Faculteit Sociale Wetenschappen

Departement Politieke Wetenschappen

Building the Bomb

An organisational approach to the nuclear terrorism threat

Proefschrift voorgelegd tot het behalen van de graad van doctor in de sociale wetenschappen: politieke wetenschappen aan de Universiteit Antwerpen te verdedigen door

Brecht Volders

Promotor: Prof. dr. Tom Sauer

Antwerpen, 2019

Members of the doctoral committee

Prof. dr. Tom Sauer (University of Antwerp, promotor)

Prof. dr. Wouter Van Dooren (University of Antwerp)

Prof. dr. Jacob Shapiro (Princeton University)

Members of the jury

Prof. dr. Jorg Kustermans (University of Antwerp)

Prof. dr. Wyn Bowen (King's College London)

Table of contents

Acknowledgments

Writing a PhD manuscript is in many ways similar to a nuclear terrorism project. It can also be considered to be a nonroutine endeavour. Various unexpected surprises arise along the way, and reflection about resolving these problems requires a considerable amount of time. It follows that the successful implementation of this project would be not at all possible without the help of many people. These people's skills and experience were indispensable in guiding me through this project.

Most of all, I would like to thank prof. Tom Sauer. On the one hand, this manuscript would have not been possible without him. Tom gave me the opportunity and resources to start this project. Moreover, most importantly, he gave me the necessary autonomy and freedom to develop both myself and my manuscript. He trusted me from the beginning on. On the other hand, my time at the university of Antwerp would not have been as enjoyable as it was without a boss like Tom. He was always correct, flexible and understanding. That has been a blessing.

A special word of thanks is also extended to a number of other people involved in this project. The members of my doctoral committee, Prof. Wouter Van Dooren and prof. Jacob Shapiro, were always ready to weigh in when I had questions or doubts. Their comments, feedback and advice enabled me to substantially improve the quality of my manuscript. Next, the members of my doctoral jury, prof. Wyn Bowen and prof. Jorg Kustermans, were willing to voluntary read and review this manuscript. For their sake, I hope I did indeed improve the quality of my manuscript. Third, besides being willing to be a member of my jury, I also had the pleasure to be in a desk right across the desk of prof. Jorg Kustermans. Whether we were talking about my manuscript, his work, or any other non-related topic, Jorg's analytical precision, depth of knowledge and witty remarks contributed to both the quality of my work and a pleasant professional atmosphere. Finally, my fellow doctoral candidates and colleagues contributed each day – both directly and indirectly – to the successful conclusion of this dissertation. Thank you.

Moreover, I was lucky enough to enjoy the company and support of many other people that facilitated this process. First, my colleagues at the University of Antwerp were truly unique. It was due to them and our countless non-academic endeavours that I can count the number of days that I reluctantly went to work on one hand. Working at the university was a true pleasure. Outside of university-life, I could always count on a group of friends that systematically neglected my research or – at most – asked how things were going with my 'little paper.' They were essential to putting things into

perspective. Finally, and by far the most important, I want to thank my mom, dad, Klaartje, Thijs, Mien, Hanne and Greet. There are few dull moments in such a big family. Yet, each of them brought me to where I am today. I am proud of where I am, but I owe it all to them. Having the support of loving parents, sisters and a brother was and is of invaluable importance to me. Thank you.

Figures, tables and photos

Figures

Tables

Photos

1. Introduction

It is time. Al Qaeda succeeded in assembling a simple fission device. A similar device devastated Hiroshima more than 70 years ago. Now, justified by their religious beliefs, they intend to destroy Manhattan. Tens of thousands of people will die; an even higher number will be injured. The project team spent years quietly planning their mission. The crude nuclear bomb's essential components had secretly been stolen bit-by-bit from nuclear facilities in Pakistan, Iran and Russia. It took them years to collect, hide and secure this material. An abandoned house at the outskirts of Peshawar served as a machine-shop to assemble the improvised HEU device. Once ready, the project team illicitly smuggled the device to American soil by means of maritime transport in a matter of weeks. Now, parked in their truck at the 9/11 memorial, the attacking team just finalised the last checks with respect to the device and received the go-ahead by their leader…

This type of scenario is often topic of both popular, academic and political concern. The nexus between indiscriminate terrorism and nuclear proliferation is generally considered a risk to international security. Yet, assessing this risk is a challenging task. There are a variety of diversely motivated terrorist organisations, a multitude of potential pathways to success for a terrorist organisation, and a range of security measures designed to prevent (particular aspects of) such a nuclear plot. Moreover, security considerations related to the sensitive nature of this topic invariably cloud discussions on this topic, terrorist organisations might be intelligent and adaptable, and nuclear terrorism threat assessments need to cope with a paucity of data.[1] There are no empirical cases. Downes and Hobbs therefore describe nuclear terrorism as a "virtual risk." While it is true that relevant information is available, this is often "limited, incomplete, open to interpretation, or only applicable to small part of the overall puzzle."[2] Considering the large number of unknown variables, it follows that both quantitative and qualitative assessments often disagree with respect to the likelihood of a nuclear terrorism plot enfolding.[3] The input parameters to these threat assessments are attributed very diverging

[1] Brecht Volders and Tom Sauer, "Introduction to the Book," in *Nuclear Terrorism: Countering the Threat*, Global Security Studies (London & New York: Routledge, 2016), 3–12.

[2] Robert Downes and Christopher Hobbs, "Nuclear Terrorism and Virtual Risk: Implications for Prediction and the Utility of Models," *European Journal of International Security* 2, no.2 (2017): 212-213. This is, e.g. also argued by: Peter Zimmerman, "The impossibility of probabilities", *AIP Conference Proceedings,* 2017. https://aip.scitation.org/doi/pdf/10.1063/1.5009233 (accessed April 1, 2019). While these authors are specifically writing about numerical probability estimates, this argument also holds true for more qualitative probability assessments.

[3] The topic of nuclear terrorism is widely explored. More sceptical opinions on the likelihood of nuclear terrorism are voiced by, e.g., Michael Levi, *On Nuclear Terrorism* (Cambridge & London: Harvard University Press, 2009); John Mueller, *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al Qaeda* (Oxford: Oxford University Press, 2010); Robin Frost, *Nuclear Terrorism after 9/11* (USA & Canada: Routledge, 2005). Other scholars and experts are

probabilities. This study, however, aims to deepen our understanding of the probability of this threat as the output of analysis. This way, we aim to contribute to the validity of future nuclear terrorism threat assessments.

Yet, before approaching this theme, we need to reflect upon the societal and scientific relevance of this doctoral study. First, we should ask ourselves whether this is a relevant societal topic to study: is there actually a good reason for popular, academic and political attention to this risk? In this context, it is interesting to note that any risk assessment is considered to be function of the probability of the phenomenon occurring and its potential consequences. On the one hand, the *probability* of this type of scenario is generally considered low. Notwithstanding substantial disagreements in particular nuclear terrorism threat assessments, it is clear that "most terrorist attacks involve readily available weapons and rarely include sophisticated tactics that require long-term planning."[4] LaFree, Dugan and Miller illustrate that "of the more than 113,000 attacks recorded in the GTD (Global Terrorism Database) only 220 used chemical weapons and only 32 used biological weapons." More specifically, they continue by stating that "only 13 used radiological weapons and none used nuclear weapons."[5] Likewise, a seminal study on "complex engineering efforts" by researchers at START identified only 22 candidate cases to analyse.[6] These examples illustrates that the general prevalence of this type of advanced technical terrorist attacks is low.[7] On the other hand, however, a risk equation also needs to take into account the *consequences* of a particular scenario. Terrorist organisations constructing and detonating a (crude) nuclear device would lead to unseen socio-economic, physical and psychological disruption and destruction. The effective detonation of a terrorist atomic device can change societal order as we know it. At least two terrorist organisations (Al Qaeda and Aum Shinrikyo) are known to have demonstrated interest in this type of attack. In reflecting upon the societal relevance of this study, we should therefore take into account the difference between *probabilistic* and *possibilistic* thinking. It is true that we need probabilistic thinking in terms of chances and odds; it leads to prescriptions on how society ought to be organised. Yet, this does not imply that we should forget the *possibility* of such an event occurring.

---

more concerned about nuclear terrorism. For instance.: Matthew Bunn and Anthony Wier, "Terrorist Nuclear Weapon Construction: How Difficult?," *The Annals of the American Academy* 607 (2006): 133–49; Charles Ferguson and William Potter, The Four Faces of Nuclear Terrorism (United States: Center for Non Proliferation Studies, 2004); Charles Blair, "Jihadists and Nuclear Weapons," in *Jihadists and Weapons of Mass Destruction* (London & New York: CRC Press, 2009), 193–240; Graham Allison, *Nuclear Terrorism: the Ultimate Preventable Catastrophe* (United States: Henry Holt & Company, 2005).

[4] Gary LaFree, Laura Dugan, and Erin Miller, *Putting Terrorism in Context: Lessons from the Global Terrorism Database*, Contemporary Terrorism Studies (London & New York: Routledge, 2015), 173.

[5] Ibid., 184 & 191.

[6] Gary Ackerman, "Designing Danger: Complex Engineering by Violent Non-State Actors: Introduction to the Special Issue," *Journal of Strategic Security* 9, no.1 (2016): 1–11.

[7] Note that, at this moment in the dissertation, I do not focus on the exact conceptualisation of this type of attacks. These examples merely function as a generic illustration of the frequency of this type of attacks occurring.

Worst-cases do happen.[8] It therefore can be downright dangerous to completely neglect possibilities in favour of probabilities.[9] The mere consequences of such an event should remind us to continuously reflect on this topic. It remains a relevant theme to study.

Second, moving to the scientific relevance of this study, we need to reflect on how we should then assess this nuclear terrorism threat? Paradoxically, as we focus on the possibility of this scenario and its consequences, we are insurmountably confined to probabilistic thinking. Yet, in doing so, we need to remain thoughtful of assessing the probability as the "output of analysis."[10] This is true for both quantitative and qualitative assessments. There are no empirical cases of a well-developed nuclear terrorism plot. Selective use of data and insights can lead to both speculative and exaggerated threats.[11] Secrecy, in this context, can have a generative effect.[12] A variety of conceivable scenarios might converge in a single worst-case nuclear threat projection, thereby resulting in excessive and adverse countermeasures.[13] Probability assessments should therefore aim to be the result of an encompassing analysis. It is overly simplistic – and by consequence wrong - to merely assign probabilities to individual (input) parameters. It is necessary to understand a diverse variety of variables and their interplay. A terrorist group's decision and implementation of nuclear terrorism project is dependent on, e.g., a group's capabilities, the tactical and strategic aims of this organisation, their perceptions regarding success or failure, and counterterrorism security measures.[14] This is in line with Michael Levi's argument that we should not only consider isolated variables or individual parts of a nuclear terrorism plot.[15]

Aiming to contribute to this type of encompassing analysis, this study therefore focuses on one often overlooked dimension in nuclear terrorism threat assessments: the organisational challenges to implementing a nuclear terrorism project. While organisational dynamics and variables are no

[8] Look, for instance, at a variety of nuclear safety accidents/close calls (in the military sector). Scott Sagan, *The Limits of Safety: Organisations, Accidents, and Nuclear Weapons* (Princeton: Princeton University Press, 1993). Although this book is about accidents/close calls, it functions as a useful reminder to always consider the possibility of any event occurring.

[9] Lee Clarke, *Worst Cases: Terror and Catastrophe in the Popular Imagination* (Chicago & London: The University of Chicago Press, 2006).

[10] Downes and Hobbs, "Nuclear Terrorism and Virtual Risk," 216-217.

[11] Magnus Ranstorp and Magnus Normark, *Unconventional Weapons and International Terrorism*, Political Violence (London & New York: Routledge, 2009), 2

[12] Kathleen Vogel, *Phantom Menace or Looming Danger? A New Framework for Assessing Bioweapons Threats* (Baltimore: The John Hopkins University Press, 2013), 13.

[13] Exaggerated threats might lead to (public) hysteria. At the broad counterterrorism level, undue measures could steer away limited resources from more urging (conventional) counterterrorism measures. Likewise, specifically at the nuclear counterterrorism level, it could divert resources to unrealistic scenarios. This argument has been developed by, e.g., Mueller, *Atomic Obsession.*

[14] Downes and Hobbs, "Nuclear Terrorism and Virtual Risk." Again, while these authors are specifically writing about numerical probability estimates, this argument also holds true for more qualitative probability assessments.

[15] Levi, *On Nuclear Terrorism*.

omnipotent causal force, it is remarkable that this dimension has not been identified in-depth and systematically explored in the traditional scientific literature on nuclear terrorism. While this study does not aspire to develop an all-encompassing model to assess this phenomenon as a whole, nor does it aim to provide any numerical estimates on the threat, it does hope to enable a deeper understanding of the probability of nuclear terrorism – as the output of analysis – by exploring this critical gap in the literature on this theme. By exploring this underdeveloped dimension in nuclear terrorism probability assessments, I hope to contribute to the encompassing nature of future nuclear terrorism threat assessments. This might simultaneously help in bridging the gap between differing opinions on this theme.

Indeed, as will be illustrated in chapter two, traditional nuclear terrorism threat assessments focus primarily on terrorist motivations to use nuclear devices, the availability of nuclear know-how and technology, and/or clandestine organisations' opportunities to obtain fissile material. Few experts, however, systematically focus on exploring the complexity for a terrorist organisations to implement a nuclear armament project. Experts often refer to a *well-organised and sophisticated,*[16] a *technically sophisticated,*[17] or *organisationally sophisticated* [18] terrorist group. Yet, rather than systematically reflecting upon the meaning of these concepts, most of the literature diverts attention to circumscribing the threat by means of the aforementioned traditional variables. One should, however, not only focus on the individual components, but also reflect on the system. Implementation of the armament project is taken for granted and the process itself is understudied. Traditional approaches insufficiently integrate questions like: who should make the decisions in a nuclear terrorism project, how can unforeseen obstacles dealt with, and/or how should security considerations be taken into account throughout assembly of the nuclear device?[19] An organisational approach enables thorough reflection upon these questions, and might add to our better understanding of the nuclear terrorism threat.

This study will thus adopts such an organisational approach in order to supplement future nuclear terrorism threat assessments. This is not incompatible with previous discussions and insights on the three traditional nuclear terrorism variables. In contrast, exploring this organisational dimension might shed new light on the three aforementioned intertwined debates, and enable a deeper understanding of the nuclear terrorism threat. That is the goal of this study.

[16] Bunn and Wier, "Terrorist Nuclear Weapon Construction: How Difficult?" 133.
[17] Rolf Mowatt-Larssen et al., "The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism" (Harvard Belfer Center, May 2011), 10.
[18] Peter Zimmerman and Jeffrey Lewis, "The Bomb in the Backyard," *Foreign Policy* (2009).
[19] Ackerman, "Designing Danger," 6-7.

1.1. Setting the research boundaries

"Nuclear terrorism" is a complex phenomenon. It can manifest itself in various ways and may be achieved through a diversity of pathways. The exact challenges in *organising* a nuclear terrorism project can therefore strongly vary. Setting the research boundaries is subsequently of essential importance in keeping focus. In order to explore these organisational challenges, I have delineated the scope and design of this research project in three interrelated ways:

First, this study specifically focuses on the construction and detonation of an "improvised nuclear device" (IND) by a terrorist organisation. While I will use this term interchangeably with a "crude nuclear device" or a "terrorist nuclear device," it is of importance to clearly mark what I mean by these conceptually ambiguous terms. Given that it would be inherently arbitrarily to determine a basic yield that would be required to qualify as an IND, I start from a definition of an IND as any device with a yield-producing explosion based on a chain reaction created by the fission of nuclear material. This thus can range from a fizzle (that results in a few tons to a 100 tons) to the terrorist equivalent of Hiroshima (which would result in around 15 kilotons). While the latter - more efficient – type of terrorist nuclear device would imply an increased technical complexity, the development of each type of IND on this continuum would often imply the implementation of a *nonroutine* plot. Even the development of a nuclear plot that would result in a fizzle would often go beyond standard operations for any terrorist organisation (infra). This study will, however, often touch upon the differences between diverging scenario's on this continuum.

In order to further clarify the exact research focus, I will also elaborate explicitly on what is not covered by the use of this term in this study. This term does not refer to a neutron flux or other type of nuclear terrorism, such as an attack on a nuclear facility of radiological terrorism (e.g. a radiological dispersal or emission device). While these types of nuclear terrorism can cause substantial psychological and physical damage, their consequences are mostly less destructive and disruptive compared to an actual nuclear explosion.[20] Next, an improvised nuclear device neither refers to an actual nuclear weapon. A nuclear weapon is understood as a military qualified item. It is ready to be delivered by aircraft, missile or glide bomb. It is more reliable, safe and predictable. A crude nuclear device does, however, not need to be more advanced than an "experimental assembly" in order to create substantial levels of

[20] Admittedly, the consequences of a nuclear meltdown could potentially tie with those of the detonation of an improvised nuclear device.

destruction.[21] Finally, as will be outlined in more depth in the next chapter, I do not focus on a scenario of a terrorist organisation stealing or buying an intact nuclear device. This type of scenario would unduly broaden the research focus. Admittedly, various cases of (near) loss of control over nuclear weapons, state terrorism sponsors in conflicts zones, uncertainty with respect to security measures in several states (e.g. Pakistan or North-Korea), and problems with nuclear forensics should suffice to remain aware of this option.[22] Yet, I believe that the counterarguments that stringent security measures are often in place, that attribution to the responsible state is likely, and that a state is unlikely to allow losing control over these unique and destructive weapons still prevail.[23]

Second, and closely related to this last remark of the first demarcation, this research project will start from a particular nuclear terrorism scenario. Even merely considering the construction and detonation of a crude nuclear device, there is a myriad of pathways for a terrorist organisation to achieve this type of nuclear capacity. The exact pathway depends on the terrorist organisation's resources, the (state) assistance that they can acquire, their exact operational environment (and its opportunities), the organisation's strategic and operational goals, etc. Organisational dynamics and variables will subsequently play a different role in different pathways to a terrorist nuclear capacity. Given that it is impossible to systematically include every potential course of action, I will build on expert opinion to adopt a particular nuclear terrorism scenario. This – as we will call it - *nonroutine* nuclear terrorism scenario will be outlined in detail in the next chapter. Such a scenario provides a formal way to structure thinking about this phenomenon. It provides focus to my study. Although it will inherently remain open to discussion, I portrayed a scenario that does not needlessly complicate the project while

[21] Nic Von Wielligh and Lydia Von Wielligh-Steyn, *The Bomb: South Africa's Nuclear Weapons Programme* (Pretoria: Litera Publications, 2015), 135.

[22] Ferguson and Potter, *The Four Faces of Nuclear Terrorism*; Gary Ackerman et al., "Anatomizing Radiological and Nuclear Non-State Adversaries: Task 1: Identifying the Adversary" (Maryland: National Consortium for the Study of Terrorism and Responses to Terrorism, September 27, 2009); The International Institute for Strategic Studies, "Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks - A Net Assessment," Strategic Dossiers (London: International Institute for Strategic Studies, 2007); X, "Broken Arrows: Nuclear Weapons Accidents," *Atomic Archive* (blog), n.d., http://www.atomicarchive.com/Almanac/Brokenarrows_static.shtml. (accessed April 1, 2019).

