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 3

"Designing Danger": Complex Engineering by Violent Non-State Actors: Introduction to the Special Issue

Gary A. Ackerman
START Center, University of Maryland, ackerman@umd.edu

pp. 1-11

Recommended Citation
Ackerman, Gary A.. "“Designing Danger”: Complex Engineering by Violent Non-State Actors: Introduction to the Special Issue." *Journal of Strategic Security* 9, no. 1 (2016): : 1-11.
DOI: http://dx.doi.org/10.5038/1944-0472.9.1.1502
Available at: https://scholarcommons.usf.edu/jss/vol9/iss1/3

“Designing Danger”: Complex Engineering by Violent Non-State Actors: Introduction to the Special Issue

Author Biography

Dr. Gary A. Ackerman is the Director of the Unconventional Weapons and Technology Division at the National Consortium for the Study of Terrorism and Responses to Terrorism (START). Prior to taking up his current position, he was Research and Special Projects Director at START and before that the Director of the Weapons of Mass Destruction Terrorism Research Program at the Center for Nonproliferation Studies in Monterey, California. His research encompasses various areas relating to terrorism and counterterrorism, including terrorist threat assessment, radicalization, terrorist technologies and motivations for using chemical, biological, radiological, and nuclear (CBRN) weapons, and the modeling and simulation of terrorist behavior. He is the co-editor of Jihadists and Weapons of Mass Destruction (CRC Press, 2009), author of several articles on CBRN terrorism and has testified on terrorist motivations for using nuclear weapons before the Senate Committee on Homeland Security. He completed his PhD in War Studies at King’s College London, dealing with the impact of emerging technologies on terrorist decisions relating to weapons adoption.

Abstract

This Special Issue of the *Journal of Strategic Security* (JSS) presents the results of a series of case studies of prior efforts by VNSAs to engage in complex engineering tasks, in the hope of informing strategic assessments of the threat of VNSA exploitation of emerging technologies.

One particular concern in international security lies at the nexus of violent non-state actors (VNSAs) and sophisticated technologies. When it comes to the assessment of such threats, much of the analysis hinges upon being able to accurately judge the desire and capability of adversaries to successfully carry out complex engineering operations. Yet, the actual process of how and why VNSAs engage in these efforts and the determinants of their success or failure are understudied aspects, at least in terms of systematic comparison across actors, technologies and time periods. This special issue presents the results of a series of case studies of prior efforts by VNSAs to engage in complex engineering tasks, in the hope of informing strategic assessments of the threat of VNSA exploitation of emerging technologies. The introductory article defines a complex engineering effort, summarizes the existing literature on the topic and sets out the methodology and framing questions used in the case studies.

Disclaimer

Editor's Note: This article forms part of a series of related case studies collected in this Special Issue and should be viewed in the context of the broader phenomenon of complex engineering by violent non-state actors. Readers are advised to consult the introductory and concluding papers for a full explanation and comparative analysis of the cases.

Acknowledgements

This work was supported by Sandia National Laboratories, Contract #1525332. Any opinions, findings, conclusions and recommendations in this issue are those of the authors and do not necessarily reflect views of Sandia National Laboratories or the U.S. Department of Energy.

Introduction

Among the many global dynamics rising to the fore in the 21st century, two of the most prominent are the growth in the systemic influence of terrorists and other violent non-state actors (VNSAs), and the advent of a range of transformational technologies. In the context of international security, there is particular concern with respect to the nexus of these two forces, where it is feared that VNSAs might adopt emerging technologies, such as synthetic biology or quantum computing, to magnify the threat that they pose.

On the one hand, it is tempting to inflate the threat, painting VNSAs as Bondian-supervillians capable of casually constructing doomsday weapons, while ignoring the multiple hurdles inherent in such enterprises and the empirical fact that in the past most VNSAs most of the time have shown themselves to be conservative and imitative rather than innovative in their tactics and weapons.[1] On the other hand, it may be even more hazardous to assume that VNSAs will never be able to successfully adopt new technologies, when there exist several historical examples of VNSAs doing just that.

