SCIENCE & GLOBAL SECURITY
2020, VOL. 28, NO. 1, 1
https://doi.org/10.1080/08929882.2020.1737419

Routledge
Taylor & Francis Group

EDITORS' NOTE

This issue of *Science & Global Security* is made up of articles applying ideas about securing, collecting, storing and processing data to three critical nuclear issues. The articles cover the vulnerabilities to cyber-threats of U.S. nuclear-armed intercontinental ballistic missiles and potentially those of other nuclear-armed states as these systems undergo modernization; the need to improve the reliability of detecting nuclear weapons, weapon materials, and radioactive materials that might be hidden inside global shipping containers transported through ports around the world; the challenge of protecting nuclear weapons information which some states might insist on treating as sensitive as warheads are authenticated during a process of verified disarmament.

Assessing Priorities toward Achieving Dependable and Secure Computing in the U.S. ICBM Force by Lauren J. Borja offers a first principles assessment of cybersecurity for the more than 400 U.S. land-based nuclear-armed intercontinental ballistic missiles which are slated to be modernized over the next several decades. The article applies core ideas from computer security, dependable computing, and systems analysis to explore the types of vulnerabilities that may be at play and which may emerge as the system is modernized. It highlights the need to reconsider U.S nuclear weapons policies that potentially further add to these cybersecurity vulnerabilities and increase the risks of accidental or inadvertent nuclear weapons use.

The article *Data Science in Support of Radiation Detection for Border Monitoring: An Exploratory Study* by Christopher Hobbs, Peter McBurney and Dominic Oliver offers the beginning of a new approach to speed up the process of identifying shipping containers bearing naturally occurring radioactive materials which produce false alarms each day at radiation portal monitors installed at many ports around the world. Using a data set from portal monitors in three countries, the article uses data science techniques to look at the radiation profile generated by containers which set off alarms as containers pass through these portals to show that it is possible to characterize and identify containers carrying common radioactive materials. This may reduce the amount of time it takes to investigate and resolve false alarms.

The third article in the issue is *Physical Public Templates for Nuclear Warhead Verification* by Alexander Glaser, Boaz Barak, Moritz Kütt, and Sebastien Philippe. The authentication of electronic hardware and software used for national security related data storage and processing is always difficult. It can be an especially serious concern in a nuclear weapons inspection that is part of a treaty arrangement if there are suspicions on either side about efforts to subvert the inspection. This article offers two new ideas for how to protect the potentially sensitive gamma spectrum from a nuclear warhead collected as part of a treaty-mandated inspection. First, it suggests moving to a non-digital data storage media and explores the case of traditional punch cards to store the data, which is released as a cryptographic hash. Second, it suggests a non-digital method to partially release this data by using masks that can be placed on top of the punched card to release selective bits as required. The concept is demonstrated using a sample gamma radiation spectrum from a 4.5-kilogram solid plutonium ball measured at the U.S. National Nuclear Security Administration's Device Assembly Facility.