[23] 55% of the respondents (nuclear experts) of the 2005 Lugar survey saw the manufacturing of a nuclear device by a terrorist organisation more likely than them stealing an intact nuclear device: Richard Lugar, "The Lugar Survey On Proliferation Threats and Responses," (Survey, June 2005), https://fas.org/irp/threat/lugar_survey.pdf. (accessed 24 July 2017). See also, e.g.: Allison, *Nuclear Terrorism,* 92; Morten Bremer Maerli, Annette Schaper, and Frank Barnaby, "The Characteristics of Nuclear Terrorist Weapons," *American Behavioral Scientist* 46, no. 6 (2003): 730; Keir Lieber and Daryl Press, "Why states won't give nuclear weapons to terrorists?," *International security* 38, no. 1 (2013): 80-104.
Intact nuclear devices might also be bought by a terrorist organisation at a nuclear black market. Yet, besides stories about missing Russian suitcase nukes in the 90s – which are difficult to substantiate and often do not take into account the potential deterioration of the nukes' critical components - there are no known cases of missing nuclear bombs (Ackerman et al., "Anatomizing Radiological and Nuclear Non-State Adversaries," 65).

simultaneously enveloping most potential pathways. This way, I avoid exaggerating the impact of organising this nonroutine endeavour. Note, moreover, that the last chapter of this study will reflect upon other scenarios which are less (or not) nonroutine, and how my insights might apply to these scenarios. This enables us to deepen our understanding of the probability of this threat as the output of analysis.

Third, any study on this issue inherently struggles with the lack of empirical cases. The core empirical challenge of this study is that there are no cases of a terrorist organisation successfully constructing and detonating an improvised nuclear device. This lack of direct empirical evidence of this phenomenon impedes any confirmatory study. It limits the empirical evidence for studying this phenomenon, and forces us to look for alternative ways to empirically assess the threat. I have therefore opted to build on case studies of four projects that were facing a *nonroutine* nature of technology. As will be outlined in depth, the adopted nuclear terrorism scenario would also be such a *nonroutine* case. We are subsequently able to better understand the specific nuclear terrorism case by knowing about these other nonroutine cases. To be precise, I will extrapolate relevant insights with respect to a nuclear terrorism plot by building on this shared organisational feature (infra). Each case is characterised by a similar nonroutine nature of technology, and therefore contains relevant insights with respect to a better understanding of the nuclear terrorism threat. This type of systemic comparison has not been done in the nuclear terrorism literature. Yet, let it be clear that, rather than proving anything, I hope this research design enables us to explore and learn something about an underdeveloped dimension to the nuclear terrorism threat.

1.2. Plan of the book

The goal of this study is to enable a deeper understanding of the nuclear terrorism threat. Chapter two embarks upon this journey by embedding this study's particular approach in the broader nuclear terrorism literature. To be precise, I will do so by outlining a potential nuclear terrorism scenario, assessing today's literature on the nuclear terrorism phenomenon, and cross-referencing this latter field of literature with the literature on innovation and technology acquisition by a terrorist organisation. This literature review will substantiate the argument that an organisational approach is necessary in today's nuclear terrorism threat assessments.

Simultaneously, this chapter will narrow down the exact focus by illustrating that particular attention needs to be given the role of a terrorist group's organisational design. To be precise, I will demonstrate

that some parameters with regards to innovation and technology acquisition by a terrorist organisation are inadequately covered by today's nuclear terrorism literature. These parameters can be categorised under one common denominator: the organisational design. This variable refers to the control and coordinating mechanisms vis-à-vis the work that needs to be completed. It consists of three particular dimensions: the interconnectedness of the group, the level of hierarchical control, and the degree of specialisation. These dimensions shape the aforementioned issue of control and coordination. The research question will thus be: "what is the role of a terrorist group's organisational design in implementing the construction and detonation of an improvised nuclear device?"

Chapter three will develop some hypotheses on this relation between the organisational design of a terrorist organisation and the nuclear terrorism threat. To this end, I will draw on both the broader terrorism literature and literature that is focused on the role of the organisational design. In general, I will argue that I expect that a more organic organisational design would increase the likelihood that a terrorist organisation can effectively complete a nuclear terrorism project. Yet, simultaneously, I also expect that this type of organic design would be an inefficient way for a terrorist organisation to guarantee the security of its nuclear terrorism plot. Moreover, building on these insights, I will also argue that I expect that the implementation of a nuclear terrorism plot via an organic organisational design can be perceived to be inefficient strategy for a terrorist organisation. These three hypotheses thus generally introduce the idea of an effectiveness-efficiency trade-off.

Chapter four subsequently elaborates on the research design of this study. On the one hand, this chapter will account for the exploratory nature of this study and the implications of this approach. On the other hand, this chapter will outline that I have opted for a case study research design with four cases: the construction of the first atomic bombs at Los Alamos, the South African PNE program, Aum Shinrikyo's CB armament activities, and Al Qaeda's implementation of 9/11. Each of these four cases was characterised by a nonroutine nature of technology. This is similar to the nature of technology of the adopted nuclear terrorism scenario. Thus, building on this shared organisational feature, each case study enables me to extrapolate relevant insights with regards to the hypotheses on the nuclear terrorism threat. Chapter five to eight will each cover one empirical case study and its extrapolations to a nuclear terrorism plot.

Finally, chapter nine will provide a cross-case analysis that brings together the findings of each of the four case studies. It is necessary to aggregate these findings. This analysis will emphasize recurrent findings, take into account potentially qualifying conditions, and explore how these insights might relate to traditional nuclear terrorism threat assessments. In general, this chapter will support the plausibility

of the suggested effectiveness-efficiency trade-off. Moreover, it will specifically highlight some issues that remain underdeveloped in today's nuclear terrorism threat assessments. Next, this chapter will also reflect upon other nuclear terrorism scenarios. I will illustrate how the suggested approach and insights might enable a better understanding of these other nuclear terrorism scenarios. This way, I hope this study meets its goal of contributing to a more comprehensive understanding of the nuclear terrorism threat.

2. Assessing nuclear terrorism: the need for an organisational approach?

There is a relatively high number of publications on the threat of a terrorist improvised nuclear device. By way of illustration, an online search in the databases of the University of Antwerp results in 648 hits with the term 'nuclear terrorism' in the title between 2001 and 2018. Considering the destructive and disruptive consequences of such an attack, it was to be expected that - particularly after 9/11 - this threat would attract a lot of scholarly, political and popular concern. In order to enable a deeper understanding of this threat, this chapter aims to first embed and situate the particular focus of this study in the broader literature on this topic. Specifically, it will be demonstrated that an organisational approach is necessary in nuclear terrorism threat assessments, and that particular attention needs to be given to the role and impact of the organisational design.

In order to do so, this chapter will develop two arguments. On the one hand, this chapter will develop and elaborate on the nuclear terrorism scenario that I adopt as a starting point. Besides the fact that this provides a framework for reasoning in this study, outlining the different tasks and activities of such a scenario simultaneously highlights the need for *organisation* and sheds light already on some of the organisational dynamics that can be expected to be at play during a nuclear terrorism plot. On the other hand, this chapter will elaborate on the literature on nuclear terrorism and more systematically cross-reference this literature with the broader literature on innovation and technology acquisition by a terrorist organisation. It will be made clear that some parameters identified in the literature on innovation and technology acquisition by a terrorist organisation are inadequately studied by traditional research on nuclear terrorism. Specifically, these parameters can be categorised as part of the organisational design. Given that nuclear terrorism would be a case of innovation and technology acquisition by a terrorist organisation, focus on the organisational design can thus be assumed to fill a critical gap in the literature on nuclear terrorism.

2.1. Developing a nuclear terrorism scenario

Organisation can be described as a "system for getting work done."[1] It will have an impact on the implementation of the different tasks and activities that need to be completed by a group. Logic

[1] Charles Perrow, "A Framework for the Comparative Analysis of Organisations," *American Sociological Review* 32, no.2 (1967): 195. I have opted here for such a broad description because this captures *all* organisations. It is true that organisations can have many divergent features (see, e.g. Richard Scott and Gerald Davis, *Organisations and Organising: Rational, Natural, and Open System Perspectives* (new Jersey: Pearson Prentice Hall, 2003) and that

therefore dictates that any group – including violent terrorist groups - must be *organised* to successfully implement an advanced technical attack.[2]

This chapter will first elaborate on the possible tasks and activities in a nuclear terrorism plot. Besides illustrating the necessity of considering organisational dynamics, the development of one particular scenario simultaneously sheds light already on some of these organisational dynamics that can be expected in such a nuclear terrorism scenario. Indeed, any organisation's performance is to a large extent linked to the actual work that they aim to complete. It is clear that there is not "one best way" to organise. A firm that produces office chairs will be differently organised than a firm that specialises in aerospace engineering. The type of organisation needs to fit the technology that they are pursuing.[3] In order to better understand the organisational dynamics and variables in a nuclear terrorism project, we therefore first need to understand the work and technology that a terrorist organisation might face while pursuing a nuclear terrorism plot

Let it be clear, however, that the adopted nuclear terrorism scenario does not constitute a claim on the probability that this scenario represents the exact tasks and activities that a potential nuclear terrorism plot would entail. The adoption of a particular nuclear terrorism scenario merely provides a framework for reasoning on this phenomenon. Rather than getting lost in a variety of scenarios and pathways, it offers a starting point to assess the impact of the organisational dynamics and variables. Adopting a way to structure thinking about this phenomenon makes the role of the organisational dimension amenable to investigation.[4] Yet, that being said, it is also true that I have aimed to develop a scenario that remains as realistic possible while enveloping as many potential pathways as possible. I have substantiated the step-by-step development of this scenario by building upon the relevant (technical) literature and

there are – closely related – different ways to think about organisations (see, e.g. Gareth Morgan, *Images of Organisation* (California: Sage Publications, 2006). Yet, starting from this broad description of an organisation neatly illustrates that an organisational approach is relevant and necessary in nuclear terrorism threat assessments. Other definitions, not surprisingly, are often in line with Perrow's broad definition. For instance, Gareth Jones defines organisation as "a tool used by people to coordinate their actions to obtain something they desire or value – that is, to achieve their goals"(Gareth Jones, *Organisational Theory, Design and Change: Text and Cases*, 4th ed. (Pearson Prentice Hall, 2003), 2). Likewise, Etzioni states that organisations are "social units that serve specific purposes." (Amitai Etzioni, "Organisational Control Structure," in *Handbook of Organisations* (Chicago: Rand McNally & Company, 1965), 650). Such a broad description is meant to clearly illustrate the relevance of an organisational approach. It clearly covers terrorist organisations, thereby illustrating the relevance of this approach.

[2] Gina Ligon et al., "Putting the 'O' in VEO's: What Makes an Organisation?," *Dynamics of Asymmetric Conflict* 6 (2013): 116.

[3] Lex Donaldson, *The Contingency Theory of Organisations* (London: SAGE Publications, 2001).

[4] Robert Downes and Christopher Hobbs, "Nuclear Terrorism and Virtual Risk: Implications for Prediction and the Utility of Models," *European Journal of International Security* 2, no.2 (2017): 219.

various conversations with nuclear experts.[5] Admittedly, expert opinion can be biased and/or characterised by diverging judgements. Yet, by weighing the different opinions and elaborating on the scenario in a relatively abstract manner, I believe this scenario provides a reliable starting point to structure my thinking about the phenomenon. Moreover, the final chapter of this study reflects upon this starting point, considers other potential scenario's, and elaborates on how my insights might be applicable to these scenario's.

In short, this chapter will argue that a nuclear terrorism scenario can often be characterised by facing "nonroutine" technology. Building on the work by Charles Perrow, a leading organisational sociologist, this refers to a project that can be expected to encounter many new situations and problems when executing the various tasks and activities. Moreover, the procedures to cope with these exceptional situations are expected to be difficult to work out in advance.[6]

2.1.1. The physics behind a 'first generation' nuclear weapon

The first assumption of this nuclear terrorism scenario presumes that a terrorist organisation would aim to construct and detonate a crude nuclear device similar to the first generation of nuclear weapons. The design of nuclear weapons has become increasingly complex more than 70 years after the Manhattan project. Whereas the first generation of nuclear weapons was based on the fission of atoms, today's boosted and hydrogen nuclear weapons combine both fission and fusion of atoms. Weapons with a yield up to 50 megaton – referring to the amount of energy released – have been tested. In contrast, the Hiroshima bomb had a yield of approximately 15 kiloton (kT) and the Nagasaki bomb had a yield of approximately 20 kT.[7] Such 'first generation' weapons require a less complex design and less challenging engineering tasks. Not surprisingly, there is a consensus in today's scholarly literature on this theme that terrorist organisations are most likely to focus on such– what is sometimes coined - "conceptually simple devices."[8]

---

[5] See table 4.1 for a detailed overview of my sources. It should be noted that any such hypothetical scenario will inherently remain open to discussion. Yet, in drafting this scenario, I have aimed to remained realistic and not portray a scenario that needlessly complicates the project. This way, I hope to avoided any exaggeration on the complexity of *organising* this unique endeavour. Although this scenario is thus not necessarily *carved in stone,* and potentially lacks some technical depth, I believe it does illustrate the complexity of a terrorist nuclear project.

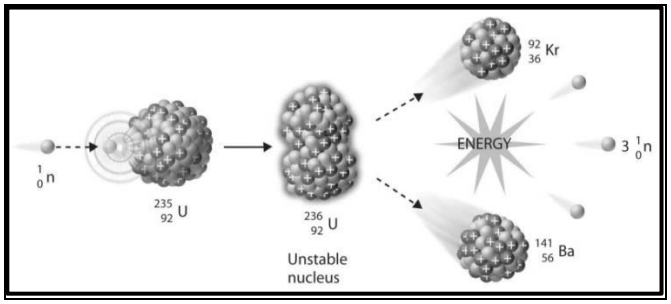
[6] Charles Perrow, *Organisational Analysis: A Sociological View* (Great Britain: Tavistock Publications, 1970), 75-77.

[7] Frank Barnaby, *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction* (London: Granta Books, 2003), 20.

[8] Peter Zimmerman and Jeffrey Lewis, "The Bomb in the Backyard," *Foreign Policy* (2009), 2.

This first generation of nuclear weapons rely on the process of nuclear fission. This works as follows: atoms consist of a mix of protons, neutrons and electrons. Protons and neutrons form the nucleus of the atom. Electrons are bound to the atom's nucleus in a sort of electron cloud. The number of protons in the atom determine its element. For instance, uranium has 92 protons and plutonium has 94 protons. The different elements, on their turn, come in various types of isotopes. This means that the nuclei have a different number of neutrons. Uranium, for instance, has 92 protons and 143 neutrons. This is the isotope uranium-235. The isotope uranium-238, in contrast, has 92 protons and 146 neutrons. In case a single outside neutron would strike an uranium nucleus, this neutron can be – depending on the stability of the nucleus – absorbed, change direction, or split the uranium nucleus into smaller pieces. It is this latter option that is called nuclear fission. As indicated in figure 2.1, this process amounts to the release of both energy and approximately 2 to 3 new neutrons. In some cases, these neutrons then again induce fission, thereby releasing energy and neutrons again. It is possible to produce a massive amount of energy in the form of a nuclear explosion in case a chain reaction can be started and sustained.[9]

Figure 2.1. The process of nuclear fission [10]

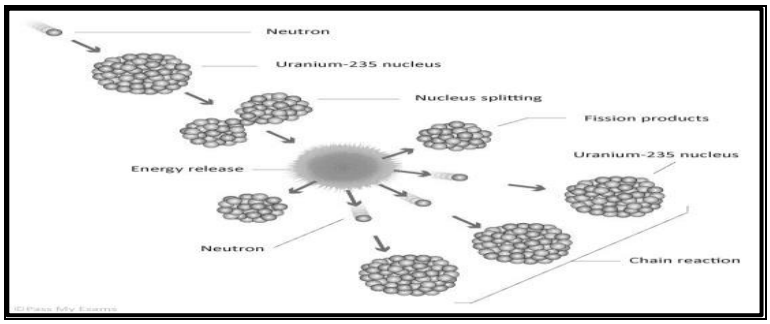


The creation of a sustained chain reaction and actual nuclear explosion is dependent on two interrelated issues. First, sufficient neutrons must cause fission in other nuclei. A nuclear chain reaction cannot be sustained if too much neutrons escape from the fissionable mass due to an insufficient amount of fissile material or the material is insufficiently dense. Such a configuration is called a subcritical mass of fissile material. A critical mass refers to a configuration where there is a balance between the lost neutrons and newly produced neutrons. As Levi puts it: "just enough neutrons leak to balance their production through fission."[11] The reaction becomes self-sustaining. Yet, in order to create a chain reaction leading

[9] Michael Levi, *On Nuclear Terrorism* (Cambridge & London: Harvard University Press, 2009), 26-36; Carey Sublette, "The Nuclear Weapons Archive: A Guide to Nuclear Weapons," n.d., available at: http://nuclearweaponarchive.org/Nwfaq/Nfaq2.html (accessed March 20, 2016).
[10] This image was found on the website of 'Nuclear Power for Everyone.' Available at: http://www.nuclear-power.net/nuclear-power/fission/ (accessed April 2, 2019).
[11] Levi, *On Nuclear Terrorism*. 36

to a nuclear explosion, it is necessary to have a configuration of material which leads to an exponential growth in fissioning nuclei. In (overly) simple terms, it takes about 82 generations to produce a 20 kT nuclear bomb: generation zero has one neutron, generation one has two neutrons, generation two has four neutrons, etc.[12] Because you develop extra neutrons in each generation - which is the difference with a critical configuration - the released energy ultimately leads to a nuclear explosion (see figure 2.2). This type of configuration is called a supercritical mass.[13]

Figure 2.2. A nuclear chain reaction[14]



Second, in order to create an actual nuclear explosion, it is also necessary to sustain this supercritical configuration for a sufficiently long period of time. Indeed, when a nuclear chain reaction proceeds, the released energy simultaneously causes the fissile material to expand. The expanding space between the atoms allows neutrons to more easily escape, rather than induce fission from other nuclei. This ultimately makes the configuration subcritical again. The fission device is "in a race with itself."[15] Matthew Bunn and Anthony Wier indicate that "the key to making a nuclear bomb is getting enough nuclear material together fast enough so that a substantial amount of explosive energy is released before the bomb blows itself apart and the reaction stops."[16] In order to have a "substantial amount of explosive energy released,"[17] it is necessary to have enough fissions occurring. The number of fissions depends on when the chain reaction actually starts. In case the chain reaction starts early – with the two subcritical components not close together yet – it only takes a small amount of expansion and time for the supercritical configuration to become subcritical again. The number of fissions and released

[12] Sublette, "The Nuclear Weapons Archive: A Guide to Nuclear Weapons."
[13] This information is based on, e.g.,: Barnaby, *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction*; Levi, *On Nuclear Terrorism*; Alex Wellerstein, "Critical Mass," *Restricted Data: The Nuclear Secrecy Blog* (blog), http://blog.nuclearsecrecy.com/2015/04/10/critical-mass/. (accessed June 7, 2016); Sublette, "The Nuclear Weapons Archive: A Guide to Nuclear Weapons."
[14] This image was found on the website of 'Nuclear Power for Everyone.' Available at: http://www.nuclear-power.net/nuclear-power/fission/ (accessed April 2, 2019).
[15] Sublette, "The Nuclear Weapons Archive: A Guide to Nuclear Weapons."
[16] Matthew Bunn and Anthony Wier, "Terrorist Nuclear Weapon Construction: How Difficult?," *The Annals of the American Academy* 607 (September 2006): 134
[17] Bunn and Wier, "Terrorist Nuclear Weapon Construction," 134.

energy remains relatively low. However, when the reaction starts later – when the two subcritical components have come close together – it takes a larger amount of expansion and time to make the supercritical configuration subcritical again. This results in a higher release of energy and a nuclear explosion.[18] The subsequent question then becomes: when does the chain reaction actually start? This depends on both the amount of incoming neutrons and the speed of assembly of the two subcritical configurations. A nuclear chain reaction might start each time a neutron enters the fissile material. When the emission of neutrons is high, there is an increased likelihood that the chain reaction will start earlier. This will result in fewer fissions. At the same time, the faster that two subcritical components are brought together, the more likely that the configuration will reach a higher degree of supercriticality. It takes a longer time for the material to expand. A low emission of neutrons and a high assembly speed would therefore maximize the *efficiency* of a nuclear weapon, which refers to the amount of energy that is actually released in relation to the potential amount of energy that could have been released.[19]

In building a first generation nuclear device, a terrorist organisation would thus need to develop a supercritical configuration for a sufficiently long time so as to produce a yield-producing explosion based on the fission of nuclear material. The exact yield of this device can substantially differ. Yet, the question remains how a terrorist organisation would need to go about in actually completing such a project. After having highlighted the physics behind such a device, the next sections will elaborate in more detail on the potential tasks and activities that a terrorist organisation that pursues the construction and detonation of a nuclear device would need to complete. Taken together, these hurdles will form the nuclear terrorism scenario that I adopt.