While a large part of the security concern lies in the fact that many emerging technologies render it easier, safer and less costly for non-experts to adopt new weapons and tactics,[2] for several prominent threats—especially those stemming from the potential VNSA use of so-called "weapons of mass destruction"—the process of adoption and deployment as a whole still requires a complex application of knowledge and materials in a practical context. Thus, when it comes to the assessment of such threats, much of the analysis hinges upon being able to accurately judge the desire and capability of adversaries to successfully carry out complex engineering operations.

Yet, the actual process of how and why VNSAs engage in these efforts and the determinants of their success or failure are understudied aspects, at least in terms of systematic comparison across actors, technologies and time periods. A team of researchers at the National Consortium for the Study of Terrorism

---

[1] Jenkins, Brian, "Defense Against Terrorism," *Political Science Quarterly 101, Reflections on Providing for "The Common Good,"* 101:5 (1986), 777-778; Hoffman, Bruce, *Terrorist Targeting: Tactics, Trends, and Potentialities* (Santa Monica, California: RAND, 1992), 15; Dolnik, Adam, *Understanding Terrorist Innovation: Technology, tactics and global trends* (New York: Routledge, 2007), 56.
[2] Ackerman, Gary, "'More Bang for the Buck': Examining the Determinants of Terrorist Adoption of New Weapons Technologies" (PhD Dissertation: King's College London, 2014), 23, available at: *https://kclpure.kcl.ac.uk/portal/files/32901277/2014_Ackerman_Gary_0715371_ethesis.pdf*.

and Responses to Terrorism (START) therefore came together with the objective of deriving insights regarding the dynamics and outcomes of complex engineering efforts undertaken by VNSAs. This special issue presents the results of a series of case studies of prior efforts by VNSAs to engage in complex engineering tasks, in the hope of informing strategic assessments of the threat of VNSA exploitation of emerging technologies.

Before proceeding, it is necessary to define a complex engineering effort, as undertaken by a VNSA. Thus, for the purposes of this volume, a complex engineering effort by a VNSA is one that involves:

- Multiple components (sub-tasks) of different types (e.g., mechanical, chemical, machining) that must integrate properly in order for the effort to succeed;
- The manpower of more than just one person;[3]
- A variety of technical skills (such as chemical synthesis, welding, or electronics); and
- A more sophisticated effort than standard operations for the context (time and place) in which the VNSA is operating.

Framing the Study[4]

There has been almost no discussion in the terrorism,[5] insurgency or organized crime literatures that is specifically directed towards complex

[3] Complexity usually implies an interaction of multiple parts and, since we are focused here on VNSA organizations rather than lone actors, we restrict the definition of a complex engineering effort to one involving multiple people. It is partly the very requirement for different individuals within an organization to cooperate and integrate their activities in order to achieve a common goal that makes a particular task "complex" in this sense. Therefore, no matter how ingenious and versatile a particular single member is, their individual efforts, at least in the current instance, can be complicated, but not complex.

[4] The author would like to acknowledge the efforts of Daniel Smith, James Halverson, Molly MacCalman and Michelle Jacome in assisting him in assembling a broad literature review from which this section is drawn.

[5] Without wanting to enter the definitional fray surrounding terrorism, in this issue the term is used in the sense of "The intentional use or threatened use of violence by an ideologically motivated non-state actor in a manner that would be regarded in wartime as contravening international humanitarian law and that is directed against victims selected for their symbolic or representative value, as a means of instilling anxiety in, transmitting one or more messages to, and thereby manipulating the attitudes and behavior of a wider target audience or audiences"—based on the definition espoused by Jeffrey Bale. See Gary Ackerman, et. al., *Assessing Terrorist Motivations for Attacking Critical Infrastructure*,

https://scholarcommons.usf.edu/jss/vol9/iss1/3
DOI: http://dx.doi.org/10.5038/1944-0472.9.1.1502

