Abstract

Academics disagree on the risk of VNSAs being able to build or acquire CBRN weapons. Their analysis is based on motivation, geographical factors, potential targets, and VNSA group attributes. Missing is the detailed investigation of how and where a VNSA obtains the necessary precursor materials and the type of security surrounding common materials used for CBRN weapons. This paper will explore the possible routes an actor could take to acquire the knowledge, skills, and materials necessary to make an operable CBRN weapon.

Case studies are used to show past routes that allowed VNSAs to achieve capability and the type of weapon and attack utilized. The implementation of regulations, both in response to CBRN attacks and their effectiveness in preventing VNSA CBRN weapon capability, are analyzed. Public online forums, weapons manuals and weapons research along with past prosecuted criminal CBRN attacks revealed the financial capacity needed to acquire materials as well as the technical capacity required to build a successful CBRN system. Existing databases logging insecurity in nuclear facilities, radioisotope thefts, chemical and biological incidents and more are used to establish trends among past and present pursuits and use of CBRN weapons.

Viable routes to CBRN capability remain reenforcing the high-risk level of VNSA ability to achieve general CBRN capability. The risk level of VNSAs achieving government equivalent CBRN capabilities is low. Technology and globalization have closed the gap between access to materials and knowledge on building homemade weapon systems. Security is ineffective around some of the world's most dangerous weapons materials and the proliferation of information allows for any VNSA to gain enough knowledge to produce a crude CBRN weapon. In most cases, personal production of agents or lack of access to sophisticated lab equipment impedes the production of highly effective CBRN weapons.

Identifying the commercial paths or unregulated materials open for exploitation by VNSAs will aid in the prevention and deterrence of VNSAs becoming CBRN capable. Motivations and organizational structures of VNSAs can shift unexpectedly and if internal vulnerabilities are not addressed an attack would be unpredictable and unpreventable. Nonproliferation measures work but they need to be addressed and enacted now while the risk assessment is relatively low.