2.1.2. Various hurdles to a terrorist nuclear device

Any nuclear terrorism project consists of a diverse number of tasks and activities that need to be completed. Yet, the exact pathway that a terrorist organisation might follow to achieve its nuclear ambitions can strongly vary. This depends, among others, on the terrorist organisation's resources, the (state) assistance they would receive, their ideological and strategic goals, and/or their operational opportunity environment. Yet, building on the available literature – and various conversations with nuclear (terrorism) experts - I believe that we can generally expect four key hurdles in a nuclear

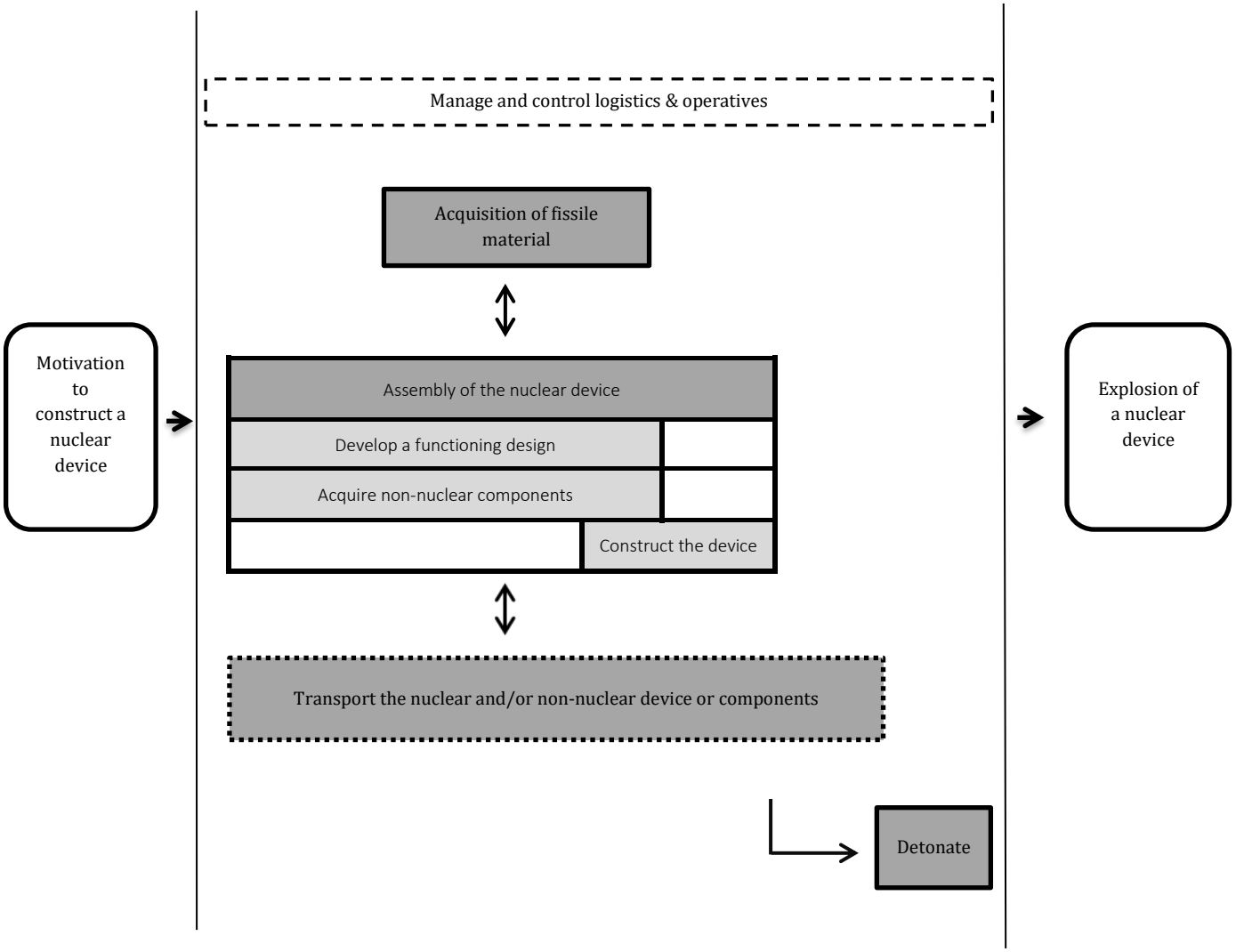
[18] This is based on, e.g., Levi, *On Nuclear Terrorism,* 35-38; Bunn and Wier, "Terrorist Nuclear Weapon Construction," 134-143; Charles Blair, "Jihadists and Nuclear Weapons," in *Jihadists and Weapons of Mass Destruction* (London & New York: CRC Press, 2009), 195–198. Mason Willrich & Theodore B. Taylor, "Nuclear Theft: Risks and Safeguards" (Cambridge: Ballinger Publishing Company, 1974), 7 - 8.
[19] Levi, *On Nuclear Terrorism,* 37.

terrorism scenario.[20] I expect terrorist organisations to have to: (1) acquire fissile material; (2) assemble the (crude) nuclear device; (3) transport the nuclear and/or non-nuclear device or components; and (4) detonate the (crude) nuclear device. Even though the first hurdle is generally considered to be the most challenging - and the last hurdle considered to be relatively easy - each of these hurdles contain various tasks and activities. These might be taken by alternate courses of action. While the outcome of some tasks and activities can have an impact on the requirements with respect to other hurdles, it should be noted that some steps might be taken in parallel (and can even be tried again, if a first attempt fails). Terrorist organisations can – moreover - opportunistically try to complete some tasks while awaiting the right time to complete other tasks. As will become clear, figure 2.3 is designed in such a way to demonstrate this.

Before elaborating on this figure and the four key hurdles – which will lead to the final identification of the adopted nuclear terrorism scenario – it is important to note already that this figure includes a box "manage and control logistics and operatives." Whereas the remainders of this section will primarily outline the more tangible and technical tasks of a nuclear terrorism project, this study primarily focuses upon this more intangible organisational dimension. This organisational dimension is to some extent function from the technical tasks, but simultaneously also impacts their execution. They are mutual dependent. Yet, this organisational dimension is hardly ever the focus of any nuclear terrorism threat assessment.

[20] This is based on, e.g. Gary Ackerman et al., "Anatomizing Radiological and Nuclear Non-State Adversaries: Task 1: Identifying the Adversary" (Maryland: National Consortium for the Study of Terrorism and Responses to Terrorism, September 27, 2009); Matthew Bunn, "Guardians at the Gates of Hell: Estimating the Risk of Nuclear Theft and Terrorism and Identifying the Highest-Priority Risks of Nuclear Theft" (Massachusetts Institute of Technology, 2007); John Mueller, *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al Qaeda* (Oxford: Oxford University Press, 2010); Levi, *On Nuclear Terrorism*; Charles Ferguson and William Potter, *The Four Faces of Nuclear Terrorism* (United States: Center for Non Proliferation Studies, 2004); Morten Bremer Maerli, Annette Schaper, and Frank Barnaby, "The Characteristics of Nuclear Terrorist Weapons" *American Behavioural Scientist* 46, no. 6 (2003); Barnaby, *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction*. Naeem Salik, "Nuclear Terrorism: Assessing the Danger, " *Strategic Analysis* 38, no. 2 (2014): 173-184; and conversations with several nuclear (terrorism) experts (see table 4.1).

Figure 2.3. (Potential) pathway to an improvised nuclear device



Acquisition of fissile material

The acquisition of fissile material is by a majority of the nuclear terrorism experts considered to be the most difficult step for a terrorist organisation pursuing a nuclear capacity. It is generally believed that a terrorist organisation cannot indigenously produce fissile material. Considering there is still a substantial stockpile of fissile material worldwide, this scenario subsequently expects a terrorist organisation to externally procure fissile material. As will become clear, and as indicated in figure 4, the exact type and quantity of fissile material that a terrorist organisation might obtain will have a strong impact on the other hurdles in their nuclear terrorism project; it is the basic ingredient for any nuclear explosion. I will first elaborate on this latter issue before outlining the different tasks and activities related to this hurdle.

Fissile material refers to material of which the nuclei of the atoms are fissionable. While there are a variety of fissionable isotopes, most of them – such as protactinium, neptunium or americium - are only available in very small quantities, or have isotopic properties that substantially complicate their potential application in a (crude) nuclear device.[21] The three isotopes that are generally considered to be most suitable for use in nuclear weapons are uranium-233, uranium-235 and plutonium-239. Yet, the publicly available literature primarily focuses on the two latter types considering "the small number of secure locations where kilogram quantities of this (uranium-233) material exist" and "workers handling typical U-233 without shielding for several hours will begin to suffer radiation sickness."[22] This scenario therefore focuses on the possibility that terrorist organisations would acquire fissile material by means of obtaining uranium-235 (U-235) or plutonium-239 (Pu-239).

A first option for a terrorist organisation is the acquisition of uranium-235. Natural occurring uranium is widely available. Yet, out of thousand atoms of naturally occurring uranium, there are approximately only 7 atoms of U-235 and 993 atoms of uranium-238 (U-238).[23] The low concentration of U-235 in the material impedes the creation of a fission chain reaction needed for a nuclear explosion. In order to increase the concentration of U-235, it is necessary to industrially enrich the material. With a higher concentration of U-235 in the bomb-material, it would become increasingly easier to create a runaway chain reaction. The less U-235 is diluted with U-238, the less material is necessary to acquire a critical mass, the less risk of pre-initiation of the bomb, and the higher the yield.[24] In order to be able to create a nuclear explosion, uranium preferably needs to be enriched to at least – and likely far more – 20% of U-235.[25] This is generally referred to as Highly Enriched Uranium (HEU). In contrast, Low Enriched Uranium (LEU) refers to material with less than 20% of U-235. So-called weapon grade uranium – which would be the easiest material to create a nuclear explosion – is considered to be enriched material to 93% or more U-235. The question at this point becomes how much material a terrorist organisation would need to potentially create a nuclear explosion.

[21] Blair, "Jihadists and Nuclear Weapons," 195; Sublette, "The Nuclear Weapons Archive: A Guide to Nuclear Weapons." written correspondence with Nic Von Wielligh, 17th of October 2017.
[22] Bunn, "Guardians at the Gates of Hell," 234.
[23] Barnaby, *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction,* 73.
[24] See, e.g., Willrich & Taylor, "Nuclear Theft: Risks and Safeguards," 16 – 19, Bunn, "Guardians at the Gates of Hell," 222-225. A low concentration of U-235 can be overcome by, e.g. a higher quantity of material. Yet, this would complicates the process of bringing the material sufficiently fast together. Moreover, U-238 has a higher neutron background, thus it emits more neutrons. A higher concentration of U-238 therefore increases the chances that a chain reaction would begin prematurely. This would quickly make the configuration subcritical again. The yield of the device would decrease.
[25] Bunn, "Guardians at the Gates of Hell," 66. For a more detailed explanation, see also Willrich & Taylor, "Nuclear Theft: Risks and Safeguards," 16-17.

Figure 2.4. The bare critical mass of an unreflected sphere of uranium as a function of U-235 enrichment[26]

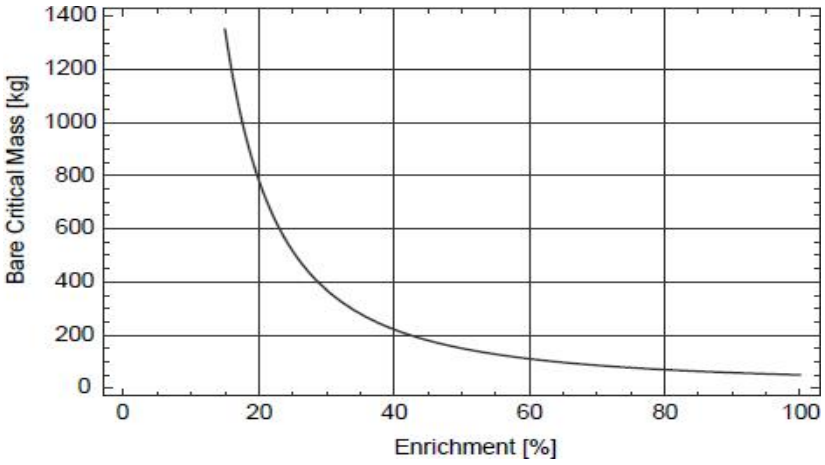


Figure 2.4 roughly describes the bare critical mass (in kg) – which refers to the amount of material necessary to start a self-sustaining chain reaction in a solid sphere (with nothing around it and at normal atmospheric conditions) - in relation to its enrichment levels. For a gun-type device, a bare-sphere critical mass of weapon-grade HEU of about 50 kg would suffice to potentially create a supercritical mass and a substantial nuclear explosion.[27] For an implosion-type design, much less material is expected to be needed to potentially create a substantial yield. This type of design configures the fissile material more efficiently, thereby requiring less material than the gun-type design (infra: design of a nuclear bomb). Matthew Bunn suggests that 22,5 kg of weapons-grade HEU would be enough for an implosion device.[28] While nuclear devices can also be made with less material – at the price of a reduced yield or an increase in design sophistication[29] - these numbers do provide a general idea on the amount of material that is often considered to be necessary for a terrorist organisation pursuing a nuclear capacity.[30] As of January 2017, the global stockpile of HEU is estimated to be about 1340 tons.[31] This number again stresses why this remains an important topic to study. There are inherent risks related to such a high quantity of fissile material.

[26] This image was found in a report by the National Academies Press (Reducing the use of highly enriched uranium in civilian research reactors; available at https://www.nap.edu/read/21818/chapter/4 (accessed April 2, 2019), and was based on data by Alexander Glaser (On the proliferation potential of Uranium Fuel for Research Reactors at Various Enrichment Level, *Science and Global Security* 14, no. 1 (2016): 1-24).

[27] For a more detailed explanation, see, e.g., Willrich & Taylor, "Nuclear Theft: Risks and Safeguards," 16-17. Bunn, "Guardians at the Gates of Hell," 217.

[28] Bunn, "Guardians at the Gates of Hell," 218.

[29] Ibid., 218.

[30] Note that these numbers merely function to provide the reader with a general idea on the required quantity of fissile material. A research note by Brown and Glaser, for instance, points to lower quantities that would be required (e.g. 31 kg of 20% enriched uranium might suffice to create a nuclear explosion). Andres Brown & Alexander Glaser, "On the Origins and Significance of the Limit Demarcating Low-Enriched Uranium from Highly Enriched Uranium," *Science and Global Security* 24 (2), 2016.

[31] International Panel on Fissile Materials. Available at: http://fissilematerials.org/ (accessed August 22, 2018)

A second option that is often mentioned for terrorist organisations pursuing a nuclear capacity is the acquisition of plutonium-239. Even though other plutonium isotopes can also potentially sustain a chain reaction, Pu-239 would be the most desirable option to create a nuclear explosion.[32] Other isotopes are, for instance, very likely to cause a pre-detonation. Yet, Pu-239 does not exist in nature. Pu-239 is produced when U-238 absorbs neutrons and becomes U-239. This is often a side-effect of the fissioning of uranium as fuel for a nuclear reactor. This isotope then decays in 2.5 days to Pu-239.[33] If these fuel elements would stay in the reactor for a longer period, Pu-239 would absorb neutrons itself, thereby producing the less suitable Pu-240 and Pu-241.[34] Weapon-grade plutonium contains a concentration of 93% of Pu-239, and 7% or less Pu-240. This would be the preferable option for a terrorist organisation. Yet, reactor grade plutonium – with 18% to 30% of Pu-240 - is also often considered as feasible to be used in a crude nuclear device.[35] The bare critical mass of the isotope Pu-239 is 10 kg.[36] Weapon-grade Pu-239 is considered to have a critical mass of around 11.5kg. This is approximately three quarters the critical mass of reactor-grade plutonium.[37] Thus, it is clear that substantially less plutonium would be needed than HEU (see photo 1). As of January 2017, the global stockpile of separated plutonium is about 520 tons.[38] Although this again stresses that there are inherent risks to such a stockpile, it should be noted that this type of fissile material can only be used in the more complex implosion-type design (infra).

Photo 1. Harold Agnew carrying the plutonium core of the Nagasaki Fat Man bomb, 1945[39]

[32] Willrich & Taylor, "Nuclear Theft: Risks and Safeguards," 12. Bunn, "Guardians at the Gates of Hell," 226.
[33] John McPhee, *The Curve of Binding Energy* (New York: Farrar, Straus and Hiroux, 1980), 35.
[34] Barnaby, *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction,* 88.
[35] Bunn, "Guardians at the Gates of Hell," 226-233.
[36] Sublette, "The Nuclear Weapons Archive: A Guide to Nuclear Weapons."
[37] International Panel on Fissile Materials, "Global Fissile Material Report 2013", 96; Bunn, "Guardians at the Gates of Hell," 229.
[38] International Panel on Fissile Materials. Available at: http://fissilematerials.org/ (accessed August 22, 2018)
[39] Source: Los Alamos National Laboratory

In order to further substantiate my claim that the exact type and quantity of fissile material will have an impact on the other hurdles in a nuclear terrorism project, I will elaborate more on the different forms in which fissile material can be obtained. My goal in the following paragraph is not to provide a comprehensive overview on the various forms of fissile material. Rather, it is to illustrate how the diverging features of the material can influence the following steps in a nuclear terrorism scenario. I will highlight the role of the element, the shape, the chemical composition and the emitted radiation of the fissile material.