engineering efforts by VNSAs, as here defined. However, there is a fair amount of material on both related superordinate and subordinate topics. In a broader sense, a complex engineering effort in the VNSA context will almost always represent a qualitative departure from the status quo operating posture for a particular VNSA, since it is rare (except perhaps in the case of sophisticated IEDs for some rebel groups in places like Iraq) for a VNSA to have "industrialized" its logistical or weapons acquisition systems to the extent that complex efforts become merely incremental changes to a long-standing standard operating procedure. Therefore, complex engineering efforts can usually be situated within the wider topic of VNSA innovation, about which there is a growing literature.[6] Nonetheless, only a subset of VNSA innovations will qualify as complex engineering efforts. Therefore, the extent to which more general findings about VNSA learning and innovation apply to the specific situation of complex engineering efforts, or whether additional dynamics might characterize these efforts, is still an open question.

Similarly, one subset of complex engineering efforts by VNSAs—the potential for them to produce their own high-level chemical, biological, radiological and nuclear (CBRN) weapons—has been extensively discussed,[7] especially in the case of improvised nuclear devices.[8] Yet, this literature has largely focused on

---

Report for Lawrence Livermore National Laboratory for the Department of Homeland Security (Monterey, California: Monterey Institute of International Studies, 2004), available at https://e-reports-ext.llnl.gov/pdf/341566.pdf, 10 January 2010, p. 15 (ftn 51).

[6] Ranstorp, Magnus and Magnus Normark (eds.), *Understanding Terrorism Innovation and Learning: Al-Qaeda and Beyond*, (New York: Routledge, 2015); Dolnik, *Understanding Terrorist Innovation*; Rasmussen, Maria J. and Mohamed Hafez (eds.) *Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators* (Defense Threat Reduction Agency, Advanced Systems and Concepts Office, Report Number ASCO 2010-019, 2010), 18, available at: *https://www.hsdl.org/?view&did=9908*; Jackson, Brian A. et al., *Aptitude for Destruction-Vol. 1. Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism* (Santa Monica: RAND, 2007); Gill, Paul, John Horgan, Samuel T. Hunter and Lily D. Cushenbery, "Malevolent creativity in terrorist organizations", *Journal of Creative Behavior* 47:2 (2013), 125-151; and Kenney, Michael, *From Pablo to Osama* (University Park, PA: Penn State University Press, 2008).

[7] See, for example: Waller, Jr., Forest E. and Michael A. George, "Emerging WMD Technologies," in Russell D. Howard and James J.F. Forest (eds.), *Weapons of Mass Destruction and Terrorism* (New York: McGraw-Hill, 2008), 499-511; Bunn, Matthew, "Guardians at the Gates of Hell" (PhD dissertation: Massachusetts Institute of Technology, 2007); Koblentz, Gregory D., *Living Weapons: Biological Warfare and International Security* (Ithaca: Cornell University Press, 2011); and Smithson, Amy E., "Indicators of Chemical Terrorism" in Ranstorp and Normark (eds.), *Unconventional Weapons and International Terrorism*, 67-94.

[8] Ferguson, Charles D. and William Potter, et. al., *The Four Faces of Nuclear Terrorism* (New York: Routledge, 2005); Levi, Michael, *On Nuclear Terrorism* (Cambridge, MA: Harvard University Press, 2007); and Jenkins, Brian Michael, *Will Terrorists Go Nuclear?* (Amherst, NY: Prometheus Books, 2008).

the narrow technical requirements of the specific weapon type under consideration, with little reference to whether these requirements extend to the topic of complex engineering efforts outside the CBRN realm or to novel, emerging technologies. The decision making and requirements surrounding the construction of as unique a weapon as an improvised nuclear device might very well be *sui generis* and less applicable to other complex engineering efforts.

Therefore, while existing scholarship can provide a guide for understanding complex engineering efforts by VNSAs, there is still a gap in the understanding of exactly which of the many factors and dynamics identified in the literature on VNSA innovation and WMD development apply in the case of complex engineering efforts, how strongly they act on the process, and whether there are certain factors that become especially salient in the context of complex engineering efforts.

