Technologies and IPNDV Diversion Pathways

December 2025

Phase III of the International Partnership for Nuclear Disarmament Verification (IPNDV) considered verification aspects of both a reduction of nuclear warheads and limiting the number of nuclear warheads to a specific, agreed upon maximum limit.

In both cases, there is a risk that nuclear warheads are diverted from accountability under a treaty verification regime, thus leading to the state retaining more nuclear warheads than the treaty permits. Mitigating that risk requires robustness in terms of the processes, procedures, techniques and technologies employed by the verification regime.

The Technology Track explored the technological aspects of four different potential diversion pathways, shown below. All four cases enable a nuclear warhead to be diverted.

- Creating a simulated nuclear warhead in order to circumvent the verification regime and count such a simulated warhead as an accountable nuclear warhead.
- Disguising a nuclear warhead as a non-treaty accountable item by changing the defining characteristics of the item, for example by shielding radiation signatures.
- Tampering with radiation detection equipment; this is related to the previous case, but instead of evading the detection by shielding, the detection equipment itself is either altered or made to give false information by changing the environment (e.g., by surrounding radiation).
- Tampering with monitoring systems, such as portal monitors and/or closed-circuit television (CCTV). This is similar to the third case above, but because monitoring systems may be used when inspectors are not present, they are also potentially more vulnerable to tampering.

The cases above focus on different signal detection methods (including CCTV as an optical sensor), but the available verification technologies also include chain of custody measures. Using tamper indicating tags/seals and/or unique identifiers (UID) together with radiation detection technologies when warranted creates a two-layer system that reduces the attractiveness of diversion pathways.

In Table 1 below, we summarize the findings of the Technology Track with regard to technologies and diversion pathways trying to make use of the four scenarios described above. For each diversion pathway scenario, two columns show some of the more prominent challenges and opportunities to implementing the diversion. These two columns thus look at the diversion from two perspectives: technology aspects the inspecting party has to consider to reduce the probability of diversion, and from the host party side the opportunities for diversion that the verification and monitoring technologies offer. The last column offers some additional technical comments and clarifications for each scenario.

Finally, it should be underscored that the Technology Track has only considered the following technology aspects:

- The inspecting entity has an interest in minimizing diversion pathways, under the constraints of the regime and the resources available.
- The host party has an intention to divert nuclear warheads.

The considerations below do not take into account the presence or absence of such intentions.

Table 1. Technology Track Findings of Challenges and Opportunities to Detect Diversion

Diversion Category	Challenge to Implement Diversion	Opportunity to Implement Diversion	Notes
Simulating the Presence of a Nuclear Warhead	• Large effort, timeline, and logistics required to implement, which should be further complicated by the choice of monitoring and verification (M&V) technologies in the regime as noted below • Template should be robust to aging to protect against change in signatures due to material aging through the duration of the agreement or as otherwise stipulated • If golden template is spoofed, it requires all future measurements to be spoofed as well • Mimicking exact spectra, especially with attribute measurements is very challenging • Safety/security of special nuclear material limits options for diversion • M&V procedures: take background, make calibration, ensure algorithm is appropriate for respective stockpiles, etc.; collimation • M&V technology can anticipate potential diversions and be selected accordingly • Broader M&V regime (chain of custody, notifications, etc.) and treaty lifetime complicate long-term successful diversion	• Constraints within M&V procedures such as only from one orientation of TAI or material • Availability of relevant materials to simulate TAI (reactor grade plutonium) • Measurement tools may bin broad categories of spectra • If using a template approach, the golden template may be incorrect • Host has absolute knowledge of the agreed upon detector (hyperpure germanium vs. sodium iodide vs. cadmium zinc telluride) and can plan for diversion accordingly • Ability to alter environment, for example by interfering with measurements by including a radioactive source in the environment, or by otherwise making measurement conditions non-ideal (e.g., cluttered or high-background environment) • Large amounts of shielding could prevent inspectors from accurately measuring the signal of a TAI and potentially make it easier for a host to mimic	• Diversion is easier with highly enriched uranium (HEU) • If the simulating materials are only nuclear materials , the use of less such material (<200 grams compared to kilograms) in specific geometries could be difficult to distinguish from a nuclear warhead with passive techniques; this represents an opportunity for diversion • Risk of small diversions accumulating over time