First, the role of the element of the fissile material refers to the difference in obtaining HEU or plutonium. Plutonium is generally considered to be less desirable for a terrorist organisation. It impedes the use of the more simple gun-type design and is more toxic and radioactive than uranium. Moreover, as a metal, plutonium is considered to be more difficult to handle than HEU.[40] Second, the design and assembly of a crude nuclear device is also influenced by the shape of the fissile material. Fissile material might need to be casted in the appropriate shape before it can be used in a nuclear device. For instance, an important difference is whether the material comes in an oxide or metal form. Given the density of a metal shape, this would most-likely be the most preferable option for a terrorist organisation.[41] Third, HEU and plutonium both exist in a wide range of chemical forms. In general, a distinction can be made between mixed compounds or (more) pure compounds. While mixed compounds could be used directly – although putting more strict requirements to the quantity of material and concentration of weapon-usable material – more pure compounds are most suitable to be used in nuclear weapons. Recipients of mixed compounds would probably prefer to, or have to, separate the HEU or plutonium. While this is generally considered to be relatively easy, the complexity of processing the material ultimately depends on the exact type of material.[42] Finally, the emitted radiation can lead to extra challenges throughout the implementation of a nuclear plot. While this most likely will not cause any substantial and direct health problems, it is worth noting that plutonium is more radioactive and radiotoxic than HEU. This, for instance, modestly increases the chance that the stolen items might be found back or detected when illicitly smuggled.[43]

Having elaborated on the importance of the type and quantity of fissile material, I will now reflect upon how a terrorist organisation might obtain this necessary ingredient for any nuclear device. It is generally believed that a terrorist organisation cannot indigenously produce fissile material. Mining, milling and

[40] Bunn, “Guardians at the Gates of Hell," 221.
[41] See, e.g., Willrich & Taylor, “Nuclear Theft: Risks and Safeguards,” 13.
[42] Bunn " Guardians at the Gates of Hell", 239-243.
[43] Ibid., 221.

enriching natural uranium still requires a complex, timely, expensive, and large-scale industrial endeavor. This would require a substantial investment by a terrorist organisation and would raise the risks of detection dramatically.[44] I thus assume that a terrorist organisation would aim to externally procure fissile material.[45] Zooming in on this pathway, the literature on this theme generally identifies three options to obtain fissile material: (1) by means of systematic state assistance, (2) via theft or attack, or (3) by purchasing the fissile material.[46]

First, a terrorist organisation could acquire fissile material via systematically organised state assistance. There are no publicly documented cases of such a scenario. Yet, some states, such as those with cordial relations with a terrorist organisation or those that would face imminent regime change, might potentially be inclined to support terrorist organisations. Terrorist organisations could help these states by hurting these states' opponents.[47] In this scenario, a terrorist organisation would be relieved from various challenges to the acquisition process. Yet, even though that this is one potential pathway, this nuclear terrorism scenario adopts the argument that any state would be inherently reluctant to relinquish control over this precious material. On the one hand, the loss of control could result in the counterproductive use of the fissile material by the terrorist organisation. The terrorist organisation might not act in line with the preferences of the state. On the other hand, even a remote prospect of retaliation is likely to have a strong deterrent effect. The possibility of attribution to the responsible state is expected to reduce the likelihood of systematically organised state assistance.[48] This, however, does not imply that this scenario precludes assistance by rogue elements within the state apparatus.

---

[44] Admittedly, there is currently some research on more simple enrichment procedures (e.g, Scott Kemp, "The Non-proliferation Emperor Has No Clothes: The Gas Centrifuge, Supply-Side Controls, and the Future of Nuclear Proliferation," *International Security* 38, no. 4 (2014): 39-78; M. D. Zentner, G. L. Coles, and R. J. Talbert, *Nuclear Proliferation Technology Trends Analysis,* PNNL-14480, *Pacific Northwest National Laboratory*, 2005). This might imply an increased possibility for terrorist organisations to enrich fissile material themselves. Moreover, it is also true that some facilities – such as clandestine centrifuge facilities – might be difficult to detect by counterterrorism forces. Yet, at this moment in time, the cost and complexity of such an endeavour still leads me to assume that this is an unrealistic scenario for any terrorist organisation.

[45] There are different cases of fissile material gone missing. See, e.g.: Henry Sokolski, *Nuclear Weapons Materials Gone Missing: What Does History Teach?* (United States: Strategic Studies Institute and U.S. Army War College Press, 2014).

[46] See for instance: Ferguson and Potter, *The Four Faces of Nuclear Terrorism*; Bunn, "Guardians at the Gates of Hell"; Ackerman et al., "Anatomizing Radiological and Nuclear Non-State Adversaries."

[47] Ferguson and Potter, *The Four Faces of Nuclear Terrorism,* 125-127.

[48] This is also suggested by quantitative research by Victor H. Asal, Gary A. Ackerman, and R. Karl Rethemeyer, "Connections Can Be Toxic: Terrorist Organisational Factors and the Pursuit of CBRN Weapons," *Studies in Conflict & Terrorism* 35, no. 3 (March 2012): 243. They found that there appears to be no effect from state sponsorship on the decision to pursue CBRN weapons by a terrorist organisation. This "further lends weight to the claims that nation-states are leery of assisting or encouraging their terrorist proxies in any CBRN endeavors, viewing such a proposition as far too risky and destabilizing. The lack of any correlation (or even a consistent sign on the relationship) between CBRN use and state sponsorship in the historical record perhaps signals that state sponsors go out of their way to discourage the use of CBRN amongst their proxies."

Indeed, this type of lower-level inside assistance is often part of the second and third options to obtain fissile material. This scenario considers these options to be more-likely options for a terrorist organisation pursuing the acquisition of fissile material.

The second pathway that is often identified by experts is the acquisition of fissile material by means of theft or attack of a nuclear facility.[49] As mentioned earlier, this type of scenario often entails state officials and/or fissile material workers and custodians that might assist the terrorist organisation. These insiders might be motivated by, e.g., economic incentives, coercion, or ideological beliefs. Yet, notwithstanding potential insider assistance, such a scenario would still not be a standard effort for a terrorist organisation. For instance, the RANNSAD database (Radiological and Nuclear Non-State Adversaries Database) identifies 32 "higher threat" cases (that were at least moderately substantiated) of security incidents at facilities that housed sensitive nuclear materials. The apparent motivation of these perpetrators ranged from making a symbolic statement, disrupting the facility's operation, or the actual search for nuclear material.[50] While this shows that the threat is real, this limited number of cases simultaneously illustrates that such a scenario is not *business as usual* for a terrorist organisation. A few of the most likely tasks in doing so are the identification and reconnaissance of the target, brokering reliable contacts to carry out the mission, ensuring the flow of material and financial support, circumventing security measures at the target, and establishing a viable way out. Considering these tasks and the clandestine operational environment in which they need to be completed, this scenario expects that the likelihood that unexpected problems will arise throughout the implementation of this plot is relatively high. A prime example is the often cited "Pelindaba case." This case refers to a substantial security breach in the Pelindaba nuclear facility (in South Africa) by two teams of unidentified assailants with unknown intentions. Both teams succeeded in penetrating the guarded perimeters of the facility. Yet, one team that entered the control center came across an off-duty facility firefighter. This guy, Anton Gerber, was however not supposed to be there at that time.[51] He succeeded in alerting security. While this case is – rightly so - often referenced to because of the substantial security weaknesses it exposes, it simultaneously illustrates the possibility of unexpected situations for the perpetrators implementing the attack.

---

[49] For a more detailed explanation, see: Willrich & Taylor, "Nuclear Theft: Risks and Safeguards," 107-120. Ferguson and Potter, *The Four Faces of Nuclear Terrorism,* 127-131.

[50] For more detailed information, see Gary Ackerman and James Halverson, "Attacking Nuclear Facilities: Hype or Genuine Threat?," in Brecht Volders & Tom Sauer (eds.), *Nuclear Terrorism: Countering the Threat*, Global Security Studies (London & New York: Routledge, 2016). These incidents were not always terrorism related.

[51] Based on reports by, e.g.: CBS News, "Nuke Facility Raid An Inside Job?" Available at: https://www.cbsnews.com/news/nuke-facility-raid-an-inside-job-19-06-2010/ (accessed August 22, 2018). Micah Zenko, "A Nuclear Site Is Breached. "Available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/12/19/AR2007121901857.html (accessed August 22, 2018).

Finally, the literature on this theme refers to the purchase of fissile material on a nuclear black market as the third possibility for a terrorist organisation to acquire fissile material.[52] Reference is often made to the Incident and Trafficking Database of the IAEA – with a particular emphasis on trafficking issues in the Black Sea region – or Abdul Qadir Khan's nuclear smuggling network. While there is – to my knowledge - no publicly available evidence on a functioning black market that connects smugglers with terrorist organisations, these example do illustrate the possibility of the clandestine proliferation of nuclear technology and material.[53] Yet, the adopted scenario does not expect this to be a standard effort for a terrorist organisation. While such a scenario would not entail the same need for military-style capabilities, it would require the capability to connect to a nuclear black market and organise a transfer. Some of the most likely tasks and activities would be the brokering of reliable contacts, raising a sufficient amount of money, setting up and hiding large financial transactions, and organising the secure transfer of the material.[54] The implementation of these tasks in a clandestine operational environment would probably imply an increased likelihood that any unexpected situations would arise. It appears, for instance, that "Qaeda has been scammed on several other occasions in attempts to acquire what it thought was weapons-usable nuclear material."[55]

In conclusion with respect to this first hurdle in the adopted nuclear terrorism scenario, it is plausible to assume that this hurdle would require - at least - a small group of people with diverse skills. These skills will depend on the exact pathway the terrorist organisation adopts (e.g. operational military skills, networking skills, coordinating skills, and/or financial skills). As a way of example, Matthew Bunn suggests that a group of 4-9 well armed outsiders and 1-2 insiders would have a reasonable chance of success in stealing fissile material out of a facility with modest nuclear security measures.[56] Obviously, the group's operational environment and resources will inherently impact the exact challenges they face.[57] Yet, taking into account these tasks and activities, and the organisation's clandestine operational

[52] See, e.g., Rolf Mowatt-Larssen, "The Armageddon Test: Preventing Nuclear Terrorism," *The Bulletin of the Atomic Scientists*, 2009, 60–70.
[53] See, e.g., Molly MacCalman, "A.Q. Khan Nuclear Smuggling Network," *Journal of Strategic Security* 9, no. 1 (March 2016): 104–18.
[54] Considering this third option, respondents of the Lugar survey generally believed this option to be the most-likely option for a terrorist organisation (Lugar, "The Lugar Survey On Proliferation Threats and Responses," 16). There are, however, also more sceptical opinions. See, e.g. Sonia Ben Ouagrham-Gormley, "An Unrealized Nexus? WMD-related Trafficking, Terrorism, and Organised Crime in the Former Soviet Union," *Arms control today* (2007). Available at: https://www.armscontrol.org/act/2007_07-08/CoverStory (accessed April 2, 2019). Given the uncertainty and secrecy related to nuclear terrorism hampers an in-depth assessment of the exact scenario, I will not position myself exactly in this debate. As will become clear, the adopted nuclear terrorism scenario just assumes that terrorist organisations will externally acquire the fissile material.
[55] Bunn, "Guardians at the Gates of Hell," 41.
[56] Ibid., 169.
[57] In this context, the importance of the group's geographical location should be highlighted. For instance, Ackerman and Halverson ("Attacking Nuclear Facilities") illustrate that - notwithstanding that incidents in nuclear

environment, any unnoticed security measures, (moral) doubts by the perpetrators, early detection of the plot, or any other contingent factors (e.g. personal disagreements) might lead to unexpected situations that were not foreseen by the terrorist organisation. These exceptional situations can interfere with the successful implementation of the plot.

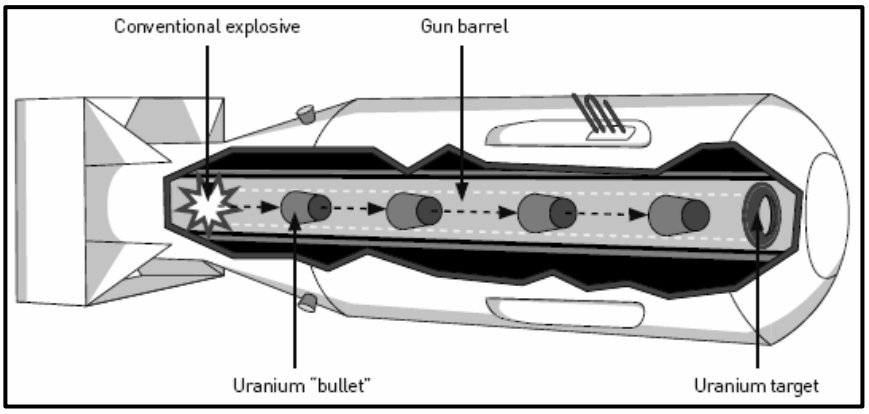
Assembly of the nuclear device

The second key hurdle in the adopted nuclear terrorism scenario is the assembly of an improvised nuclear device. The literature on this theme generally divides this hurdle in the development of a functioning design, the acquisition of the necessary non-nuclear components, and the actual construction of the atomic device in a sufficiently safe and secure manner. As indicated in figure 2.3, it might be that a terrorist organisation starts the two first tasks while awaiting the opportunity to acquire fissile material. As mentioned before, some tasks in a nuclear plot might be taken in parallel. Yet, this does not change the fact that these different steps need to be attuned to each other. The exact design, the necessary non-nuclear components, and the actual construction of the nuclear device need to be aligned with each other. This is ultimately function of the type and quantity of fissile material that the terrorist organisation might obtain. I will first elaborate on the technicality of these issues before outlining the corresponding tasks and activities related to this hurdle.

First, a terrorist organisation would need to develop a functioning design for an improvised nuclear device. The gun-type design and the implosion-type design are two proven types of first generation nuclear weapons. While both options are considered possible in the adopted nuclear terrorism scenario, it is worth mentioning that the publicly available literature often identifies the gun-type design as the easiest design for a nuclear device.

facilities have been relatively widely dispersed - it seems that "the threat has historically been concentrated in regions with a higher density of nuclear facilities." Proximity to a nuclear facility would thus probably facilitate the terrorist organisation's implementation of such a plot.

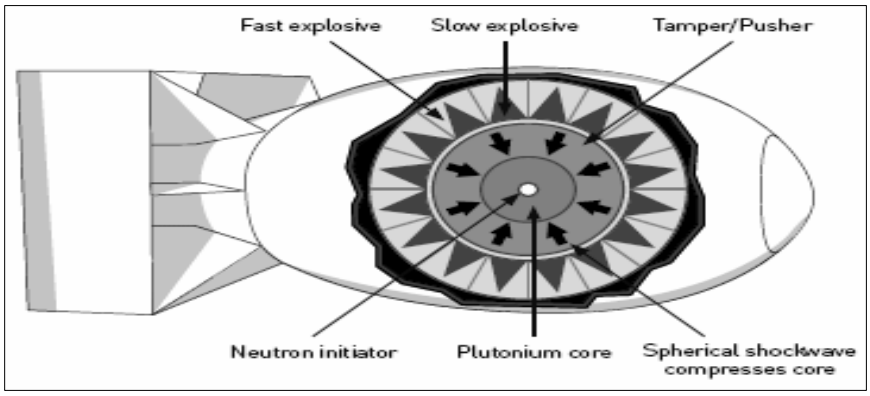
Figure 2.5. A gun-type design



Considering a gun-type design, one subcritical configuration of fissile material – the bullet – is fired through a barrel to another subcritical configuration of fissile material – the target (see figure 2.5). Once these subcritical configurations come together, they can form a supercritical configuration. A type of conventional explosive probably needs to be used to drive the subcritical configurations together. This method of assembly is a relatively straightforward method, but - considering the slow pace at which it creates a supercritical configuration – it is also a relatively *inefficient* way to create a nuclear explosion. This does not mean that it cannot create a substantial yield (e.g. *Little Boy* was based on a gun-type design). Yet, the slow pace of assembly leads to a rapid start of the chain reaction. Neutrons can more easily escape – rather than create new fissions – thereby quickly establishing a subcritical configuration of fissile material again. As only a small amount of fissile material will actually fission during the explosive chain reaction, this type of design requires a higher amount of fissile material.[58] Moreover, this type of design is only feasible by making use of HEU. Considering plutonium generates a high neutron background, a plutonium gun-type device would almost certainly result in a pre-detonation.[59] This would result in a detonation of only a few tons to perhaps 10-20 tons.[60] If a terrorist organisation would be able to acquire plutonium (or an insufficient amount of HEU), they are thus better off in opting for an implosion-type design in case they hope to develop a substantial nuclear explosion.

[58] Ferguson and Potter, *The Four Faces of Nuclear Terrorism,* 131
[59] Lillian Hoddeson et al., *Critical Assembly: A Technical History of Los Alamos During the Oppenheimer Years, 1943-1945* (United Kingdom: Cambridge University Press, 2004), 228-248.
[60] Bunn, "Guardians at the Gates of Hell," 221.

Figure 2.6. An implosion-type design



Rather than firing two subcritical configurations together, the implosion-type design aims to implode a single subcritical mass of fissionable material (see figure 2.6).[61] Imploding the fissile material leads to an increase in its density. This potentially leads to a supercritical configuration. As Bunn & Wier state: "The critical mass decreases with the square of the density, so if the nuclear material can be crushed to twice its normal density, only a quarter as much material would be needed."[62] High-speed explosives are spread evenly over a subcritical configuration of fissile material. Precision-timing of the explosion is necessary to crush the critical material into a smaller sphere. If the timing is off, it might flatten the material rather than increase its density. Moreover, Bunn explains that "an implosion device using either plutonium with a low Pu-240 content or HEU requires a means for generating a burst of neutrons to start the chain reaction at the right moment, before the conventional explosion destroys the configuration that will sustain a nuclear chain reaction."[63] This refers to the use of an initiator, which is not considered to be absolutely necessary for the gun-type device (the South-African nuclear program, e.g., produced gun-type device nuclear weapons without an initiator).[64] These type of design issues make an implosion-type design a more complex design than a gun-type design.

Both types of design could - or potentially would need to - make use of a reflector to enhance the efficiency of the nuclear device. This refers to material that surrounds the fissile material and reflects the neutrons back. Less neutrons will escape. This implies a reduction in the amount of required fissile

[61] Blair, "Jihadists and Nuclear Weapons," 198.
[62] Bunn and Wier, "Terrorist Nuclear Weapon Construction: How Difficult?" 134.
[63] Bunn, "Guardians at the Gates of Hell," 61. Bunn notes in this respect that terrorist organisations might prefer reactor-grade plutonium because it has higher neutron background (and they might thus be able to do without a neutron generator).
[64] For a more detailed description on initiators, see, e.g. "Military Critical Technologies List (MCTL) Part II: Weapons of Mass Destruction Technologies, Nuclear Systems Technology," *U.S. Department of Defense,* 1998, Section 5, 60. Available at: http://www.fas.org/irp/threat/mctl98-2/p2sec05.pdf (accessed April 2, 2019).

material or an increase in the yield of the device.[65] Thus, in case a terrorist organisation was not able to obtain an appropriate quantity of fissile material, the use of a reflector might enable them to nevertheless create a substantial nuclear explosion.