In order to inform our exploration of the topic, we drew on the existing literature described above as a source of insights that might be relevant to investigating VNSA complex engineering efforts, focusing on those that seem most appropriate to the current topic. It should be noted that this is a preliminary investigation and we are not at this stage laying out or formally testing hypotheses. Rather, we seek to identify potentially salient factors and dynamics that can be formally validated by further research. Among the key theories and findings from the broader literature that guided our examination of VNSA complex engineering efforts were the following:

1. The process of decision making surrounding VNSA technology adoption is *equifinite*. In other words, there is no single (and not necessarily even a predominant) causal path to deciding to adopt, say, a new weapon.[9]

2. Major identified drivers of VNSA innovation in general and the pursuit of WMD in particular include: countermeasures imposed by opponents;[10] desensitization of the target public or the intended constituency;[11] a desire for greater status either within the VNSA,

[9] Ackerman, 'More Bang for the Buck', 219.
[10] Dolnik, *Understanding Terrorist Innovation,* 153; Hoffman, Bruce, *Inside Terrorism* (New York: Columbia University Press, 2006), 252, Jackson, et al., *Aptitude for Destruction,* 19.
[11] Schmid, Alex P. and Janny de Graaf, *Violence as Communication: Insurgent Terrorism and the Western News Media* (Beverly Hills, CA: Sage Publications, 1982), 172.

https://scholarcommons.usf.edu/jss/vol9/iss1/3
DOI: http://dx.doi.org/10.5038/1944-0472.9.1.1502

relative to other VNSAs, or as an actor on the world stage;[12] and an ideological or psychological need on the part of leaders to engage in technologically sophisticated operations (sometimes referred to as "techno-fetishism").[13]

3. The decision to innovate and/or the process itself can be facilitated by: champions either within or outside the VNSA,[14] demonstration of the technology by[15] and collaboration[16] with other VNSAs (especially those within the same social network); a willingness to learn and experiment;[17] and an overall organizational tolerance for taking risks.[18]

4. Having a separate, institutionalized "engineering" or R&D organ within the organization[19] and a safe haven[20] are important factors in both a positive decision to innovate and the ultimate success of innovation adoption attempts. Conversely, intra-organizational discord[21] and pressures from security forces can impede adoption efforts.[22]

5. Some technology development efforts can take on their own momentum within an organization, as vested interests for the effort develop.[23]

---

[12] Ferguson, Charles D. and William C. Potter, *Improvised Nuclear Devices and Nuclear Terrorism* (Stockholm, Sweden: Weapons of Mass Destruction Commission, 2006), 6.
[13] Jeffrey M. Bale and Gary A. Ackerman, "Profiling the WMD Terrorist Threat" in Stephen M. Maurer (ed.), *WMD Terrorism: Science and Policy Choices* (Cambridge, MA: MIT Press, 2009); Ronfeldt, David and William Sater. *The Mindsets of High-Technology Terrorists: Future Implications from an Historical Analog* (Santa Monica, CA: RAND, 1981), 15, 27; Jackson, Brian A., "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict and Terrorism*, 24:3 (2001), 193; Rasmussen and Hafez, *Terrorist Innovations in Weapons of Mass Effect,* 18.
[14] Ackerman, 'More Bang for the Buck," 52, 93.
[15] Ibid., 106.
[16] Hargadon, Andrew. 2003. *How Breakthroughs Happen: The Surprising Truth about How Companies Innovate* (Boston: Harvard Business School Publishing, 2003), ix, 60.
[17] Jackson, *Aptitude for Destruction*, 46; Rasmussen and Hafez, *Terrorist Innovations in Weapons of Mass Effect*, 3.
[18] Jackson et. al., *Aptitude for Destruction*, 46; Dolnik, *Understanding Terrorist Innovation*, 167.
[19] Jackson et. al., *Aptitude for Destruction*, 46; Ackerman, 'More Bang for the Buck', 240.
[20] Jackson, et. al., *Aptitude for Destruction,* 43.
[21] Ackerman, 'More Bang for the Buck', 150.
[22] Jackson, et. al., *Aptitude for Destruction,* 57.
[23] MacKenzie, Donald, *Essays on Technical Change* (Cambridge: MIT Press, 1996), 58.

