

Working Group 2 – Arms Control

Chairs: Mona Dreicer (LLNL) and Martin Morgan- Reading (AWE)

Rapporteurs: Bonnie Canion (NNSA), Lance Garrison (NNSA), Peter Marleau (SNL)

In today's complex national security arena, there are no new arms control agreements that drive the development of concepts, approaches or technical capabilities for arms control verification. After a few decades of following the path set after the START Treaty, the research and development (R&D) community is ready to consider new approaches to achieve confidence in effective verification for possible future arms control commitments. This working group was organized around three key questions designed to structure the discussion, as follows:

- What technologies do we need?
- How do we protect sensitive information while providing access for verification?
- Is there a way to systematically assess the requirements and priorities that can focus future analysis and technology R&D?

Session A: Novel Technologies for Arms Control Verification

Moderator: Arden Dougan (NNSA)

While grappling with the fundamental question of *why develop methods and technologies when there is no treaty on the horizon*, the group agreed that if we waited, it could be too late to have the necessary approaches and tools required to effectively verify a treaty that protects national security equities. Without a treaty, there is time to define the problem and broadly identify verification capabilities so that we are prepared, if and when the need arises. Having a clear understanding of the capabilities could aid in the development of future national treaty negotiation positions.

One approach to predicting future treaty requirements is to extrapolate from the existing treaties, past negotiations, and technology trends, recognizing that treaty partners will participate in the development of the verification regime and technology choices. We believe that we can make reasonable assumptions allowing work to proceed towards predicted desired capabilities while being mindful of the pitfalls of extrapolating.

Confidence is derived from both the technology and concept of operations. In many cases the main challenges are not with the technical capabilities but in the non-functional aspects of utilization. For example, it is important to make sure that the technologies developed will eventually be fieldable. One danger is relying on a single solution to perform complete verification, rather the considering how an agglomeration of solutions might achieve the desired result. It was agreed that a defined and practiced systems engineering process could help—an approach based on novel engineering rather than novel technology. It is also important to consider the choreography required for realistic measurements – how sensitive are technologies to slight inconsistencies, such as position changes? Many of these issues are brought to light during exercises, which is one of the greatest values to practicing arms control scenarios.

Military and other communities use Capabilities-Based Assessments to provide a framework to support analysis and facilitate risk management when future requirements are unknown. These well-known techniques could be used to plan for unknown requirements of future treaties. Another common approach to fully understanding the risks is employing “red teams” to critically evaluate a planned regime.

In addition to discussing how to determine what technologies are needed the group did focus on what technologies might be needed. The title of the session generated discussion on the utility of the term “novel” technologies for arms control, so the group focused on possible: (a) new technology ideas, (b) existing verification technologies whose use is redefined, or (c) technologies used in another community repurposed for arms control purposes. It was noted that much could be learned from safeguards implementation as well as from revisiting older technologies taking into account evolutions and improvements in ancillary technologies (e.g. wireless communication).. Two specific technology options were presented:

(1) An established technique that could be re-engineered for arms control creates a template, which protects the release of sensitive information by a feature decomposition of a radiographic image to help address non-functional requirements (info protection, speed of data collection); and

(2) An instrument that verifies the separation of the high explosives (HE) from the fissile material (FM) in a device by looking at the ratio of slow neutrons to fast neutrons radiating from plutonium based weapons. By utilizing a ratio and never exposing the counts or count rate of the object to the inspector, sensitive design information remains secure while still allowing verification of dismantlement.

Session B: Balancing Transparency vs. Protection of Sensitive Information

Moderator: Keir Allen (Atomic Weapons Establishment)

Transparency and secrecy are two aspects of national security measures -- cooperative security versus competitive security. Overall, the discussions followed two important strands - technical and political. It is generally perceived that release of information increases confidence, however, the desired information and the levels of confidence required is dependent on the arms control objectives, political-military context, etc. In considering future agreements – we cannot simply apply today’s classification and security postures, but should assess which information could be most useful for future verification purposes (in relation to treaty aims). We discussed how three fundamental aspects of nuclear weapons information would likely be protected under all circumstances – design information, use control and any vulnerability concerns, but that many other forms of information could be available for consideration.

A good place to start is figuring out exactly what we need to protect, followed by what is needed for verification of commitments. Once this is identified, determining how to avoid sensitivities can be addressed. Two issues that complicate the sharing and handling of sensitive information are the differences in national classification rules and

that the agglomeration or additional context to unclassified information can result in higher classification levels. If sufficient confidence cannot be achieved using cooperative measures, confidence can be increased by the non-cooperative collection of monitoring information using National Technical Means.

Existing nuclear arms control agreements have largely been based on the number of delivery platforms, to which agreed numbers of warheads have been attributed. Future agreements may also consider counting or limiting the total number of nuclear weapons and warheads in the arsenals and would require new verification approaches (such as allowing for inspections of individual nuclear warheads in storage and warheads entering the dismantlement queue) without exposing the highly classified information to international inspectors. But will we really need to verify individual warheads? Some feel it's needed, and others believe that a rigorous operational verification approach doesn't require it.

The notion that sharing warhead information between NWS would be easier was not universally shared. NWS are in military competition so it is unlikely that those states would share information with competitors but not NNWS. In any case a formal process on the handling and transferring of sensitive or classified information will be a requirement, in particular for nuclear weapons information. Even though this will be difficult, there is precedence for transmission of classified information between states/treaty partners, including the IAEA. The UK-Norway cooperation on dismantlement verification has been useful in understanding how this type of interaction could be accomplished at an unclassified level between NWSs and NNWSs. It is likely that we could benefit from other communities that deal with information protection.