Second, besides the development of a functioning design, I assume that a terrorist organisation would need to acquire a diversity of non-nuclear components as well. On the one hand, this can refer to the required tools and machining equipment to assemble the nuclear device. Some of the most often mentioned tools are, e.g. metallurgical melting and casting furnaces, robotics, glove boxes, metrology tools, chemical processing tools, or tools for removing or cutting metals.[66] On the other hand, non-nuclear components can also refer to other components of the nuclear device. In case of a gun-type design, this can refer to a gun barrel, a chemical explosive propellant, and some kind of firing circuitry. In case of an implosion-type design, this can refer to high-explosive lenses. In case the design of the device would require an initiator and/or reflector, the terrorist organisation would respectively need to require access to beryllium (or some other light element) and a suitable alpha emitter,[67] and/or access to reflector material such as beryllium, tungsten and, possibly, iron.[68]

This assumption that non-nuclear components will be necessary follows from the fact that the adopted nuclear terrorism scenario assumes that the acquired fissile material will need to be processed and adapted to some extent before it can be used in an improvised nuclear device. In other words, the terrorist organisation will carry out some work to prepare a supply of fissionable material of adequate purity and shape.[69] Admittedly, this assumption is open to debate. Luis Alvarez, for instance, notably claimed that a terrorist organisation "would have a good chance of setting off a high-yield explosion simply by dropping one half of the material onto the other half." [70] If this is true, this assumption that some preparation will need to be carried out seems unlikely. Yet, I nevertheless stand with this assumption in the adopted nuclear terrorism scenario. On the one hand, various experts have

[65] Levi, *On Nuclear Terrorism*. 45-46. Maerli, Schaper and Barnaby, for instance, state that a beryllium reflector of 15 cm thick could reduce the required critical mass to 12 kg. Maerli, Schaper, and Barnaby, "The Characteristics of Nuclear Terrorist Weapons," 737-738.

[66] For an overview on components to manufacture nuclear technology, see "Military Critical Technologies List (MCTL) Part II: Weapons of Mass Destruction Technologies, Nuclear Systems Technology," Other interesting literature referring to this topic is, e.g., Anna Pluta & Peter Zimmerman, "Nuclear terrorism: A disheartening dissent," *Survival* (2006), 55-69. (Note in this respect that Peter D. Zimmerman chaired the interagency technical working group that evaluated the technologies, set the limits and produced the MCTL).

[67]"Military Critical Technologies List (MCTL) Part II: Weapons of Mass Destruction Technologies, Nuclear Systems Technology," 60.

[68] Ibid., 62; Levi, *On Nuclear Terrorism,* 45-46.

[69] John Foster, cited in Willrich & Taylor, "Nuclear Theft: Risks and Safeguards," 7.

[70] Luis Alvarez, *Adventures of a Physicist*, vol. Alfred P. Sloan Foundation Series (New York: Basic books, inc., Publishers, 1987), 125.

confirmed to me that the Alvarez quote is true, even though the explosion would probably be a small one.[71] On the other hand, other experts have argued that this quote might be exaggerated. Pluta and Zimmerman, for instance, stated that "if the device to be fabricated were to be gun-assembled… the requirements on technology decrease substantially, although not to the level of the Alvarez concept described earlier."[72] Notwithstanding the exact veracity of these quotes, it is however important to note that Alvarez ultimately seemed to assume that a terrorist organisation would obtain an appropriate type and quantity of fissile material.[73] Yet, while it is true that the nuclear security regime remains vulnerable,[74] it is also true that progress has been made in protecting vulnerable sources of fissile material. See, for instance, at the achievements of the Nuclear Security Summits.[75] It is thus not the case that the most preferable type and quantity of fissile material is simply available to a terrorist organisation. Research reactors seem, for instance, the most vulnerable targets. Yet, a terrorist organisation would most-likely need to remove the aluminum from the fissile material being used in a research reactor (e.g. in fresh fuel).[76] Taking together these considerations, the adopted nuclear terrorism scenario thus assumes that the terrorist organisation will need to carry out some work to prepare a supply of fissionable material of adequate purity and shape.[77] Non-nuclear components and skills will consequently be necessary.[78]

This brings us to the third and final technical step in this hurdle: the actual fabrication of the nuclear device. Considering the uncertainty and secrecy with respect to the exact pathway of a nuclear terrorism

[71] Conversations with Zia Mian & Moritz Kutt, 18th of September 2018. Conversation with Frank Von Hippel, 19th of September 2018. Conversation with Alexander Glaser, 20th of September.
[72] Pluta & Zimmerman, "Nuclear terrorism: A disheartening dissent," 63; Bunn, "Guardians at the Gates of Hell," 214; Ackerman et al., "Anatomizing Radiological and Nuclear Non-State Adversaries," 69; Levi, *On Nuclear Terrorism,* 15-18.
[73] Alvarez does not specify the type and quantity of fissile material that would be necessary.
[74] See, for instance, the report by Brian Danielle and Stockton Peter, "U.S. Nuclear Weapons Complex: Security at Risk," the Project on Government Oversight (POGO), 2001 (available at: https://www.pogo.org/report/2001/10/us-nuclear-weapons-complex-security-at-risk/#heading-15). This report states, for instance, "In a force-on-force test in October 2000 at TA-18, at Los Alamos, the protective force failed to stop the "terrorists" from gaining access - therefore a sizable nuclear detonation was possible."
[75] See, e.g., Graham Allison, "Did We Beat the Odds or Change Them?" *Prism* 7, no. 3 (2018): 9; Matthew Bunn et al., "Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline" (Cambridge: Harvard Belfer Center, March 2016); Matthew Bunn et al., "Advancing Nuclear Security: Evaluating Progress and Setting New Goals," Project on Managing the Atom (Cambridge: Harvard Belfer Center, March 2014).
[76] Conversation with Moritz Kutt, 18th of September 2018; Conversation with Frank Von Hippel, 19th of September 2019. Von Hippel, for instance, stated that "it is harder than it was" to obtain the appropriate type and quantity of fissile material. Conversation with Alexander Glaser, 20th of September 2018.
[77] Willrich & Taylor, for instance, also seem to imply that some work will be necessary when they reflect upon the skills and non-nuclear resources required to make a fission bomb. Willrich & Taylor, "Nuclear Theft: Risks and Safeguards," 20-21.
[78] Remember that the adopted scenario does not formulate any absolute claims on the probability of this scenario. It merely provides a way to structure my reasoning. In what follows in this dissertation, I will also point to other scenarios.

plot, I cannot go in more depth with respect to the exact technical tasks related to the actual fabrication of the nuclear device. Yet, considering the previous assumptions, some of the most-often mentioned tasks are, e.g, the casting of fissile material in the right shape, the actual manufacturing of the gun-type or implosion-type arrangement, and the potential testing of non-nuclear components (e.g. after the firing mechanism is triggered in a gun-type design, the velocity of the propellant that would move the bullet towards the target might need to be tested).[79] This latter issue again clearly touches upon the fact that there are different technical requirements for different types of improvised nuclear devices. A more efficient nuclear device – which refers to a device that releases a high amount of energy in relation to the total amount of energy that could have been released – can be achieved by a more precise and correct construction of the design (e.g. via testing), an increasingly sophisticated design (e.g. the inclusion of a reflector), or access to a more appropriate type of fissile material. It follows that the creation of a nuclear explosion of a few tons to a 100 tons is technically less challenging than the development of crude nuclear device with a 15kT yield. This study reflects upon the differences between such diverging scenario's throughout the following chapters.

Going beyond these technical tasks – which are hard to pinpoint exactly due to the uncertainty of the exact nuclear terrorism pathway – I will now turn to the corresponding tasks and activities that this hurdle would probably entail for a terrorist organisation. As mentioned before, the adopted nuclear terrorism scenario assumes that a terrorist organisation would not receive systematically organised state assistance in assembling the improvised nuclear device. I believe a state would not want to lose control over this type of technology and would fear the potential retaliation by opponents. This subsequently implies the following challenges for a terrorist organisation.

On the one hand, it has become clear that a variety of the expected tasks and activities (e.g. the drawing of a feasible design, the processing of fissile material, or the testing of the bomb components) requires particular tangible and intangible skills and expertise. Scientists and technicians need to alter the raw fissile material into a functioning crude nuclear device. A terrorist organisation would thus need to recruit (or train) and steer people with these necessary skills. The literature on this topic often mentions

[79] This issue is topic of debate: Nic Von Wielligh, for instance, states that testing is a necessary part of any nuclear terrorism plot (Written correspondence, 22nd of April 2017). Ferguson & Potter state that the testing of components is likely (Ferguson and Potter, *The Four Faces of Nuclear Terrorism*, 134). Others (e.g. Stanislav Rodionov, "Could Terrorists Produce Low-Yield Nuclear Weapons?" High-Impact Terrorism: Proceedings of a Russian-American Workshop, National Academies Press, 2002), 5) do not agree. I therefore conclude that the testing of components (not the bomb as a whole) would probably improve the likelihood of an efficient improvised nuclear device, and would be preferable for a terrorist organisation. They do not want to minimize the likelihood that they completely ruin the precious material. It would intensify the dynamics outlined in what follows in this dissertation.

the (potential) need for nuclear physicists, metallurgists, explosives experts, chemists, engineers, and/or electricians.[80] These people might be inclined to cooperate due to, e.g., coercion by the terrorist organisation, economic incentives, or ideological beliefs. For instance, scholars often point to disgruntled scientists in Iran, Russia or Pakistan that might help a terrorist organisation in pursuing a nuclear capacity.[81] On the other hand, a terrorist organisation would need to set up a machine shop and secure its people throughout the assembly of a nuclear device. The organisation would need to procure the necessary non-nuclear components while hiding from law enforcement efforts. This can happen via means of theft, attack or purchase. While generally not considered to be the hardest challenge to a nuclear terrorism plot, the necessity and availability of these components will to some extent be function of the exact type and quantity of fissile material and the sophistication of the design. Next, this machine shop – and the people working in it – will need to be secured. The organisation needs to remain wary that neither noises nor effluents from the group's work would be detected.[82] Ramzi Yousef's so-called Bojinka plot, for instance, was detected by the Philippine authorities after his work with chemicals accidentally caused a fire in his apartment. In this respect, it is interesting to refer to the role and impact of the geographical location of a terrorist organisation. Its operational environment can facilitate or complicate the safekeeping of their facilities and a nuclear terrorism plot.

In conclusion with respect to the second key hurdle in this nuclear terrorism scenario, it is thus plausible to assume that this step will also require a (small) group of people with a skillset that is – for the most part - different from the skills that were needed in the previous step in this scenario (e.g. nuclear physicist and engineers, electricians, people with illicit procurement experience, recruiters, or explosives experts). Building on the publicly available literature on this topic, the adopted nuclear terrorism scenario assumes that a small team – ranging between 5 to 20 people – will be necessary to assemble the nuclear device.[83] It might however be possible that this team consists of more persons. Considering the technical complexity of the different tasks and the organisation's clandestine operational environment, the adopted scenario again entails a relatively high likelihood of exceptional

[80] See, e.g., Zimmerman and Lewis, "The Bomb in the Backyard"; Bunn, "Guardians at the Gates of Hell"; Carson Mark et al., "Can Terrorists Build Nuclear Weapons?" (Washington: Nuclear Control Institute, 1987), http://www.nci.org/k-m/makeab.htm; Ferguson and Potter, *The Four Faces of Nuclear Terrorism*; Albert Narath, "The Technical Opportunities for a Sub-National Group to Acquire Nuclear Weapons," XIV Amaldi Conference on Problems of Global Security, April 27, 2002. Note in this context that, even if the scenario would become technically less complex, these people are still required to identify the possibility and opportunity for such a type of attack (e.g. identify where the best type and quantity of fissile material is available).

[81] See, e.g., Ferguson and Potter, *The Four Faces of Nuclear Terrorism,* 223.

[82] Bunn, "Guardians at the Gates of Hell," 215.

[83] See, e.g., Zimmerman and Lewis, "The Bomb in the Backyard"; Bunn, "Guardians at the Gates of Hell"; Mark et al., "Can Terrorists Build Nuclear Weapons?"; Ferguson and Potter, *The Four Faces of Nuclear Terrorism*; Narath, "The Technical Opportunities for a Sub-National Group to Acquire Nuclear Weapons"; Willrich & Taylor, "Nuclear Theft: Risks and Safeguards," 20-21.

problems to arise that are hard to systematically analyse in advance. I expect various instances of, e.g., unexpected engineering hick-ups or errors, a (threat of) interruption by law enforcement efforts, (moral) doubts or personal disagreements by perpetrators, or any other contingent factors that might interfere with the effective implementation of the assembly of a nuclear device.

Transport the nuclear and/or non-nuclear device or components

The third key hurdle in the adopted nuclear terrorism scenario is the transport of the nuclear and/or non-nuclear device or components. This refers to the illicit transport of fissile material or non-nuclear components to the machine shop and/or the illicit transport of the (assembled) nuclear device to the target.[84] Admittedly, this is an issue of substantial debate in the literature. Zimmerman and Lewis, for instance, consider a terrorist organisation to be more likely to build the device within the target country. This would eliminate "the risks of moving the bomb [or its nuclear and non-nuclear components] across a border."[85] Moreover, it is also true that several terrorist organisations have set up relatively complex machine shops in the countries that they have attacked (e.g. the FARC's production of submarines in Colombia). This would limit the need to illicitly transport nuclear or non-nuclear components. Yet, considering the potential loss of a vast amount of investments by the terrorist organisation and the potential backlash to the group when detected, I believe a terrorist organisation would be reluctant to assemble the device in the target country. The targeted country is probably hostile towards the terrorist organisation. Procuring nuclear and non-nuclear components, securing the machine-shop, and protecting and steering the assembly team would become less challenging in case the terrorist organisation operates in a less hostile environment. This enables the group to maximise security while assembling this unique and valuable device; a process which could easily take several months. Considering the plot as outlined in figure 2.3, note that the dotted line indicates that the illicit transport might take place at any point throughout the project. It is not possible to pinpoint the exact timing and might happen in parallel with some of the other tasks. Moreover, the double arrow in the figure highlights that the required nuclear and non-nuclear components will influence the exact requirements for this step. I will first elaborate on this latter technical issue before outlining the different tasks and activities related to this hurdle.

[84] This is discussed by, e.g., Michael Levi, *On Nuclear Terrorism*; Steve Sin and Marcus Boyd, "Searching for the Nuclear Silk Road: Geospatial Analysis of Potential Illicit Radiological and Nuclear Material Trafficking Pathways," in Brecht Volders & Tom Sauer (eds.), *Nuclear Terrorism: Countering the Threat*, Global Security Studies (London & New York: Routledge, 2016), 159–81; Ferguson and Potter, *The Four Faces of Nuclear Terrorism*; Rolf Mowatt-Larssen et al., "The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism"; Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (United States: Holt Paperbacks, 2005).
[85] Zimmerman and Lewis, "The Bomb in the Backyard."

First, the illicit trafficking of fissile material is influenced by the type and quantity of this material. Nuclear material emits particles – nuclear radiation – that are susceptible to detection. Gamma rays and neutrons are most often the primary targets of a radiation detector. Yet, radiation detection is hard. The main challenge for any nuclear detector is the need to distinguish between radiation by actual nuclear material and - so-called - background radiation. Background radiation is present in every environment, but the amount of radiation is not known exactly. It is therefore complex to detect whether the amount of radiation follows from a source of nuclear material or is just the consequence of background radiation. The likelihood that the illicitly trafficked nuclear material will be detected depends on, e.g., the availability of detection tools, geographical distance of the tool to the radiation source, the observation time, and the amount, type and shielding of the fissile material.[86] Considering the latter, it should be noted that plutonium is slightly more radioactive than HEU. Yet, neither of both sources is considered "radioactive enough to require any special equipment to carry them, or to make them easy to detect."[87] Graham Allison, for instance, refers to ABC news successfully smuggling depleted uranium – which gives a radiological signature similar to weapon-grade uranium when it is shielded – from Indonesia to one mile from the Los Angeles Convention Center.[88] The overall likelihood of detection of nuclear material is generally considered to be low.

Second, this hurdle also refers to the illicit smuggling of various non-nuclear components. Like the illicit trafficking of nuclear material, this task is generally not considered to be very difficult. Many of the relevant items can be easily bought or stolen and subsequently smuggled to the machine shop or target country. Given the uncertainty and secrecy with respect to the exact pathway of a nuclear terrorism plot, it is hard to systematically describe the availability and control over the exact non-nuclear components required. Yet, Zimmerman & Lewis gave a few illustrative examples: considering a gun-type design, they argued that "terrorists could use a surplus light artillery gun barrel, something that's easily available today on the global arms market or the Internet for much less than $10,000." Likewise, considering the tools that probably would be necessary in a nuclear terrorism plot, they state that "the group could find the vacuum furnace to fit their specifications by searching on the Internet, and could probably purchase it for less than $50,000," and "new or used lathes large enough to properly finish the roughly cast pit can be bought on the Internet, even on eBay, for $10,000 … our terrorist outfit could probably find all the standard machine shop equipment it would need in any university physics department."[89] While Zimmerman & Lewis assume that the device will be built within the target country,

[86] Levi, *On Nuclear Terrorism,* 49-61.
[87] Author unknown, "Nuclear Terrorism FAQ's", *Harvard Belfer Center,* 2007. Available at: http://belfercenter.ksg.harvard.edu/publication/17529/nuclear_terrorism_faq.html (accessed April 2, 2019).
[88] Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 105.
[89] Zimmerman and Lewis, "The Bomb in the Backyard."

the abundant availability of most components suggests that illicit trafficking of this material will be relatively easy as well. Indeed, although the availability and control over various necessary non-nuclear components will become more complicated in case of a more sophisticated nuclear design, experts generally agree that the illicit trafficking of non-nuclear components is no difficult task.[90]

Going beyond these technical issues, the question remains how a terrorist organisation would actually go about in illicitly trafficking nuclear or non-nuclear material or components. While this hurdle to the adopted nuclear terrorism scenario is generally considered to be relatively easy, it does involve some particular tasks and activities that need to be completed.

A terrorist organisation would first need to compile a list of goods that they would need in order to construct a nuclear device. Next, the organisation needs to identify the "suppliers" of this material. In doing so, nuclear expertise needs to be combined with (illicit) trafficking expertise. As mentioned before, the acquisition of material can happen via theft, attack or purchase. I assume that the terrorist organisation will not receive systematic state assistance. Next, in case they are able to successfully identify the material, terrorist organisations need to identify a preferable pathway to transport the material to either the machine shop and/or the target country. The potential speed and probability of success depends on, e.g., the group's geographical location and boundaries, the material that needs to be smuggled, the security measures in place, and the group's operational resources. This determines the advantages and disadvantages of each potential route.[91] Important decisions need to be made throughout this process. For instance, considering the potential trafficking of a nuclear device to the target country, the organisation has to choose between smuggling the precious good as one intact device or smuggle the diverse components separately. The terrorist organisation would thus need to have access to an adequate number of people familiar with trafficking techniques, tactics and procedures. This group would need to remain secure and loyal throughout the implementation of this third hurdle. For instance, a terrorist organisation might outsource some of these tasks to a criminal organisation or conventional transporting firms. They might make use of middlemen, brokers and/or other intermediaries involved in the smuggling of the material. Yet, the question then becomes whether these persons can be trusted with the terrorist organisation's precious goods. There is always a risk that

[90] See, e.g., Ferguson and Potter, *The Four Faces of Nuclear Terrorism,* 138-142.
[91] Sin and Boyd, "Searching for the Nuclear Silk Road," 159–81. It is thus very difficult to pinpoint a "most-likely" illicit trafficking pathway. Only looking at potential trafficking methods, for instance, Sin and Boyd identify, e.g., small fixed-wing aircrafts, ultralight aircrafts, business jets, go-fast boats, panga boats, semi-submersibles, illicit foot travel and/or tunnels.

they are confronted with amateur criminals, scam artists or undercover police operations.[92] I therefore assume that – although the organisation can be assisted by outsiders – it would prefer their most valuable goods to be cared for by someone from the own group.