6. With respect to obtaining the requisite expertise for innovation, the literature suggests that VNSAs do not necessarily require members with outstanding technical expertise, but instead a membership that is stable, proficient in analyzing existing methods and resources, and can reconfigure these to meet an organization's goals.[24]

7. While VNSAs may vary considerably with respect to the value they place on the safety and security of members involved in innovation efforts, key members with technical skills and experience will generally be protected, as their loss can severely diminish a group's capabilities.[25]

One feature of existing scholarship is copious discussion of the different pathways by which VNSAs could acquire a WMD capability, such as by theft, transfer from a patron, or purchase on a putative black market. However, in the current context of complex engineering efforts by VNSAs, by definition we presume that the bulk of the adoption process consists of internal development activities carried out by group members, with perhaps only raw materials or equipment being procured through other means. Furthermore, the existing literature says relatively little about the process by which a complex engineering task is implemented, other than to prescribe acquiring the necessary knowledge and skills, ensuring adequate funding, equipment and materials, and establishing a development site. There was therefore particular emphasis placed in the current study on the implementation aspects of complex engineering efforts.

The collective insights extracted from related literatures thus led the research team to adopt the following framing questions to shape its exploration of complex engineering efforts by VNSAs:

- What drives VNSAs to undertake complex engineering tasks?
- Who makes decisions and what is the role of risk perceptions?
- How is the relevant expertise required?
- How are the security and safety of the effort ensured?

[24] Rasmussen and Hafez, *Terrorist Innovations in Weapons of Mass Effect,* 2; Jackson, et. al., *Aptitude for Destruction,* 48.
[25] Jackson, "Technology Acquisition by Terrorist Groups", 194.

https://scholarcommons.usf.edu/jss/vol9/iss1/3
DOI: http://dx.doi.org/10.5038/1944-0472.9.1.1502

- How are obstacles dealt with?

- Why do these attempts either succeed or fail?

Methodology

Given that there is little to no prior research on complex engineering efforts by VNSAs, it is appropriate to examine the topic in an exploratory fashion.[26] This approach places less emphasis on controlling for certain variables or comparing both positive and negative cases, as would be necessary if the objective was to test an existing theory. Therefore, in order to gain from our preliminary analysis as much direction as possible regarding where to steer future research, we focused on those cases where complex engineering tasks had at least been attempted, leaving more complicated comparative analyses[27] to later studies. Similarly, we sought to gain as much variety in temporal, geographic and cultural context between cases as possible, in order to more easily and accurately identify organizational factors fundamentally associated with the decision to engage in complex engineering tasks and the successful completion of such tasks.

To select cases, we therefore sought instances that met the following criteria: a) the activity undertaken by the VNSA must qualify as a complex engineering effort, as defined above; b) cases that showed variety in terms of the context in which they occurred and the activity engaged in; and c) for practical purposes, cases for which sufficient data existed in the open sources to allow for a detailed description of the dynamics involved. An initial survey of available literature and databases yielded 22 candidate cases, as listed chronologically in Table 1.1.

[26] George, Alexander L. and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge, Mass.: MIT Press, 2005), 20-22, 45
[27] These include controlled comparison, congruence procedures and process tracing – see Van Evera, Stephen, *Guide to Methods for Students of Political Science* (Ithaca: Cornell University Press, 1997), 56-67.

