SCIENCE & GLOBAL SECURITY
2021, VOL. 29, NO. 1, 1–2
https://doi.org/10.1080/08929882.2021.1943061

Routledge
Taylor & Francis Group

Editorial

This issue of *Science & Global Security* includes two articles shaped by concerns in nuclear weapons establishments about protecting information on warhead facilities, components, and designs during monitoring of nuclear warhead dismantlement as part of an arms reduction or disarmament treaty process. Both articles include authors from Britain's Atomic Weapons Establishment, Aldermaston.

Managing information during the verification of nuclear weapons dismantlement as part of achieving disarmament goals has been of long-standing concern in nuclear weapon states, and the journal has published earlier articles on this and related topics. A pioneering article in the very first issue of this journal noted that "All detailed information about the design of specific nuclear warheads is now classified. This includes yields and total weights; quantities of contained materials, including but not restricted to tritium, highly enriched uranium, and plutonium; and dimensions, configurations, and weights of fabricated components. … It is therefore assumed here that countries will be unwilling to reveal this information in the warhead dismantlement process" [Theodore B. Taylor, "Verified Elimination of Nuclear Warheads," *Science & Global Security*, 1, no. 1–2, (1989): 1–26.]. Recently, the application of cryptography to nuclear verification to help resolve information management issues has become of increasing interest [Sébastien Philippe, Alexander Glaser, Edward W. Felten, "A Cryptographic Escrow for Treaty Declarations and Step-by-step Verification," *Science & Global Security*, 27, no. 1 (2019): 3–14].

The use of cryptography for photographs taken during inspections is taken up in "Review and Redaction-Tolerant Image Verification Using Cryptographic Methods" by Robert J. Hughes. The article outlines cryptographic methods and approaches that could allow the host state to review any imagery taken during inspections and have confidence that "no sensitive information can be derived from the information and images given to the inspectors" while seeking to ensure that the host does not alter the images even during redaction to remove any sensitive information before releasing the images to inspectors. It demonstrates a simple example of the method using a DSLR camera and Raspberry Pi running a Python script to trigger the camera and calculate a hashed message digest of the image as it is saved to the camera. The inspectors could then compare this initial hash with that for the image once it is provided by the host. A partial redaction of the image by the host to remove or obscure something deemed sensitive would, however, lead to a different message digest that could not be the same as the digests produced during the inspection. This problem is resolved using a more complex but familiar cryptographic method for confirming that a portion of data is actually a genuine part of a larger data set.

The second article expands the scope of concern about information management to the dismantlement facility level. A classified US study, the "Final Report on Field Test 34 on the Demonstrated Destruction of Nuclear Warheads" (1969) sought to assess what might be learned by inspectors about weapon-design information in the effort to verify that real warheads were being dismantled. A summary of this report after declassification published in this journal noted that "One of the conclusions drawn

from the project was that, if the US actually undertook to dismantle warheads in a verifiable manner, this should be done at a specially designed integrated facility. In such a case, the exposure of classified information could be much reduced." [Frank von Hippel, "The 1969 ACDA Study on Warhead Dismantlement," *Science & Global Security*, 2, no. 1, (1990): 103–108.]

This issue is revisited by a team from the Swedish Defence Research Agency, Stockholm, and the UK Atomic Weapons Establishment at Aldermaston, in "Verified Nuclear Warhead Dismantlement: An Analysis and Methodology for Facility Assessment" (Anders Axelsson, Jennifer Schofield, Daniel Sunhede, Nicholas J. Thompson, Ian Laurie, Katarina Wilhelmsen, and Benjamin Carter). By taking a systems engineering approach to "verification issues and challenges such as protection of information and safety and security," the analysis concludes that a new dedicated dismantlement facility is not after all the best option and that an "existing nuclear warhead facility not currently in use for active-stockpile work" would better serve as the site for verified nuclear warhead dismantlement. This finding would imply that in a treaty that required elimination of all nuclear weapons (such as the new Treaty on the Prohibition of Nuclear Weapons) where there would be no work to maintain nuclear weapons, then current nuclear weapon assembly/disassembly facilities could best meet the need for sites for verified warhead dismantlement.