Thus, in conclusion with respect to the third hurdle in this nuclear terrorism scenario, it is plausible to assume that a small team specialised in illicit trafficking techniques, tactics and procedures will be needed in a nuclear terrorism plot. These tasks and activities do not seem to be particularly complex. Yet, they do constitute an extra barrier for any terrorist organisation aiming to effectively complete a nuclear terrorism plot. The group's operational environment (e.g. geographical location) and resources will impact the effective implementation of these tasks. Yet, notwithstanding these variables, there is an inherent risk that unexpected situations which were not analysed in advance by the terrorist organisation will arise throughout its implementation. A scam by a middlemen, unnoticed security measures at the border, or any other other contingent factors might interfere with the effective implementation of the illicit trafficking of nuclear and/or non-nuclear components.

Detonate the (crude) nuclear device

The actual detonation of an improvised nuclear device by a terrorist organisation is often taken for granted in the literature on this theme. McIntosh and Storey argue that the acquisition of a nuclear device should not be equated with the use of this device. They argue that there are other strategic options available as well (e.g. using the weapon as a bargaining chip or deterrent). Yet, considering the detonation of a nuclear device is the focus of most threat assessments on this theme, I start from the assumption that the terrorist organisation would aim to detonate the IND.[93] It is true that this final step in the adopted nuclear terrorism scenario is probably the least challenging one. Yet, the literature on this theme does not sufficiently acknowledge that this hurdle also entails some particular tasks and activities. It should not simply be taken for granted.

---

[92] On the topic of nuclear smuggling, see, e.g., Lyudmila Zaitseva and Kevin Hand, "Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users," *American Behavioral Scientist* 46, no. 6 (2003): 822-844; Lyudmila Zaitseva, "Nuclear Trafficking: 20 years in review", *Contribution to WFS Meeting* 2010. Available at: https://www.belfercenter.org/publication/stopping-nuclear-smuggling; Elena Sokova, "Nuclear material trafficking: historical trends and current patterns," *Presentation at Antwerp workshop on Preventing Nuclear Terrorism: the Role of Nuclear Security,* 2014.

[93] Christopher McIntosh and Ian Storey, "Between Acquisition and Use: Assessing the Likelihood of Nuclear Terrorism," *International Studies Quarterly* 62, no. 2 (2018).

In order to detonate an improvised nuclear device, a terrorist organisation might opt for either an surface burst or an airburst nuclear explosion. A surface burst is a nuclear explosion on the ground. A terrorist organisation might opt, for instance, to rent a truck and drive the truck to the target. This type of explosion will destroy less ground structures but create more radioactive fallout because a lot of debris is pulled into the mushroom cloud. Barnaby, for instance, states that a nuclear explosion equivalent to that of 100 tons of TNT "would produce a crater, in dry soil or dry soft rock, about 30 metres across. The area of lethal damage from the blast would be roughly 0.4 square kilometres."[94] In contrast, an airburst nuclear explosion is a nuclear device that is being detonated when still in the atmosphere. Given that the ground structures do not shield each other, such an explosion will destruct more ground structures. Yet, while the blast radius is bigger, there will be less radioactive fallout because less debris is being pulled in the mushroom cloud. A terrorist organisation might opt, for instance, to rent a (small) airplane and detonate the device in the air. Although a surface burst is by most experts considered to be the most-likely option, it seems that neither of both options is implausible. The adopted nuclear terrorism scenario does assume that the delivery of the crude nuclear device will not happen via means of the "tip of a missile."[95] The development of a nuclear-armed missile is generally considered to be out of reach for a terrorist organisation. They would need to miniaturise the nuclear warhead. Delivery of the device by means of, e.g., a truck or Cessna is less costly, easier to acquire, and more reliable.

Considering this scenario assumes that a terrorist organisation would not receive systematic state assistance – given the loss of control and fear of retaliation by opponents – it is up to the terrorist deployment team to effectively detonate the crude nuclear device at its target. Although the size and composition of this team will depend on the target and delivery method, I expect the need for a small team that - at least - consists of "a "bomber" (the person who actually delivers the weapon to its final target and triggers it), a weapons expert with adequate technical training to ensure that the weapon continues to function after being transported to the staging area, and two or more members to ensure "security" and to engage in the manual labor required to handle the weapon itself."[96] This team needs to remain secure during the implementation of this hurdle. It is true that terrorist organisations have proven that they are capable of setting up a suicide team to carry out such a mission. Yet, similar to the previous hurdles in this nuclear terrorism scenario, it should be noted that any last-minute doubts, malfunctions in the device, detection by counterterrorism forces, or any other contingent factors might

[94] Barnaby, *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction*, 36.
[95] Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 107.
[96] Gary Ackerman, Charles Blair, and Jeffrey Bale, "Anatomizing Radiological and Nuclear Non-State Adversaries Task 2: Potential RN Adversary Behavioral Profiles" (START consortium, 2010). 60.

complicate the effective implementation of this hurdle in the adopted nuclear terrorism scenario. For instance, Ahmed Ressam (the so-called "Millenium Bomber") was captured after a coincidental encounter with a Customs agent that became suspicious when he attempted to cross into the United States at Port Angeles.[97] Such unexpected situations can disrupt the effective implementation of any terrorism plot.

Going beyond this step-by-step development of the adopted nuclear terrorism scenario, the following section will summarise this scenario in order to more systematically reflect upon the nature of technology that a terrorist organisation would face in such a plot. This is necessary to better understand the organisational dynamics and variables in a potential nuclear terrorism project. Moreover, as will become clear, this assessment of the nature of technology will provide the basis for the selection of the empirical cases that are analysed in this study. In this context, I will argue that the adopted nuclear terrorism scenario is characterised by a "nonroutine" nature of technology.

2.1.3. A nuclear terrorism scenario: coping with a nonroutine nature of technology

A broad conceptualisation of the term "technology" is adopted. It refers to the way that an organisation creates the intended output. This broad conceptualisation comprises both the particular knowledge and competences required to complete the diverse tasks and the more general procedures that the group needs to come up with to complete the project.[98] It goes beyond the mere technical tasks of conversing input into output, but also includes, e.g., the procurement procedures to acquire raw materials. Any organisation's performance is to a large extent linked to the actual technology that they aim to adopt. In order to better understand the organisational dynamics and variables in the adopted nuclear terrorism scenario, we thus first need to understand the nature of technology that a terrorist organisation would be confronted with.

In order to do so, I start from Charles Perrow's model with respect to the "technology" variable. On the one hand, while I will add some insights by other authors, the work by this leading organisational

[97] Erik J. Dahl, "The Plots That Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks Against the United States," *Studies in Conflict & Terrorism* 34, no. 8 (2011): 627. This report states, e.g., that some of the reasons for thwarted attacks are "human intelligence, detainee interrogation, chance encounters with police, other law enforcement action, signals intelligence, intelligence from overseas, and public threats and announcements by the terrorists themselves." This points to some of the ways that a terrorism plot can be foiled or thwarted.

[98] This is based on the work by: Jones, *Organisational Theory, Design and Change*, 265-268; Perrow, *Organisational Analysis: A Sociological View,* 76.

sociologist captures best – to my knowledge and assessment - the varying nature of technology and its determinants.[99] Joan Woodward, for instance, identifies 10 levels of technological complexity and how they influence the organisational structure. Yet, she hardly touches upon the determinants of this technology.[100] This complicates our understanding of the challenges to different types of technology. On the other hand, Charles Perrow adopts a two-dimensional framework (in contrast to, e.g., Woodward's 10 levels of technological complexity). This is straightforward and comprehensible. Given that the uncertainty and secrecy related to nuclear terrorism scenarios hampers an in-depth assessment of the exact tasks and activities, this type of lucid matrix is most suitable to enable this study's analysis. Indeed, a more meticulous and detailed classification of the nature of technology of a nuclear terrorism scenario would simultaneously entail a more questionable classification. In this exploratory study, I aim to develop the concept into a form that enables analysis rather than obfuscates it.

This model by Charles Perrow is two-dimensional (see figure 2.7). First, he identifies the "degree of variability of stimuli." This so-called *task variability* refers to the "variety of problems which may lead to search behavior."[101] A high task variability implies that there are high number of new or unexpected situations that a person encounters throughout the implementation of a project.[102] This depends on the familiarity of this person with the tasks and activities. While not explicitly acknowledged by Perrow – to my knowledge – it makes sense that the task variability will be higher when there is a wider scope of tasks,[103] and when these tasks are interdependent.[104] Second, Perrow identifies the "nature of the search procedure." This so-called *task analysability* refers to the extent that search activity is necessary to resolve the aforementioned new or unexpected situations. On the one hand, there can be "known ways of solving it, and little reflection or judgement is required after one has some experience with it."[105] This refers to a high task analysability. On the other hand, a low task analysability refers to the situation where some search is necessary to resolve the unexpected situations. The person "must rely

[99] Charles Perrow's work is broadly appreciated by other authors as well. See, for instance, Raymond G. Hunt, "Technology and Organisation," *The Academy of Management Journal* 13, no. 3 (1970), 245 ; Richard Burton and Borge Obel, *Strategic Organisational Diagnosis and Design: The Dynamics of Fit* (New York: Springer Science, 2004), 249.
[100] This is claimed by Jones (*Organisational Theory, Design and Change,* 275), but also confirmed by myself. Joan Woodward ("Technology and organisation 1965", in ed. Michael Handel, *The Sociology of Organisations: Classic, Contemporary and Critical Readings* (USA: Sage Publications, 2003), does indeed hardly focus upon what explains complexity.
[101] Perrow, *Organisational Analysis: A Sociological View,* 77
[102] Jones, *Organisational Theory, Design and Change,*275.
[103] See, e.g., Robert Dewar and Jerald Hage, "Size, Technology, Complexity, and Structural Differentiation: Toward a Theoretical Synthesis," *Administrative Science Quarterly* 23, no. 1 (1978), 115.
[104] Jones, *Organisational Theory, Design and Change*, 279.
[105] Perrow, *Organisational Analysis*, 76.

upon a residue of something we do not understand at all well – experience, judgment, knack, wisdom, intuition."[106] This leads to the following matrix.

Figure 2.7. Charles Perrow's technology variable[107]

	Low task variability	*High task variability*
Low task Analysability	Craft	Nonroutine
High task Analysability	Routine	Engineering

Considering this matrix, I argue that the adopted nuclear terrorism scenario is characterised by nonroutine technology. Given the diverse technical tasks and the organisation's clandestine operational environment, this scenario expect the implementation of the nuclear terrorism plot to be entangled by many exceptional problems which are hard to systematically analyse in advance. Although this study elaborates on different nuclear terrorism scenarios in a later chapter, the following sections recapitulate the adopted nuclear terrorism scenario in order to illustrate why it can be considered to be a nonroutine plot.[108]

The first hurdle in the nuclear terrorism scenario is the acquisition of fissile material. The appropriate type and quantity of fissile material is a necessary precondition to construct a crude nuclear device. In this scenario, I assume that a terrorist organisation will externally procure the fissile material via means of theft, attack or purchase. A few of the most likely tasks in doing so are the identification and reconnaissance of the target, brokering reliable contacts to carry out the mission, ensuring the flow of material and financial support, circumventing security measures at the target, and establishing a viable way out. Various skills are expected to be necessary (e.g. operational military skills, networking skills,

[106] Perrow, *Organisational Analysis*, 76.
[107] Ibid., 78.
[108] Note that some dimensions of this scenario might deviate from what would actually happen in a nuclear terrorism plot. This will always be the case in any hypothetical scenario. Yet, this does not undermine the argument that, considering the plot as a whole, the implementation of a nuclear terrorism plot will often be a nonroutine project.

coordinating skills, or financial skills). Although I expect insider assistance to this unit, I assume that no systematically organised state assistance will help them in deliberately transferring the fissile material to the terrorist organisation. An individual cell – which can be expected to consist of at least five to ten people – might be able to obtain the fissile material. While terrorist organisations have proven to be capable of, e.g., stealing or attacking high-level targets, such a scenario is not *business as usual* for a terrorist organisation. Considering the different tasks and the clandestine operational environment in which they need to be completed, I expect a relatively high probability of nonroutine problems arising throughout the implementation of this hurdle (e.g. such as the presence of an off-duty guard during the implementation of the attack at Pelindaba).

This links to my assumption that a terrorist organisation will not attain the most appropriate type and quantity of fissile material. The quantity, element, shape, composition, and radiation of the fissile material has a strong impact on the design and assembly of the nuclear device. Although the nuclear security regime suffers from severe shortcomings, the adopted nuclear terrorism scenario assumes that a terrorist organisation would need to process and adapt the fissile material to some extent – and/or amend the design of the nuclear device - before it can actually construct the improvised nuclear device. A terrorist organisation would thus need to develop a functioning design, acquire the non-nuclear components, and fabricate the nuclear device (e.g. the casting of fissile material in the right shape, the actual manufacturing of the gun-type or implosion-type arrangement, or the potential testing of non-nuclear components). It is true that the development of a nuclear explosion of 100 tons is technically less challenging than the development of crude nuclear device with a 15kT yield. Yet, the second hurdle of this scenario is still assumed to imply various technically challenging and interdependent tasks that need to be completed in a clandestine operational environment. The skillset of this cell is entirely different from the skills needed during the first hurdle in this scenario (e.g. nuclear physicists, metallurgists, explosives and ballistic experts, chemists, engineers, electricians, and people with clandestine procurement skills). This scenario assumes that a relatively small group – ranging at least between five and twenty people – is necessary to assemble the bomb. This number can easily increase. Considering the challenging technical tasks and the group's clandestine operational environment, the adopted scenario expects that various unexpected situations will arise throughout the implementation of this second hurdle (e.g. such as the problems with the assembly of the bomb during the implementation of the "Bojinka" plot).

Next, this nuclear terrorism scenario assumes that a terrorist organisation will need to illicitly smuggle fissile material, non-nuclear components, or an intact crude nuclear device at some point during the project. This enables the organisation to maximise security during the assembly of this unique device. I

therefore expect that a terrorist organisation would require a small unit with people experienced with trafficking techniques, tactics and procedures. In case they would outsource some parts of this task, the terrorist organisation would still require people with networking skills, coordinating skills, or financial skills. Note in this context that there might be some overlap with people from the unit responsible for the first hurdle. I again expect a small group of at least five people. This group might be amounted by a number of middlemen, brokers and/or other intermediaries. Although these tasks are not considered to be very perilous, there is an inherent risk that the organisation would face nonroutine problems throughout the implementation of this step. For instance, any unnoticed security measure or unreliable intermediary might lead to operational errors or delays. This could lead to the interruption or detection of (parts of) the nuclear terrorism plot.

Finally, once the crude nuclear device arrived in the target country, the adopted nuclear terrorism scenario assumes an airburst or surface-burst delivery of the device. The small deployment team would need to check the functionality of the device, might need to ensure communication with senior leadership (depending on the command and control posture), secure the operation, and actually detonate the crude nuclear device. These tasks and activities are not considered to be insurmountable for a terrorist organisation. Yet, the implementation of this last hurdle can be confronted by nonroutine problems such as last minute doubts or interruption by law enforcement efforts (e.g. such as the detection of the Millennium Bomber during his entrance in the U.S.).

Thus, in conclusion with respect to the adopted nuclear terrorism scenario, this scenario sets a baseline with respect to the tasks and activities that a terrorist organisation would need to complete in order to effectively construct and detonate a crude nuclear device. Some of these tasks might be familiar to the terrorist organisation (e.g. moving people and money). Yet, considering the combination of the various technical challenges and the organisation's clandestine nature, this scenario expects that that every individual hurdle entails a relatively high probability that nonroutine problems will occur. In addition, these different hurdles – and its corresponding tasks and activities - need to be financed and coordinated. The diversity of people and skills need to be integrated into one well-functioning team. Consequently, reflecting upon the project as a whole, the adopted nuclear terrorism scenario can be considered to be characterised by nonroutine technology. I expect the implementation of such a nuclear terrorism plot to be entangled by unexpected problems that are hard to systematically analyse in advance. Although the degree that this actually occurs will depend on the sophistication and efficiency of the improvised nuclear device, the adopted nuclear terrorism scenario expects a relatively high incidence of, e.g., unnoticed security measures, (moral) doubts by the perpetrators, technical hick-ups, personal disagreements, detection of (parts of) the plot by counterterrorism forces, or any other

contingent factor. As Carl von Clausewitz would phrase it, the *fog of nuclear terrorism* is expected to be present.[109]

Organisational dynamics and variables will therefore have an important impact on the likelihood that a terrorist organisation can effectively implement a project that is characterised by such complexity: who should make which decisions in a nuclear terrorism project? How can unforeseen obstacles dealt with? How should security considerations be taken into account throughout the nuclear project? etc... Reflecting upon these questions directly touches upon the organisational dimension to the implementation of such a plot. Yet, these type of questions are hardly ever systematically considered in traditional nuclear terrorism threat assessments.

2.2. The organisational approach: underdeveloped in nuclear terrorism threat assessments

The second section of this chapter will further substantiate the argument that an organisational approach is necessary in today's nuclear terrorism threat assessments. Specifically, while the previous section made clear that this approach is a relevant one, this section will argue in more depth that this focus is not yet sufficiently covered by today's nuclear terrorism literature. Moreover, this section will argue that particular attention should be given to the role of the organisational design.

In order to do so, this section will first briefly elaborate on the organisational approach in the field of terrorism studies. This is not an uncommon approach in terrorism studies. Next, this section will elaborate on the literature on nuclear terrorism and more systematically cross-reference this literature with the broader literature on innovation and technology acquisition by a terrorist organisation. This will demonstrate that some parameters identified in the literature on innovation and technology acquisition by a terrorist organisation are inadequately studied by traditional research on the nuclear terrorism threat. These parameters can be categorised as part of the organisational design. Given that nuclear terrorism would be a case of innovation and technology acquisition by a terrorist organisation,

[109] The complexity of a nuclear terrorism plot is also (implicitly) acknowledged by Thomas Schelling, 'Whatever Happened to Nuclear Terrorism?' Available at: https://d3qi0qp55mx5f5.cloudfront.net/cpost/i/docs/Schelling-Nuclear-Terrorism.pdf?mtime=1397148761 (accessed April 2, 2019); Henry Sokolski, "The Nuclear Terrorism Threat: How Real Is It? Two Views by Brian Michael Jenkins and John Lauder," Working Paper 1602 (Nonproliferation Policy Education Center, 2016); Levi, *On Nuclear Terrorism,* 8. In this context, Michael Levi, for instance, also explicitly highlights that the defence against such a plot should be a system. A small change of plans in one step of the project by the terrorist organisation – because of a small barrier – might imply substantial problems for the terrorist organisation in the next step. This demonstrates the complexity of such a plot.

focus on the organisational design can thus be assumed to fill a critical gap in the literature on nuclear terrorism.