Systems-level approaches to gain confidence while protecting information could provide a structure to identify and assess information protection needs and take into account both "engineering confidence" and "regime confidence." A structured approach would identify the factors to be considered when capturing information to be released and assist in the identification of the risks. Then a systematic approach to mitigating the risk could be undertaken, including possible future technological advances (e.g. future-proofing). Red teaming and live exercises working on information protection technologies/techniques/CONOPS are essential for successful implementation. Furthermore, taking a systematic approach, and factoring in the lifetime of future agreements, can help ensure perspectives remain focused on strategic goals - multiple exercises in the past have lacked a clear strategic objective, which have severely impacted the information shared, the events of the exercise, the technologies deployed, the outcomes, and the perceptions of success or otherwise.

Technical solutions to protect information, such as designing information barriers into equipment and devising attribute and template mechanisms have been researched by the arms control verification community for decades. Templates are conceptually very useful but the challenge is operational since templates only work well if confidence is established in the template item itself. One potential concept of operations that was raised was allowing live-release (with no host redaction). This could cause the host to be more vigilant and inherently provide more confidence as the host is "at risk." Another

suggested approach, demonstrated in the UK-Norway initiative, was to have the host present to the inspector an array of possible avenues for inspection, instead of rejecting inspectors' ideas.

To advance the development of effective information protection, a unified mathematical framework could be developed, which would help identify strengths and weaknesses and help those communities in related fields contribute to the arms control application space. An upcoming workshop is being planned for 2016.

There are many lessons to be learned from the safeguards community. In Session A discussions, it was pointed out that safeguards may have relevant system level approaches that could be applicable to arms control. They also require state level confidence reporting. A couple of specific lessons that can be learned: use resolution as an information barrier (don't take more information than you need); and IAEA inspectors often have to draw conclusions at the site so that they don't take sensitive information out of a facility, which aids in sharing of sensitive information and confidence that information barriers cannot be spoofed.

Session C: Systems Concept to Arms Control Verification

Moderator: Cliff Chen (Lawrence Livermore National Laboratory)

The reduction or elimination of nuclear arms is not likely to occur absent a lower perceived need for a nuclear weapons arsenal and confidence that other states are upholding their commitments. Achieving confidence requires a coherent and comprehensive picture of the State's compliance with its obligations by piecing together, in a well-structured way, a broad range of information. Using the decades of experience of developing concepts and technologies for verifying bilateral and multilateral arms control agreements, a broad conceptual systems approach may help to take the varying levels of information and risk into account. Systems engineering can help to define a process, the inputs/outputs, and produce functional/non-functional requirements with full traceability. (e.g. such an approach is currently being applied in the UK.)

The first step in a systems engineering approach is to define the context diagram to set the boundary of the system and its environment and how the regime under consideration interacts with other aspects of a nation's security infrastructure. The requirements and design are set out in a traceable way followed by iterative stages of validation and verification to ensure consistency with customer needs and requirements. There was agreement that these models and exercises could not be used to predict the outcomes or what the next treaty will look like. Instead, the benefit of producing models and exercises is to prepare for the next treaty, ensuring we have the tools and the workforce to be effective. Because it is expensive to design, build and exercise a monitoring regime – the role for modeling and simulation might be significant. The group also discussed the potential usefulness of these models for sensitivity analyses.

Past workshops and meetings have shown that we can learn from the IAEA State Level Concept and multiple ongoing research projects in acquisition pathway analysis (APA). The first workshop was held in November 2014 in conjunction with the ESARDA VTM WG Meeting in Ispra, Italy. It focused on trying to identify and understand the acquisition pathways and the factors that influence pathway attractiveness. A second meeting was co-hosted by LLNL Center for Global Security Research (CGSR) in July 2015 to focus on identifying and prioritizing verification objectives based on a state's strategic interests and military capabilities.

The workshops involved a series of exercises for developing an APA-based systems concept for a treaty between two fictitious states. The exercises found that as APA is extended beyond the material enterprise, additional elements (research & development, human capital, enterprise capacity development, and detection of general enterprise activity patterns) need to be integrated into the overall analysis and may require an expanded framework. The most effective implementation of the systems concept required a close collaboration across diverse backgrounds and perspectives.

In one of the on-going research projects, APA was applied to identifying and prioritizing technically plausible cheating pathways. Pathway "attractiveness" was assessed based on intrinsic measures, such as technical difficulty, time and costs, but could also be estimated using extrinsic measures, such as detection probability and detection resource efficiency. In general, the definition of pathway "attractiveness" was described as crucial and complex.

EURATOM provided insights into their challenges and unique experience of implementing safeguards in both the NWS and NNWS of the European Union (EU), and of decommissioning installations in the EU NWS that were previously used for military purposes. With this background, EURATOM safeguards could contribute in the context of future disarmament or arms control agreements.

A new approach to enterprise monitoring was presented and discussed based on accepting items as warheads and monitoring their movements to identify patterns. Then anomalies to these patterns would be identified and investigated. Advantages and disadvantages of this approach were identified. Defined future work included consideration of the safeguards mailbox declarations and random inspections that could be used to augment the approach.

Next steps for applying the APA approach will be to focus on a few test cases, in order to validate the models - perhaps using real world data (e.g. North Korea, South Africa, JCPOA) and sensitivity analysis which would help identify how much different assumptions impact the final results.