Journal of Strategic Security

Volume 9
Number 1 *Volume 9, No. 1, Special Issue Spring 2016: Designing Danger: Complex Engineering by Violent Non-State Actors*

Article 2

Foreword to the Special Issue on Complex Engineering by Violent Non-State Actors

Jez Littlewood
Assistant Professor, Norman Paterson School of International Affairs (NPSIA), Carleton University, Canada

pp. i-iii

Foreword

Violent Non-State Actors (VNSAs) such as terrorists, gangs, transnational criminal organizations, and insurgents pose a range of different threats to states and to international peace and security. Few such actors are truly global in nature–by reach or influence–just as few states have global capabilities. But many VNSAs are also not simply local or national, as illustrated by the case studies in this edited collection. At the same time commentary and reportage on VNSAs tends toward simple dichotomous assessments of them being either low-level, relatively unsophisticated, and localized threats, or being endowed with capabilities that rival states or fictional supervillains that are able to develop or produce weapons capable of achieving mass destruction.

In an era of the super-empowered individual and networks of organizations with access to information technology, knowledge, and materials to pursue and fulfil their objectives, it is tempting to endow all such actors with the potential to supplant the state and its legitimate authority. Yet, states endure, and even failed and failing states are rarely destroyed or replaced by VNSAs. States are not always, however, the only or most powerful actors in any given locale or region. Why and how different VNSAs remain low-level and localized or undertake and achieve complex engineering tasks in pursuit of their objectives are at the heart of understanding the threat environment faced by states.

This special edition makes an important contribution to our understanding of VNSAs and complex engineering in a number of ways. First, it takes a wider assessment of VNSAs to incorporate more traditional terrorist groups such as the Provisional Irish Republican Army (PIRA), millenarian cults that turn to terrorism such as Aum Shinrikyo, a terrorist-insurgent force that evolved into a terrorist-criminal actor such as the Fuerzas Armaadas Revolucionarias Colombia (FARC), a listed terrorist entity that holds and administers internationally recognized territory (HAMAS), a transnational criminal organization and infamous drug cartel (Los Zetas), and the network behind some of the more complex proliferation of nuclear weapons material and components (A Q Khan Network). Each actor could be studied by type–terrorist, insurgency, crime–yet as Ackerman notes in the introduction, the respective literatures on terrorism, insurgency, and organized crime to date have not directed studies specifically towards complex engineering issues undertaken by such groups. Technology adoption by terrorist groups is perhaps the richest vein of literature to date, but even that is merely

emerging, as opposed to being accepted and widely adopted. The wide assessment herein is, therefore, a contribution that should appeal to and enrich terrorism studies, criminology, science and technology studies, and the civil war and insurgency literature. It also has clear implications for intelligence studies and security studies more broadly.

Second, the approach of this collection moves beyond weapons and embraces facilitating or logistical aspects that support the operations and objectives of the various actors. While both conventional weapons (PIRA's mortars) and unconventional weapons (Aum's nuclear and chemical weapons exploits and the A.Q. Khan proliferation activity) are addressed here, the use of submersibles and submarines to transport narcotics, of secure radio and communication networks to coordinate and communicate within a large complex organization, and the development of a tunnel network in an urban environment to trade and traffic materials, equipment, and personnel illustrate the diversity of activity that can be undertaken by VNSAs. Each, as Ackerman and respective authors note, requires technical and engineering expertise, expert personnel, organizational support, and resources to complete, in addition to a willingness to overcome or circumvent numerous obstacles to success.

Third, this collection offers a structured comparison of different types of activity among diverse organizations, geographically dispersed and covering the last four decades. The avoidance of overly similar cases allows the authors and the editor to identify similarities and differences between and among cases. As the comparative analysis underlines, the ability of any VNSA to invest substantial resources, acquire or attain the necessary technical expertise, conduct such activity under pressure and in a relatively safe haven, and imbue within the organization a culture of learning relies upon multiple factors that cut across organizational structure and leadership, geography, time, availability of materials, the very culture of the actor and its constituents, and the environment in which the VNSA operates. Here then is the clear evidence that not all VNSAs can undertake such tasks, but some certainly can and have done so. The objective of the collection in its simplest form–giving 'pause to those who too easily dismiss the potential threats posed by non-state actors'–is therefore achieved with aplomb.

The final contribution of the collection of articles herein lies in its policy-relevance. The differences and similarities among the cases all point to the need for good intelligence and situational awareness. At one level, some significant issues matter: Resource availability, size, and composition of the

http://scholarcommons.usf.edu/jss/vol9/iss1/2
DOI: http://dx.doi.org/10.5038/1944-0472.9.1.1515

organization, and strategy and tactics of the entity. At another level, more granular level information such as attitudes of the leadership toward innovation, aversion to risk and/or failure, and the specific technical and engineering expertise required to fulfil the task. The implications of this reinforce effective practices of good intelligence such as situational awareness, information sharing, all-source analysis, and the ability to detect the unusual and consider its implications. Awareness may not be able to prevent the completion of complex engineering tasks, but it should certainly permit a countering force to make that task more difficult through the identification and manipulation of choke points, development of additional obstacles for the VNSA–resources, materials, personnel, risk of detection–and making the overall operational environment more conducive to the tactical failure of the undertaking and/or weapon for the VNSA.

Overall this special edition of the journal builds upon and expands existing literature and studies and undertakes scholarly enquiry in a comparative manner on divergent issues. At the heart of this is not weapons or logistics, organizations, or cultures, but the confluence of numerous factors that can, and arguably must, come together for a VNSA to undertake and complete complex engineering activities. By increasing our awareness of these issues, the foundation is laid for more sustained inquiry, further research, and a re-evaluation of the questions we should be asking vis-à-vis the interests and capabilities of Violent Non-State Actors and the threats such actors pose.