2.2.1. The organisational approach in terrorism studies

No consensus exists on what terrorism means. While the origins of this phenomenon can be traced back in time for centuries, there are hundreds of definitions but no "precise, concrete and truly explanatory definition."[110] There are two intertwined problems in this respect. First, it is a contested concept. Considering the pejorative nature of the term, political, legal, social and popular notions on this phenomenon strongly diverge. Labelling someone as a "terrorist" is inherently subjective. It implies a moral judgement.[111] Norms and politics come into play. Second, "terrorism" is a complex concept. It "includes a wide array of tactics and is undertaken by a broad range of actors in pursuit of a great diversity of goals."[112] It does not delineate any precise modus operandi (e.g. random bombings or shootings), particular kinds of actors (e.g. non-state, religious, revolutionary or ethno-nationalist groups) or one specific goal (e.g. territorial autonomy, animal rights, or regime-change). It follows that there neither is one theory of terrorism.[113] Different studies of terrorism focus on different levels (e.g. the individual level, the organisational level, or the societal level) and come from a variety of backgrounds (e.g. international relations, political science, psychology, law, or communication studies).[114] This work subsequently does not claim that it can integrate this diversity of perspectives on terrorism. Yet, as suggested by Richard English, "the key thing is to be precise." Any work on terrorism needs to clarify how it approaches the phenomenon and what it means by the term.[115]

I therefore want to explicitly clarify that this study adopts an organisational approach. While this approach remains underdeveloped in nuclear terrorism threat assessments - as will be substantiated in the following sections - it is not an uncommon approach in terrorism studies. A variety of work in this field has often placed terrorism in a broader theoretical framework.[116] Rather than treating it as a

---

[110] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006), 1.
[111] See, e.g., Alex Schmid, "Frameworks for Conceptualizing Terrorism," *Terrorism and Political Violence* 16, no. 2 (2004),197-221; Hoffman, *Inside Terrorism;* Charles Tilly, "Terror, Terrorism, Terrorists," *Sociological Theory* 22, no.1 (2004).
[112] Bradley McAllister and Alex P. Schmid, "Theories of Terrorism", in Alex Schmid (ed.), *The Routledge Handbook of Terrorism Research* (New York & London: Routledge, 2011), 202.
[113] Tilly, "Terror, Terrorism, Terrorists," 9.
[114] McAllister and Schmid, "Theories of Terrorism," 202.
[115] Richard English, "The Future Study of Terrorism," *European Journal of International Security*, 1, no. 2 (2016): 136.
[116] Martha Crenshaw, "Terrorism Research: The Record," *International Interactions: Empirical and Theoretical Research in International Relations* 40, no. 4 (2014): 557.

phenomenon sui generis, terrorism is situated in, e.g., a political violence framework or social movement framework. Adopting such a broader literature base allows scholars to develop and reflect upon particular propositions and hypotheses.[117] In line with this view, various authors have adopted (implicitly or explicitly) theories of organisational behavior to terrorism.[118] Indeed, any terrorist group can be considered to be an organisation.[119] An organisation – broadly defined – refers to a "social unit that serves specific purposes."[120] Like conventional organisations, terrorist groups need to plan and control the effective and efficient functioning of its organisation and the achievement of the organisation's goals. Building on such shared features, these authors aim to better understand a specific organisation by knowing about other organisations.[121] Some examples will illustrate that this approach is no exception in today's terrorism studies.

Michael Kenney, to give a first seminal example, builds on theories of competitive adaptation and organisational learning to analyse the effectiveness of Islamic terrorist networks. He argues, for instance, that intuitive knowledge (which he calls metis) is often more important than technical knowledge (which he calls techne) in strengthening the effectiveness of clandestine organisations.[122] Next, Jacob's Shapiro seminal book "the terrorist's dilemma" builds primarily on principal-agent theory to demonstrate management constraints to any terrorist organisation. He elaborates on the inherent challenges for any terrorist organisation to balance security with efficiency and control, and the factors that impact this dilemma (e.g. the group's political goals, and the impact of counterterrorism efforts).[123] He would probably agree with Kenney that metis by individual terrorists is important to cope with this dilemma. Besides these influential books,[124] there are also numerous individual articles that approach

[117] Samuel T. Hunter et al., "Recruitment and selection in Violent Extremist Organisations: Exploring what Industrial and Organisational Psychology Might Contribute," *American Psychologist* 72, no. 3 (2017): 250.
[118] Crenshaw, "Terrorism Research: The Record," 562-564.
[119] This does not cover so-called lone wolves.
[120] Amitai Etzioni, "Organisational Control Structure," in *Handbook of Organisations* (Chicago: Rand McNally & Company, 1965), 650. As mentioned before, such a broad description is meant to clearly illustrate the relevance of an organisational approach. This description clearly covers terrorist organisations, thereby illustrating the relevance of this approach.
[121] Richard Scott and Gerald Davis, *Organisations and Organising,* 1. Note, obviously, that not every organisation is exactly the same. Conventional and terrorist organisations can vary in size and shape, objectives and strategies, structural and cultural characteristics, operational environment, complexity of tasks, technologies and required skills, etc. Yet, this does not imply that we cannot learn from other organisations.
[122] Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (Pennsylvania: The Pennsylvania University Press, 2007).
[123] Jacob Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organisation* (Princeton: Princeton University Press, 2013).
[124] There are obviously also other books and reports that (implicitly) integrate an organisational approach, such as the work by Eli Berman on the defection constraint in religiously motivated terrorist groups (Eli Berman, *Radical, Religious and Violent: The New Economics of Terrorism* (Cambridge: MIT Press, 2009), the work by Jackson et al. on organisational learning by terrorist organisation. (Brian Jackson et al., "Aptitude for Destruction Volume 2 Case Studies of Organisational Learning in Five Terrorist Groups" (California: RAND corporation, 2005), Marc Sageman's

terrorism from an organisational perspective. While it is not possible to describe each individual article, it is illustrative to mention the work by Asal and Rethemeyer with respect to various organisational characteristics (e.g. size, ideology, alliances) and their impact on the lethality of terrorist organisations,[125] the work by Enders and Jindapon about network externalities and the optimal structure of terrorist networks,[126] or the groundbreaking work by Martha Crenshaw on instrumental and organisational theories of terrorism.[127] It comes as no surprise that the adoption of an organisational approach – and the organisation as the unit of analysis – already yielded several interesting insights in the field of terrorism studies.

I believe – as I will demonstrate - that this will also hold true for the adoption of an organisational approach in studying the nuclear terrorism threat. This study therefore starts from a definition of terrorism in line with this organisational approach, namely terrorism as "the deliberate creation of a sense of fear, usually by the use or threat of use of symbolic acts of physical violence, to influence the political behaviour of a given target group."[128] A terrorist organisation is subsequently defined as "a collection of individuals belonging to a non-state entity that uses terrorism to achieve its objectives. Such an entity has at least some command and control apparatus that, no matter how loose or flexible, provides an overall organisational framework and general strategic direction."[129] These definitions are in line with an organisation as a "social unit that serves specific purposes."[130]

Although I believe that this approach will be of particular value in nuclear terrorism threat assessments, I need to be transparent about the fact that this is only one particular lens via which to reflect on (nuclear) terrorism. Specifically, this approach – and the corresponding definitions - often start from an organisation as an strategic actor. This does not imply that the organisation is always perceived as a

work on better understanding the functioning of terrorist networks (Marc Sageman, *Understanding Terror Networks* (USA: University of Pennsylvania Press, 2004); or Kim Cragin and Sarah Daly's work on how terrorist groups change and adapt over time (Kim Cragin and Sara Daly, "The Dynamic Terrorist Threat: An Assessment of Group Motivation and Capabilities in a Changing World" (California: RAND Corporation, 2004). This list is not exhaustive.

[125] Victor Asal and Karl Rethemeyer, "The Nature of the Beast: Terrorist: The Organisational and Network Characteristics of Organisational Lethality," *Journal of Politics* 70, no. 2 (2008): 437–449.

[126] Walter Enders and Paan Jindapon, "Network Externalities and the Structure of Terror Networks," *Journal of Conflict Resolution* 54, no. 2 (2010): 262–80.

[127] Martha Crenshaw, Theories of terrorism: Instrumental and organisational approaches, *Journal of Strategic Studies* (1987), 13-31; Martha Crenshaw, *Explaining Terrorism: Causes, Processes and Consequences* (London: Routledge, 2011).

[128] Peter R. Neumann & M.L.R. Smith, *The strategy of terrorism. How it works, and why it fails*, (London & New York, Routledge, 2008), 8.

[129] Seth Jones and Martin Libicki, "How Terrorist Groups End: Lessons for Countering Al Qa'ida'" (California: RAND Corporation, 2008), 3-4.

[130] Etzioni, "Organisational Control Structure." 650

group that rationally pursues the most valuable expected utility function. Yet, it does imply that terrorist organisations are often considered to be strategic actors that assess options, consider their interests, and aim to make decisions that match their actions with their goals.[131] This approach entails a bias towards focusing attention on group dynamics and the instrumentality of terrorism (at the level of the collectivity).[132] Attention for, e.g., psychological and individual approaches towards terrorism is minimised. It might, for instance, downplay the role of an individual to the probability of nuclear terrorism (e.g. such as an individual as the driving power behind such a plot). Nevertheless, given that the requirements and impact of such an attack are likely to push the organisation to strategically reflect upon such an attack,[133] and the fact that no individual could complete such a nonroutine project on its own, the collective level is assumed to have a lot of explanatory power. Oddly, however, such an organisational approach remains a critical gap in the literature on nuclear terrorism threat assessments. The following section will substantiate this claim in more depth and illustrate that particular attention should be given to the role of the organisational design

2.2.2. The role of the organisational design

Traditional nuclear terrorism threat assessments focus primarily on (1) a terrorist organisation's motivation to use an improvised nuclear device, (2) the availability of nuclear know-how and technology, and/or (3) these clandestine organisations' opportunities to obtain fissile material. Illustrative is the 2016 report by the U.S. Bureau of Counterterrorism that stated that: "utilization of CBRN materials and expertise remained a terrorist threat, as demonstrated by [1] terrorists' stated intent to acquire, develop, and use these materials; the nature of injury and damage these weapons can inflict; [2] the ease with which information on these topics now flows; and [3] the dual-use nature of many relevant technologies and material."[134] Little systematic attention is however given to the organisational

[131] McIntosh and Storey, "Between Acquisition and Use," 2. Treating terrorist organisations as a strategic actors is relatively common in terrorism studies. Tilly (Charles Tilly, "Terror as Strategy and Relational Process," *International Journal of Comparative Sociology* 46, no. 1–2 (2005), 21) claims for instance that such an approach is essential to explain terrorism. Other examples are: Colin Wight, *Rethinking Terrorism: Terrorism, Violence and the State, Rethinking World Politics* (UK: Palgrave Macmillan, 2015); Martha Crenshaw, "The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice," in Origins of Terrorism: Psychologies, Ideologies, Theologies, State of Mind (John Hopkins University Press, 1998).

[132] Marta Crenshaw, *Explaining Terrorism: Causes, Processes and Consequences* (London & New York: Routledge, 2011), 67-135.

[133] McIntosh and Storey, "Between Acquisition and Use," 2.

[134] U.S. Department of State Countries Report on Terrorism 2016, available at: https://www.state.gov/j/ct/rls/crt/2016/272236.htm. Note that I have added the brackets myself to clearly refer to the different traditional nuclear terrorism variables.

challenges to implementing a potential nuclear terrorism plot. This holds true for both (public) governmental assessments and the academic literature.

First, experts often concentrate on the instrumental, ideological and psychological mechanisms that influence whether a terrorist organisation would decide to construct and detonate an improvised nuclear device. Seminal books on nuclear terrorism – such as that by Graham Allison[135] or Charles Ferguson and William Potter[136] – have devoted large chunks of text about the motivation of a terrorist organisation to pursue a nuclear capacity. Other renowned experts have written articles and books dedicated (entirely or partly) to this particular issue.[137] While the increasing lethality of terrorist organisations is often referred to as an indicator for a growing interest in nuclear terrorism, most experts simultaneously acknowledge that terrorist organisations differ in their, e.g., operational skills and opportunities, strategic and organisational goals, and attitudes towards risks and innovation. It follows that various authors discuss, e.g., the operational objectives of terrorist organisations (e.g. inflict mass casualties, inspire followers, cause economic havoc and psychological trauma, or gain prestige), its ideological and strategic goals - and the extent to which these can be accomplished by an act of nuclear terror – or the opportunities for terrorist organisations to successfully complete such a plot. In general, these authors often conclude that religiously inspired or apocalyptic terrorist organisations are the actors most likely to aim to acquire – and potentially – use these weapon of mass destruction (e.g. Al Qaeda, the Islamic State, or Aum Shinrikyo). Other potential candidates – such as, for instance, single issue terrorism – are however not necessarily excluded.[138]

---

[135] Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*.

[136] Ferguson and Potter, *The Four Faces of Nuclear Terrorism*.

[137] See, e.g., Gary Ackerman, "Motivations for Engaging in Nuclear Terrorism," Expert Series Fund for Peace, 2006; Bruce Hoffman, "Terrorism and WMD: Some Preliminary Hypotheses," *The Nonproliferation Review* 4, no. 3 (1997): 45–53; Brian Michael Jenkins, *Will Terrorists Go Nuclear?* (New York: Prometheus Books, 2008); Jerrold M. Post, *Prospects for Nuclear Terrorism: Psychological Motivations and Constraints*, in Leventhal and Alexander, "Preventing Nuclear Terrorism: The Report and Papers on the International Task Force on Prevention of Nuclear Terrorism" (Massachusetts; Lexington Books, 1987); Rolf Mowatt-Larssen, "The Armageddon Test: Preventing Nuclear Terrorism," *The Bulletin of the Atomic Scientists* 65, no. 5 (2009): 60-70.

[138] This section cannot capture every detail. Yet, it is based on a variety of scholarly publications that touch upon this issue. Besides the aforementioned references, it is based on, e.g., Gary Ackerman and Jeremy Tamsett, *Jihadists and Weapons of Mass Destruction* (London & New York: CRC Press, 2009); D. Gressang Iv, "Audience and Message: Assessing Terrorist WMD Potential," *Terrorism and Political Violence* 13, no. 3 (2001): 83–106; T.J. Badey, "Nuclear Terrorism: Actor-Based Threat Assessment," *Intelligence and National Security* 16, no. 2 (2001): 39–54; Sammy Salama and Lydia Hansell, "Does Intent Equal Capability? Al-Qaeda and Weapons of Mass Destruction," *The Nonproliferation Review* 12, no. 3 (2005): 615–53. Graham Allison, "Nuclear Terrorism: Threat Briefing (2010)." Available at: https://www.belfercenter.org/sites/default/files/files/publication/threat-assessment.pdf. (accessed April 4, 2019).

Second, experts also often focus on the availability of nuclear know-how and technology.[139] Going beyond the demand side, publications on this issue primarily direct attention to the supply side of the nuclear terrorism threat. Is the know-how and technology with respect to the design and construction of an improvised nuclear device easily available to a terrorist organisation? On the one hand, various authors argue that accumulating technological progress and globalisation lead to an increase in the availability of nuclear weapons know-how and technology. Reference is, for instance, made to the N-th country experiment – where three young physicists succeeded in the mid-1960s to develop a credible nuclear weapon design with access only to the unclassified technology literature[140] – or the successful recruitment of scientists and engineers by a terrorist organisation (e.g. Al Qaeda's connections with scientists of the Umma Tameer e Nau (UTN); a Pakistani NGO with extremist thoughts).[141] On the other hand, however, sceptics to this claim traditionally point to problems for terrorist organisations to exploit these opportunities. They refer to, e.g., the need for both tangible and intangible skills, nuclear weapon design complexities, and wrong or incomplete information.[142] They quote, for instance, Stephen M. Younger – the former head of nuclear weapons research and development at Los Alamos – who stated in 2008 that "it would be wrong to assume that nuclear weapons are now easy to make, that once the secret was out anyone could read the instruction book and make one with materials found around the house. I am constantly amazed when self-declared "nuclear weapons experts," many of whom have never seen a real nuclear weapon, hold forth on how easy it is to make a functioning nuclear explosive."[143]

Finally, closely related to the previous variable, nuclear terrorism threat assessments often focus on the strengths and vulnerabilities of the nuclear security regime and the different types of fissile material that a terrorist organisation might acquire. Considering this is an essential step in any potential nuclear terrorism plot, a lot of scholarly and governmental attention is dedicated to this topic. This is illustrated by, e.g., the nuclear security summits between 2010 and 2016, or various of the seminal books and

[139] See, e.g. Mowatt-Larssen et al., "The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism,"12. Mark et al., "Can Terrorists Build Nuclear Weapons?"; Ferguson and Potter, *The Four Faces of Nuclear Terrorism*.
[140] See, e.g. Ferguson and Potter, *The Four Faces of Nuclear Terrorism,* 137; Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe,* 93-94.
[141] See, e.g., Matthew Bunn et al., "Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline" (Harvard Belfer Center, March 2016), 16 ; Rolf Mowatt-Larssen, "Al Qaeda Weapons of Mass Destruction Threat: Hype of Reality" (Harvard Belfer Center, January 2010). David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010), 169-184.
[142] See, e.g. Christoph Wirz and Emmanuel Egger, "Use of Nuclear and Radiological Weapons by Terrorists?," *International Review of the Red Cross* 87, no. 859 (2005), Mueller, *Atomic Obsession*; *S*ammy Salama and Edith Bursac*,* "Jihadist Capabilities and the Diffusion of Knowledge" in Gary Ackerman and Jeremy Tamsett (eds.), *Jihadists and Weapons of Mass Destruction* (London & New York: CRC Press, 2009).
[143] Stephen Younger, *Endangered Species: How We Can Avoid Mass Destruction and Build a Lasting Peace* (United States: Harper Perennial, 2008), 86.

reports on nuclear terrorism – such as work by the Managing the Atom project, the Arms Control Association, or the Nuclear Threat Initiative – that dedicate substantial attention to this issue. Discussions on this theme primarily focus on the strengths and vulnerabilities of the regulatory framework on nuclear security, the corresponding nuclear security culture, and individual nuclear facilities.[144] On the one hand, they often point to opportunities for terrorist organisations to obtain fissile material. Reference is, for instance, made to the nuclear security vulnerabilities of particular countries - such as Russia, Iran, North-Korea or Pakistan – or substantial security incidents (e.g. the Y-12 security incident - where a 82-year old nun succeeded to penetrate deep into a nuclear security administration facility). Yet, on the other hand, it is simultaneously also acknowledged that progress has been made with respect to securing weapons-usable material from terrorist organisations. Weapons-usable material has been eliminated in various countries, and "security rules and procedures have been tightened in essentially every country where these materials continue to exist."[145]

Secrecy and uncertainty often lead to "conflicting intuitions" in these intertwined debates.[146] Yet, going beyond these debates, it is remarkable that few experts systematically explore the complexity for a terrorist organisation to implement a nuclear terrorism plot. Experts refer to, e.g., "sophisticated organisational structures,"[147] a "technically sophisticated" terrorist group,[148] or a "well-organised international network of agents."[149] Yet, they often withhold from systematically reflecting upon the meaning of these concepts. The implementation process by a terrorist organisation is often implicitly assumed and, by consequence, often understudied. This study, however, starts from the assumption that nuclear technical achievement by a terrorist organisation is as much about organisation as it is

[144] Some notable work covering this dimension of nuclear terrorism threat assessments is: Igor Khripunov, Nikolay Ischenko, and James P. Holmes, *Nuclear Security Culture: From National Best Practices to International Standards* (The Netherlands: IOS Press, 2007); Michelle Cann, "Nuclear Security Commitment Making: Results of the Summit Process," in *Nuclear Terrorism: Countering the Threat*, Global Security Studies (London & New York: Routledge, 2016), 215–32."NTI Nuclear Materials Security Index," Nuclear Threat Initiative, 2016, Available at: http://ntiindex.org/data-results/theft-data/. (Accessed April 4, 2019). Bunn et al., "Preventing Nuclear Terrorism."