Table 1.1 Complex Engineering by VNSAs – Candidate Cases

Candidate Case (VNSA – Engineering Effort)	Extent to which CEE	Outcome[28]	Adversary Type	Time Period	Region	Data Availability
ETA (Basque separatists) – Remote-controlled Car	4	*Apocryphal*	Terrorist	N/A	Europe	N/A
Anarchists – Dynamite Weapons	2	Success	Terrorist	1880s-1900s	Europe	Yes
Ahmed Jibril (Popular Front for the Liberation of Palestine) – Barometric Pressure Bombs	3	Success	Terrorist	1960s-1970s	Middle East; Europe	Yes
Provisional IRA – Mortar system	4	Success	Terrorist	1970s-1990s	Europe	Yes
Rajneeshees – Biological Weapons	2	Success	Terrorist / Cult	1980s	N. America	Yes
LTTE (Tamil Tigers) – Fast Attack boats	3	Success	Terrorist	1980s-2000s	Asia	Yes
Aum Shinrikyo – Biological Weapons	5	Failure	Terrorist / Cult	1990s	Asia	Yes
Aum Shinrikyo – Nuclear Weapons	5	Failure	Terrorist / Cult	1990s	Asia	Yes
Aum Shinrikyo – Chemical Weapons	4	Success	Terrorist / Cult	1990s	Asia	Yes
Ramzi Yousef – Sophisticated Liquid Explosive Devices	3	Success	Terrorist	1990s	N. America; Asia	Partial
Al-Qaida – Chem / Bio Weapons	2	Failure	Terrorist	1990s-2000s	Middle East; Asia	Yes
Al-Qaida – Nuclear Weapons	5	Failure	Terrorist	1990s-2000s	Middle East; Asia	Partial
FARC – Submersibles	5	Success	Terrorist / TCO[29]	1990s-Present	South America	Yes
Hamas – Tunnels	4	Success	Terrorist	2000s	Middle East	Yes
Hezbollah – Guidance System	4	Success	Terrorist	2000s	Middle East	No
Hezbollah – Unmanned Aerial Vehicles	4	Success	Terrorist	2000s	Middle East	No
AL-Qaida in the Arabian Peninsula – Printer Cartridge Bomb	3	Success	Terrorist	2000s	Middle East	Yes
AL-Qaida in the Arabian Peninsula – Underwear Bomb	3	Success	Terrorist	2000s	Middle East	Yes
Hamas – Cyanide	2	Failure	Terrorist	2000s	Middle East	No

[28] Success denotes cases where the engineering effort yielded functional and at least partially efficacious results, failure denotes cases that did not, and apocryphal refers to cases that are mentioned in the open sources but there is no credible evidence that they ever actually occurred.
[29] TCO = Transnational Criminal Organization.

https://scholarcommons.usf.edu/jss/vol9/iss1/3
DOI: http://dx.doi.org/10.5038/1944-0472.9.1.1502

Zetas – Radio Network	4	Success	TCO	2000s-Present	N. America	Yes
Hamas – UAVs	4	Success	Terrorist	2010s	Middle East	No
Syrian Rebels – "Drive by wire" Machine Gun Vehicle	3	Undetermined	Insurgent	2010s	Middle East	No

Upon further research, one case (ETA's production of a remote-controlled vehicle) was quickly excluded because it was likely apocryphal and based on a mistranslation of news reports. Any candidate for which there was not a high degree of confidence of sufficiently detailed information being available in the open sources was also dropped from consideration. The remaining cases were prioritized in terms of the degree to which they met the definition of a complex engineering effort provided above, judged subjectively on a 1 to 5 scale. This was measured against the complexity of the task that was attempted, irrespective of the extent to which the actor succeeded. Thus, Aum Shinrikyo's attempts to produce a nuclear weapon, even though these never progressed beyond the embryonic stage, receive the highest rating given the inherent complexity of actually constructing an improvised nuclear device.

Also, for tasks where the complexity varies across subcategories of weapon or technology pursued, the rating is based on the specific type actually pursued by the VNSA. So, for example, since al-Qaida and Hamas only pursued relatively primitive chemical agents (such as cyanide), their efforts receive a lower rating than the chemical weapons exploits of Aum Shinrikyo, which pursued more sophisticated agents like sarin and VX. Similarly, while submersibles can range across multiple levels of complexity, those pursued by FARC, which included integrated and advanced propulsion, navigation and life support systems, receive a higher rating.[30] In order to explore the most clear-cut instances of complex engineering efforts, it was decided to only consider cases scoring 4 or 5. This left the cases in the highlighted rows in Table 1.1.[31]

[30] Since the scale only goes up to 5, both the efforts of FARC and Aum's nuclear efforts receive the maximum value, even though nuclear weapons are arguably somewhat more complex to construct than submersibles.

