security context and then specifically in relation to nuclear weapons. Then, I am going to present concrete interim measures to reduce risk of accidental, mistaken, unauthorized or intentional nuclear weapons detonations. I will conclude with final remarks on risks.

**What is risk?**

Human beings rarely know as much as they think they do and we often take things for granted most of the time. We take safety and security granted.

In fact, the catastrophic impact of nuclear weapons has changed, as risks associated to nuclear weapons use are higher today. Risk assessment has played a part in this fact-based analysis. Risk is defined as the product of probability and consequences. Since the probability of accidental, mistaken, unauthorized or intentional use of nuclear weapons is not zero, and the consequences of such an incident are high, the risks are high. For reduction of risks, we need to decrease the probability of an incident happening, decrease the consequences, or at best do both.

Patricia Lewis, the Director International Security Department at Chatham House, describes ‘risk’ in a very clear way. She states that risk is not a constant variable. It changes in time, under different conditions and circumstances. New information on probabilities changes the risk assessment. Cyber threats, for instance, play huge part in the calculations of nuclear weapons detonations.

New information on consequences of nuclear weapon detonations changes the risk assessment as well. Urbanization, for instance, complicates humanitarian response; and it will get only worse in the future. Future trends indicate that “cities will contain 65% of the world population” by 2040. Urbanization and population growth in mega-cities will directly bring new security and health challenges.

---

*The views expressed are those of the author, as are any inaccuracies in fact or interpretation.*
Risk perception changes as the priorities change. Humanitarian pledge, signed by 125 countries (to date), is an example of shift of priorities and a sign for a greater political commitment to nuclear disarmament.

Risk perception also changes with emerging technologies and threats. Analyses of the incidents of near nuclear misses show that technology is a challenge to the nuclear systems. In many of the near misses cases in history, it was the ‘human judgment factor’ which saved the world from destruction.\(^1\)

This takes us to the interim measures in order to reduce risks... The interim measures that I will discuss aim to create transparency, non-escalatory, and the ones that could increase the decision-making time in crisis situations. These measures, moreover, could build the bridge between nuclear weapon states, non-nuclear weapon states and nuclear host countries.

**Possible Measures to reduce risks of accidental, mistaken, unauthorized or intentional nuclear weapons detonations**

1) **Multilateral reduction of strategic and tactical nuclear weapons:**

A concrete risk mitigation measure is to reduce--and ultimately eliminate--the number of both strategic and tactical nuclear weapons. This effort has been initially conducted through bilateral efforts, such as new START Treaty.

Negotiations on multilateral reduction of strategic nuclear weapons could involve different approaches such as:
- prohibition (legal measures)
- Parity of reductions
- Proportionate reductions
- implementation of no-first use policy
- no-use commitments
- stage reductions

There is a growing concern over the safety and security of tactical nuclear weapons particularly the ones in Turkey and Italy. The United States' decision to upgrade these nuclear bases will help to reduce the risk, however, increased armed conflict and terrorist activity in neighboring countries should be factored in risk assessment. Furthermore, recent news about terrorist groups (such as ISIS) monitoring a Belgian nuclear scientist is extremely concerning for the same reason. Unauthorized use and theft are possibilities that shall not be ignored. Nuclear bases in Europe could also be targeted to cyber-attacks. As far as I know, it is the nuclear host country’s responsibility to assure cyber security at the operational level; and it is important to establish certain operating procedures to minimize cyber vulnerabilities. This takes us to the second interim measure:

---

\(^1\) Patricia Lewis, Heather Williams, Benoit Pelopidas, and Sasan Aghlani, *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy*
2- Measures to increase cyber security in nuclear power plants, nuclear laboratories, command and control systems:

2.a. Cyber Security in Nuclear Weapons Laboratories

Nuclear weapons laboratories (and nuclear power plants\(^2\)) involved with weapons design, research, or nuclear inventories are highly vulnerable to theft or illicit disclosure of information through cyber-attacks. A preliminary research on audit reports and unclassified information regarding cyber security at nuclear weapons laboratories shows that:\(^3\):

a- there are problems with implementing risk management and system security testing in nuclear laboratories,

b- routine practices are mainly missed out (such as vulnerability management practices),

c- computers continued functioning even after the identification of cyber threat. In some cases, the management thought these computers do not need urgent response,

d- personnel accounts left open for several months even after the personnel left their job at nuclear laboratories,

e- no adequate monitoring of the systems by the management, no assigned personnel for monitoring,

Similarly, command and control systems (C2 systems) are vulnerable to cyber-attacks.\(^4\)

2.b. Cyber security in command and control systems and satellite systems

Cyber threats create false/fake nuclear attacks, which may cause retaliatory action; thus escalation in response. Even computers that are separated from internet or network hubs are vulnerable to cyber-attacks without the knowledge of the end-user, such as:

- There may be virtual platforms established for maintenance entry points (i.e. to conduct performance tests, management),

- Open data ports in classified systems,

- Embedded exploits in software and hardware (by the manufacturer without the knowledge of the end-user)

These are all security vulnerabilities that could actually take place in any network with classified or unclassified scientific and/or technical knowledge.