Diversion Category	Challenge to Implement Diversion	Opportunity to Implement Diversion	Notes
Simulating the Absence of a Nuclear Warhead	• Significant shielding could impact other visible characteristics that would indicate if shielding is present • A neutron-based detection is more difficult to shield • There are ways to detect shielding (e.g., by observing that no higher energy gamma-ray peaks are in the spectra resulting from interactions between the shielding material and neutrons); this process can include other indicators such as mass and transmission measurement • Risk of failure—if there is a nuclear warhead present the inspector might obtain sensitive information • Incorporate agreements about maximum shielding constraints (with an impact on size and weight) into M&V regime • Consistent measurement location/repeatability can minimize ability to use environment to alter measurements • Host diversion could become more difficult the longer the treaty exists as inspectors become familiar with host logistics routines and whether or not these routines change over the treaty duration	• Gamma rays are easy to shield whereas neutrons are more challenging; thereby, HEU is easier to shield if passive gamma-ray methods are used • Shielding can be undetectable, especially if container design is not known and weight cannot be compared • Ability to alter environmental conditions to impact measurement	• To detect shielding, or its absence, neutron measurements could be complemented by gamma-ray spectroscopy • Gamma-ray detection needs to distinguish shielded HEU from, for example, low enriched uranium • It is important to distinguish neutron and gamma signatures indicating shielding from naturally occurring signatures due to presence of high explosives
Tampering with Radiation	• Procedures should limit flexibility to use ad hoc factors (e.g., the environment for	• Internet-connected or remotely operated equipment could make	• Data encryption can reduce tampering risk

Diversion Category	Challenge to Implement Diversion	Opportunity to Implement Diversion	Notes
Detection Equipment	neutrons); standardized measurement conditions help control the environment and avoid tampering risks • Tamper-indicating tags/seals could make tampering detectable and noticeable • Simple or familiar radiation detection technology and non-connected technology (not allowing wired or wireless connections) make tampering difficult • Nonprogrammable equipment can reduce risk of tampering • Functionality testing before each use will increase confidence in equipment integrity • Room sweeps and minimum background requirements can mitigate tampering via unknown external radiation sources • Equipment inspection, chain of custody, and procedures can mitigate risks of tampering • Robust data protection ensures that data are trusted by both parties and can make it more difficult for host to manipulate	tampering more possible (cybersecurity) • The probability of tampering increases if there is long-term unmonitored host access • Use of external unknown radioactive/neutron sources could alter information • Upgrading the firmware/software can put the equipment at risk of tampering	• Equipment should have minimum functionalities; more advanced systems can present more opportunities to disguise tampering and more challenges to discover tampering • When measuring a nuclear warhead, the shortest distance allowed should be used and collimated, and optimized detectors employed (e.g., to maximize detection efficiency to the desired direction)

Diversion Category	Challenge to Implement Diversion	Opportunity to Implement Diversion	Notes
Tampering with Monitoring Systems (portal monitoring, CCTV)	• Tamper-indicating tags/seals could make tampering with the monitoring system detectable and noticeable • Simple and familiar systems, especially non-connected (wire or wireless), make tampering more difficult • Variety of CCTV sensors available enable a layered system (video, infrared, etc.) that avoids a single point of failure • Equipment inspection, chain of custody, and procedures can mitigate risks of tampering • Robust data protection ensures that data are trusted by both parties and can make it more difficult for host to manipulate	• Digital and internet-connected equipment could make the tampering possible (cybersecurity) • CCTV often requires light, which can be manipulated by the host party • Cutting electricity can impact M&V regime • If conducting measurements while inspector is not present and handing off data, there is a risk of tampering with the shared data	• Data encryption can reduce tampering risk • Devices connected to internet can increase cybersecurity risk • Non-optical sensors in conjunction with or instead of optical can reduce impact of light (radar, thermal, lidar) • Uninterrupted power supply removes risk of tampering during electrical outage
Unique Identifiers (UIDs)	• Agreed procedure for issuing new UIDs and retiring old UIDs reduces likelihood of spoofing • Negotiated requirements for UID robustness can be specific to the amount of time UIDs will be in place on nuclear warheads • UIDs can be supported by additional regime requirements (measurements) in addition to maintaining a good history and robust metadata over the course of inspections (e.g., timestamps) increases confidence • Variety of technical UIDs available from simple to advanced (e.g., interferometry), which complicates spoofing requirements	• Advanced UIDs are a larger regime burden and simple UIDs are often prioritized • UIDs have a shelf life and will likely require replacement/updating • Detection range and shielding could prevent transmitting UIDs in automated systems • If UID replacement procedures are not negotiated, it presents an opportunity for diversion	• Data encryption can reduce tampering risk

Diversion Category	Challenge to Implement Diversion	Opportunity to Implement Diversion	Notes
	• UIDs can emit a status of health report to provide confidence in their functionality with no inspector present • Intrinsic and/or applied UIDs add to regime robustness • Robust data protection ensures that data are trusted by both parties and can make it more difficult for host to manipulate		

About IPNDV the International Partnership for Nuclear Disarmament Verification

The International Partnership for Nuclear Disarmament Verification (IPNDV) convenes countries with and without nuclear weapons to identify challenges associated with nuclear disarmament verification and develop potential procedures and technologies to address those challenges. The IPNDV was founded in 2014 by the U.S. Department of State and the Nuclear Threat Initiative. Learn more at www.ipndv.org.