[31] While Aum Shinrikyo's biological weapons program also met the criteria, this program has been extensively detailed elsewhere (for example, see Richard, Danzig, Marc Sageman, et. al., *Aum Shinrikyo: Insights Into How Terrorists Develop Biological and Chemical Weapons* (2nd Edition) (*Center for a New American Security*, 2012), available at: *http://www.cnas.org/files/documents/publications/CNAS_AumShinrikyo_SecondEdition_English.pdf*, making a detailed case study less useful. Therefore, researchers

The cases selected for this study were therefore:

1. The Provisional Irish Republican Army and the development of advanced mortar systems.

2. Aum Shinrikyo's chemical and nuclear weapons programs (combined into a single case).

3. The production of submersibles and submarines by FARC (Fuerzas Armadas Revolucionarias de Colombia).

4. The Los Zetas transnational criminal organizations' construction and maintenance of an expansive radio communication network across Mexico.

5. Hamas and the construction of attack tunnel networks from Gaza into Israel.

These five cases span six different types of engineering activity, three types of organization (terrorist, criminal and hybrid), four regions, and each decade from the 1970s to the present, thus providing ample variety in terms of context. While researching possible cases, researchers also noted the importance of the A.Q. Khan nuclear technology smuggling network. Although not itself qualifying as a complex engineering effort, the evolution and activities of this network provide a stark illustration of one avenue by which violent non-state actors might gain access to the sophisticated technology and expertise required for a particular complex engineering effort. It was therefore decided to conduct a sixth case study on the A.Q. Khan saga, which, although differing from the other five, demonstrates how illicit networks might facilitate a violent non-state actor's complex engineering efforts.

The research team then assigned one or more authors to each case, based on prior expertise and interest. This was followed by the data collection phase, which comprised extensive research of the open sources, including books, journal articles, government reports and news reports. This was supplemented in several cases by interviews with experts having intimate

regarded it as sufficient to focus on the cult's chemical and nuclear programs, the former effort regarded as at least a qualified engineering success and the latter an abject failure.

https://scholarcommons.usf.edu/jss/vol9/iss1/3
DOI: http://dx.doi.org/10.5038/1944-0472.9.1.1502

knowledge of the particular case or VNSA. Collected sources were then evaluated for relevance, reliability, and corroboration or contradiction. With respect to the actual construction of the case studies, all authors were instructed to attempt to answer the framing questions listed above and to structure their analysis according to a standardized format. This consisted of four main sections, each of which was designed to broach a number of sub-topics as far as available information allowed. Each case was therefore structured as follows:[32]

1. An introductory section providing background and a summary of the type of complex engineering effort undertaken by the VNSA.

2. A section on the decision to engage in the complex engineering effort, encompassing, where possible, the motivation behind the effort, the decision makers involved, the degree of risk tolerated by the VNSA and the length of the planning and development cycle.

3. A section on the implementation aspects of the effort, including not only a discussion of the process followed, but also descriptions of the implementing parties, sources of technical expertise, any collaboration with external parties, safety and security considerations, and obstacles that were encountered throughout the process.

4. A concluding section, providing an analysis both of why the VNSA was drawn to pursuing the particular complex engineering task and the factors that were ultimately responsible for the success (or otherwise) of its efforts.

The six case studies, together with their individual findings, are presented in the remainder this special issue. The first five cases follow the structured format shown above, while the A.Q. Khan case highlights the establishment and ultimate break-up of the nuclear smuggling network. Upon completion of the case studies, it became possible to synthesize and compare the complex engineering efforts undertaken by the VNSAs, a task carried out in the concluding article of this issue.

[32] The A.Q. Khan case, being qualitatively different from the rest, followed a somewhat different structure, focusing on the evolution of the network and why it persisted for so long, as well as why it was ultimately interdicted.