\(^2\) Since civilian nuclear power plants is not inherently related to nuclear weapons detonations, this presentation does not discuss in great depth about the risks associated to these installations. For further reading, please see Caroline Babylon with Roger Brunt and David Livingstone, Cyber Security at Civil Nuclear Facilities, Chatham House Report, September 2015, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf.


\(^4\)
Examples: There were several attempts to compromise low frequency radio communication signals to submarines (previously, submarines were believed to be air gapped), as well as system vulnerabilities due to false warning data signals. Other cases include hacking government reconnaissance satellites and attempts to spoof GNSS data (e.g. GPS).

Nuclear missile systems rely on space assets and there is a rise of concern about potential for jamming and spoofing, and issuing deliberate or inadvertent commands to missiles. In other words, nuclear command and control systems are subjected to cyber vulnerabilities.

Space systems are part of national critical infrastructure and reliance on the performance of these systems is significant in crisis situations. Yet, a tempered command, control, communications, and intelligence system may cause false information, misperception, and could trigger inadvertent escalation.

As long as nuclear weapons exist, cyber threats will persist. The best risk mitigation measure is to create resilient command and control systems that identify system vulnerabilities. Reacting to every incident would neither be efficient nor manageable.

A cyber security risk management should include immediate action measures, such as:
a- conducting risk assessments of evaluating vulnerabilities and threats to information systems,
b- identifying roles and responsibilities of personnel,
c- an international body to identify minimum needs and give guidance to the lab structures,
d- performance tests and assessment of these laboratories,
e- disablement of data ports on machines with classified information,
f- Not relying only on security scanning tools to assess risks in computer systems, but, integrating the ‘human factor’ into the monitoring of the systems. The assessment tools have shown flaws. These tools are not sufficient to show correlation of threats that may increase risks and vulnerability. In other words, a computer asset might be low-risk by itself, but combined with other factors and assets, the risks of unauthorized access may rise.
g- ensuring timely-blocking of the systems after observing cyber vulnerabilities.
h- training technical experts in the nuclear-cyber field.

The addressed two measures—reduction of strategic and tactical nuclear weapons and cyber security in nuclear power plants, nuclear weapons laboratories and satellite systems are all linked to the third measure that I am going to discuss now.

3- De-alerting nuclear weapons is an important risk reduction measure
There are approximately 1,800 nuclear weapons in high-alert status today. These weapons serve for the existing military doctrines. Risks should be factored in military doctrines. De-alerting is not only a unilateral action; it could be undertaken in a multilateral setting.

---

5 Jamming is overpowering GPS satellite signals to a level that receiver cannot operate, and spoofing is sending false signals through different satellites and fools the receiver.
6 Hans M. Kristensen and Matthew McKinzie, Reducing Alert Rates of Nuclear Weapons, UNIDIR, January 2013.
An analysis of the risks and threats posed by high-alert nuclear weapons should include possible scenarios that could lead to nuclear weapons being detonated. Interim measures could include de-alerting nuclear weapons from one of the legs of the triad, at a time: ICBM’s or ballistic missile submarines; or it could include reduction of alert levels and let nuclear readiness to take longer time.

As stated earlier, maximizing time for decision-making is crucial in crisis situations. This takes me to the fourth point:

4. Pledge against nuclear tipped cruise missiles: use and possession

Cruise missiles (long-range standoff cruise missiles) increase the risks of accidental and unauthorized nuclear weapons use. William Perry and Andy Weber have started the debate about this issue. These missiles are destabilizers when used in any conflict. They increase uncertainty as the recipient country would not know the nature of the attack (whether a cruise missile actually has a nuclear warhead or it is a conventional attack?)

There are conventional missiles systems that could penetrate to other countries air defence, which is the main role of keeping these missiles. Similarly A2D2 operations do not need nuclear tipped cruise missiles as well.

Recent use of cruise missiles in Syrian conflict, indicate that these missiles are unreliable. Russia has launched 26 cruise missiles from Caspian Sea, in a single operation, and 4 of these missiles—as claimed—had failed to reach the targets and crashed on undesigned areas in Iran. Moreover, by avoiding radar systems, these missiles reduce time for decision-making; thus, increase pressure about the nature of the attack. Decrease nuclear threshold.

Conclusion:

There are other interim measures that could help reducing risks of nuclear weapons detonations.

Several measures, I believe, are harder to pursue due to domestic and bureaucratic challenges in nuclear weapons states. Eliminating modernization efforts, preventing the introduction of new nuclear systems and designs are some of the examples. Some are less political in essence, such as creating effective programs to direct nuclear scientists into new areas of research.

Within the existing status quo, nuclear weapons exist not to be used. As a result of the logic of “non-use”, decision makers do NOT consider the consequences of nuclear weapons detonations. Such consideration necessitates risk assessment.

Behavioral psychology shows that people are risk averse when they are shown the downside of the issue. If a person knows that there is high probability of losing all his savings in gambling, he/she is less likely to take that risk.

---

States behave the same way. They are risk prone when they think through the gains and forget about the consequences/costs.

It is important to know the consequences and risks associated with nuclear weapons detonations. As long as nuclear weapons exist, the risks of unauthorized, accidental, or deliberate detonations will remain. Until the total elimination of nuclear weapons, decision-making should focus on interim measures to reduce risks. This needs more than a commitment. It needs unilateral and multilateral actions.