[145] Bunn et al., "Preventing Nuclear Terrorism," iii.

[146] Brecht Volders and Tom Sauer, "Introduction to the Book," in *Nuclear Terrorism: Countering the Threat*, Global Security Studies (London & New York: Routledge, 2016), 7.

[147] Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 42.

[148] Mowatt-Larssen et al., "The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism," 14.

[149] Ferguson and Potter, *The Four Faces of Nuclear Terrorism,* 35.

about engineering.[150] As illustrated in the first part of this chapter, constructing and detonating a nuclear device while operating in a clandestine environment can often be expected to require a large scale of operations and corresponding information and coordination needs. It is a nonroutine plot. It is therefore necessary to focus more systematically on the organisational challenges to the implementation of such a nuclear terrorism plot.

Admittedly, in contrast to considering the different variables as isolated issues or individual parts, some authors do approach a nuclear terrorism plot in a more comprehensive manner. By considering the plot as a whole, they aim to provide a more encompassing analysis of the probability of nuclear terrorism. John Mueller and Michael Levi are probably the most prominent examples. They both elaborate on the different steps and pathways that can be taken in a nuclear terrorism plot, the challenges to these steps, and the interaction between the different tasks and activities.[151] Both authors often implicitly touch upon various of the organisational issues that are identified in this study. Yet, they do not explicitly and systematically reflect upon the organisational challenges for a terrorist organisation pursuing such a capacity nor embed this in a broader theoretical framework. Likewise, while various publications by the Unconventional Weapons and Technology Unit of START often report about organisational issues to the use of WMD's by a terrorist organisation, and thus also touch upon various issues identified in this study, I believe a more systematic and in-depth exploration of the organisational challenges to the actual implementation of such a nuclear terrorism plot is still warranted.[152] Finally, a similar logic to this approach has been adopted more systematically with respect to nuclear proliferation by states (e.g. Jacques Hymans' book "Achieving nuclear ambitions: scientists, politicians and proliferation") or

[150] This approach has not been systematically adopted to nuclear terrorism. Yet, a similar claim has been made about state nuclear proliferation (e.g. Jacques Hymans, *Achieving nuclear ambitions: scientists, politicians, and proliferation* (United States: Cambridge University Press, 2012)). Moreover, other authors (Kathleen Vogel, *Phantom Menace or Looming Danger? A New Framework for Assessing Bioweapons Threats* (Baltimore: The John Hopkins University Press, 2013); Sonia Ben Ouagrham-Gormley, *Barriers to Bioweapons: The Challenge of Expertise and Organisation for Weapons Development* (London: Cornell University Press, 2014)) adopt a similar socio-technical perspective to a different WMD terrorism threat: bio-terrorism. Finally, one can note a growing appreciation for this approach in the broad terrorism studies literature (e.g. Ackerman et al. "Designing Danger: Complex Engineering by Violent Non-State Actors," *Special Issue: Journal of Strategic Security* 9, no.1 (2016)).

[151] Note that Mueller can probably be considered to be even more sceptical towards the likelihood of nuclear terrorism compared to Michael Levi.

[152] For an overview of various open publications by the Unconventional Weapons and Technology Unit of START, please see: http://www.start.umd.edu/unconventional-weapons-and-technology. (accessed April 4, 2019). For instance, to be more precise, one of the key publications (Asal, Ackerman & Rethemeyer, "Connections can be Toxic") – which is often quoted in the nuclear terrorism literature - focuses on various organisational issues related to the decision to CBRN. While this excellent article contains various relevant issues (such as the relevance of the organisational size, which I will also touch upon), they primarily focus on the decision stage (and not the implementation of such a plot). Moreover, its quantitative nature obscures salient details on some particular cases (as they indicate themselves). This is, however, needed to explore this topic in-depth. To my knowledge, there is no publication that tries to systematically and in-depth explore the actual organisational challenges to implementing a nuclear terrorism project as a whole.

biological and chemical weapons proliferation by terrorist organisations (e.g. Kathleen Vogel studied the social context shaping the development of bioweapons;[153] Sonia Ben Ouagrham-Gormley focused on the relevance of expertise and organisation for weapon development;[154] Jean Pascal Zanders focused on the internal dynamics of a terrorist group acquiring biological and chemical weapons[155]). Yet, even though I have drawn upon the analytical work of these authors to some extent, this approach is to my knowledge still not yet sufficiently explored with respect to the nuclear terrorism threat.

The fact that there is scant literature that systematically focuses on the organisational challenges to the implementation of a nuclear terrorism plot is a strange observation. This becomes particularly true when cross-referencing the nuclear terrorism literature with the broader literature on the topic of innovation and technology acquisition by a terrorist organisation. This latter strand of literature acknowledges the importance of this organisational dimension. Given that nuclear terrorism would be a case of innovation and technology acquisition by a terrorist organisation, focus on this organisational dimension can be assumed to fill a critical gap. Moreover, importantly, cross-referencing both strands of literature highlights that it might be of particular relevance to explore the role of the organisational design in future nuclear terrorism threat assessments.

Cross referencing two strands of literature

Martha Crenshaw differentiates between terrorist innovation at the strategic level, the organisational level, and the tactical level. Strategic innovation refers to "both a new goal and a new way of relating operations to that goal." Organisational innovation refers to "changes in group structure and institutions," and tactical innovation refers to "changes in method or operations." The latter most often consists of newly used weapons or targets.[156] Various authors writing about terrorist innovation often focus on this latter type of innovative technology acquisition by means of the introduction of a

[153] Vogel, *Phantom Menace or Looming Danger?*
She factors in the social context of scientific work, such as tacit knowledge, laboratory disciplines, or the role of organisational management, Yet, while I agree that attention needs to be given to these issues, the focus of this particular doctoral study is more narrow. To be precise, I will touch upon various of the issues she identifies, but will start from a particular focus on the role of the organisational design (as will be outlined in the following section)
[154] Ouagrham-Gormley, *Barriers to Bioweapons.*
[155] Jean Pascal Zanders, "Internal Dynamics of a Terrorist Entity Acquiring Biological and Chemical Weapons: Insights for the Study of Possible Nuclear Weapon Acquisition," in *Nuclear Terrorism: Countering the Threat*, Global Security Studies (London & New York: Routledge, 2016), 26–54; Jean Pascal Zanders et al., "Risk Assessment of Terrorism with Chemical and Biological Weapons," in SIPRI yearbook (ed.), *Armaments, Disarmament and Security* (Sweden: SIPRI, 2000).
[156] Martha Crenshaw, in Maria Rasmussen and Mohammed Hafez, "Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators," Defense Threat Reduction Agency Workshop report (Defense Threat Reduction Agency, 2010). 36-41.

new tactic or technology.[157] The construction and detonation of a crude nuclear device by a terrorist organisation can also be situated at this level.[158] While this type of technology acquisition is often conceived to be as simple as purchasing the required material and technology and/or get ready access to the necessary information (e.g. the design of a nuclear device),[159] the broad field of technology studies has established "that the process of technology acquisition by any organisation is often a very complex process which is both promoted and inhibited by many different pressures and variables."[160] The development and acquisition of technology is "a product of heterogeneous contingency."[161] This is also true for terrorist innovation. The situational, organisational and individual level interact with each other.[162] Innovation and technology acquisition by a terrorist organisation is neither a simple nor a linear process.

There is some work that specifically focus on this topic of innovation and technology acquisition by a terrorist organisation. Some of the most notable pioneers in this field are Adam Dolnik, Maria Rasmussen & Mohammed Hafez, and Brian Jackson. More recent work is provided by, e.g., Magnus Ranstorp & Magnus Normark, Gary Ackerman, or Paul Gill et al.[163] In order to elaborate on the different factors related to the decision and implementation of innovation and technology acquisition by a terrorist organisation, I will specifically build on the work by Adam Dolnik.[164] I believe his work can be

---

[157] See, e.g. Adam Dolnik, *Understanding Terrorist Innovation: Technology, Tactics, and Global Trends*, Contemporary Terrorism Series (London & New York: Routledge, 2007), 6. Note that Dolnik in this context also points to the fact that terrorist innovation might actually fall in the realm of emulation and adaptation, as technologies used by terrorist organisations are almost never completely new (e.g. nuclear technology exists already). Yet, he is right in avoiding this distinction, as this is not often done in the literature on this field (and would probably needlessly complicate manners in this section). Moreover, he also points to the distinction between incremental and radical innovation. Given that no type of nuclear bomb has been exploded yet by a terrorist organisation, we always mean radical innovation in this study.

[158] Note in this context, however, that such an attack might also imply/cause a shift on the strategic and organisational innovation level. These three levels are closely intertwined.

[159] Brian Michael Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict & Terrorism* 24, no. 3 (2001): 185-186.

[160] Ibid., 185.

[161] Wiebe Bijker and John Law, *Shaping Technology: Building Society* (Cambridge & London: MIT Press, 1992), 17

[162] See, e.g., Nicole Tishler, "Trends in Terrorists' Weapons Adoption and the Study Thereof," *International Studies Review* 20 (2018): 368-394; Paul Gill et al., "Malevolent Creativity in Terrorist Organisations," *The Journal of Creative Behavior* 47, no. 2 (2013): 125–51.

[163] Dolnik, *Understanding Terrorist Innovation*; Magnus Ranstorp and Magnus Normark, *Understanding Terrorism Innovation and Learning: Al Qaeda and Beyond* (London & New York: Routledge, 2015); Maria Rasmussen and Mohammed Hafez, "Terrorist Innovations in Weapons of Mass Effect"; Jackson, "Technology Acquisition by Terrorist Groups," Adam Dolnik et al., *Aptitude for Destruction-Vol. 1: Organisational Learning in Terrorist Groups and Its Implications for Combating Terrorism* and *Vol. 2: Case Studies of Organisational Learning in Five Terrorist Groups* (Santa Monica: RAND, 2007); Gary Ackerman, "'More Bang for the Buck' Examining the Determinants of Terrorist Adoption of New Weapons Technologies," doctoral dissertation, King's College, 2014. Paul Gill et al., "Malevolent Creativity in Terrorist Organisations."

[164] Dolnik, *Understanding Terrorist Innovation.*

To my knowledge, this is one of the most comprehensive overviews on the determinants of terrorist innovation. Information provided by this book strongly overlaps with other work by Jackson, "Technology Acquisition by

considered to be one of the most comprehensive studies on this topic.[165] Dolnik systematically elaborates on 11 parameters that are often considered relevant to this issue. Moreover, he presents these different variables in a relatively isolated matter. While I believe that the work by, e.g., Ackerman or Gill et al. is better in illustrating the underlying relations between these factors, treating them as relatively isolated variables will provide us with a more clear overview. This fits the illustrative purpose of this section better. Indeed, the main function of this section is merely to demonstrate that the organisational design is a relevant variable to study in nuclear terrorism threat assessments.

Adam Dolnik identified 11 parameters to better understand the decision and implementation of a (tactical) innovation by a terrorist organisation. Each of these parameters can thus be expected to also be relevant with respect to the likelihood that a terrorist organisation will effectively start and implement a nuclear terrorism project. Nuclear terrorism threat assessments should thus also reflect upon these parameters.

1. *The role of ideology and strategy*: ideology is instrumental in mapping out the group's core objectives and the strategy to achieve these ambitions. The belief systems and strategic approach of a group can subsequently have a strong impact on the need/preference for a terrorist organisation to acquire particular military capabilities.

2. *Dynamics of the struggle*: this refers to two issues: (1) the availability of an area in which the terrorist organisation can freely operate. (2) The frequency and intensity of clashes between the government and the organisation. Both factors can have an impact on the decision and capability of a terrorist organisation to acquire new technology.

3. *Countermeasures*: counterterrorism forces can introduce particular security measures against specific tactics used by terrorist organisations. This might complicate matters for a terrorist organisation to adopt this particular tactic, and/or might push them to adopt a new modus operandi.

4. *Targeting logic:* terrorist organisations identify the scope of their targets and subsequently aim to acquire the capability to attack these targets at the desired scale. This is closely related to the

Terrorist Groups," Rasmussen and Hafez, "Terrorist Innovations in Weapons of Mass Effect," Ranstorp and Normark, *Understanding Terrorism Innovation and Learning*.

[165] This is also supported by Ackerman, "More Bang for the Buck," 7.

ideology and strategy of the organisation. The rigidity and extent of discrimination of the targeting logic might influence an organisation predisposition for innovation.

5. *Attachment to weaponry*: a terrorist organisation might give significant expressive or symbolic attachment to a particular weapon or the process of innovation itself. Going beyond mere strategic cost-benefit calculations, a particular modus operandi can be preferable to a terrorist organisation due to reasons of, e.g., identity or legitimacy.

6. *Relationship with other organisations*: a terrorist organisation's operational preferences and capabilities might be related to cooperation with other organisations or competition with other organisations. The potential sharing of know-how and technology, or the possible outbidding of other organisations, might influence a terrorist organisation's likelihood of innovation.

7. *Resources*: the quantity and quality of resources available to a terrorist organisation will influence its choice of modus operandi. This refers to both material resources (e.g. weapons, financial means) and human resources (e.g. people with operational expertise).

8. *Openness to new ideas*: this refers to three issues: (1) the group's decision-making dynamics. (2) The technological awareness of the group. (3) The group's attitude toward risk-taking. Each of these elements might influence the organisation's decision and implementation of innovative ideas.

9. *Durability*: this refers to the life span of a terrorist organisation. This might influence the opportunities the organisation comes across and the operational experience they might have. Each of these factors might influence their predisposition towards successful innovation.

10. *Nature of technology*: the probability that a terrorist organisation might (tactically) innovate and acquire a particular technology is – obviously – also function of the complexity and sophistication of the selected technology.

11. *Group dynamics*: this refers to three issues: (1) the background, value system and authority of the organisation's leader(s). (2) The group structure. (3) The overall levels of internal disputes. These factors can influence the development and implementation of an innovative modus operandi by a terrorist organisation.

I have deliberately not elaborated in depth on the (negative or positive) influence of these variables with respect to the nuclear terrorism threat. As previously mentioned, "conflicting intuitions" often clash in the debates on these intertwined parameters. Yet, rather than summarising or taking position into these debates, the particular aim of this section is to focus attention to one (group of) parameter(s) in this field of literature that is systematically understudied in the nuclear terrorism literature. These parameters can be grouped together under one variable: the organisational design. Table 2.1 illustrates this claim.

Table 2.1. Overlap between variables on "innovation and technology acquisition" and "nuclear terrorism"

	Motivation	Nuclear know-how and technology	Availability of fissile material	*Organisational design*
Ideology and strategy	X			
Dynamics of the struggle		X		*X*
Countermeasures		X	X	
Targeting logic	X			
Attachment to weaponry	X			
Relationship other organisations	X	X	X	
Resources		X	X	*X*
Openness to new ideas	X	X		*X*
Durability		X	X	
Nature of technology		X	X	
Group dynamics	X			*X*

Note: considering the overlap between these different parameters is open to some interpretation, it needs to be clear that this table is based to some extent on arbitrary judgement. For instance, there is a strong overlap between "countermeasures" and "nuclear know-how and technology" and "availability of fissile material." Yet, it is probably also true that countermeasures might be relevant to a terrorist organisation's motivation to pursue a nuclear capacity. The potential differences in interpretation do not, however, undermine the claim that some (aspects of the) parameters on innovation and technology acquisition by a terrorist organisation are not adequately studied by the literature on nuclear terrorism.

This table points out to which extent these parameters on innovation and technology acquisition by a terrorist organisation are adequately enveloped by the three traditional nuclear terrorism variables: (1) a terrorist organisation's motivation to use an improvised nuclear device, (2) the availability of nuclear know-how and technology, and/or (3) these clandestine organisations' opportunities to obtain fissile material. As becomes clear by this table, some (aspects of the) parameters with respect to innovation and technology acquisition by a terrorist organisation are inadequately covered by these three nuclear terrorism variables. This thus can be assumed to be a critical gap in the literature on nuclear terrorism. I have categorised these aspects under one variable: the "organisational design." The following sections will provide more textual explanation to this table 2.1.

Discussions on a terrorist organisation's motivation to go nuclear often embrace a variety of the identified parameters with respect to innovation and technology acquisition by a terrorist organisation. First and foremost, debates on a terrorist organisation's motivation to go nuclear often revolve around the role of the ideology and strategy of the terrorist organisation (cfr. ideology and strategy). This is considered instrumental to a terrorist organisation's objectives and (military) strategy. It is, subsequently, closely related to a terrorist organisation's attitude with respect to indiscriminate attacks (cfr. targeting logic) and its attitude with respect to risk-taking (cfr. openness to new ideas). For instance, apocalyptic or religiously inspired terrorist organisations are often considered to be the most-likely perpetrators of nuclear terrorism because they often deliberately and indiscriminately target innocent civilians to achieve their objectives.[166] Moreover, discussions on a terrorist organisation's motivation to pursue a nuclear capacity also elaborate on the potential role of outbidding other terrorist organisations (cfr. relationship other organisations),[167] or the potential role of a terrorist organisation's attachment to WMD's (cfr. attachment to weaponry). These factors are taken into account when assessing the likelihood of particular organisations to be interested in this type of weaponry. Aum Shinrikyo's use of chemical and biological weapons is, for instance, often linked to its leader's fascination with futuristic arms. Finally, this latter example also illustrates that these discussions sometimes touch upon the role of the leader's background, values and authority (cfr. group dynamics). Shoko Asahara – the leader of Aum Shinrikyo – is, e.g. often considered an important driver behind their quest for WMD's.[168]

Likewise, discussions on the availability of nuclear know-how and technology and the availability of fissile material often embrace various of the identified parameters with respect to innovation and

[166] See, e.g., Ferguson and Potter, *The Four Faces of Nuclear Terrorism*, chapter 2; Ackerman, "Motivations for Engaging in Nuclear Terrorism."
[167] E.g. Ackerman, "Motivations for Engaging in Nuclear Terrorism," 4.
[168] E.g. Andrea Nehorayoff, Benjamin Ash, and Daniel Smith, "Aum Shinrikyo's Nuclear and Chemical Weapons Development Efforts," *Journal of Strategic Security* 9, no. 1 (2016): 35.

technology acquisition by a terrorist organisation. First, these discussions often start by reflecting upon the technical challenges to an improvised nuclear device. Various publications focus on how difficult it actually is to construct and detonate an improvised nuclear device (cfr. nature of technology).[169] Second, these discussions often revolve around assessing the nuclear security regime: what are the strengths of the nuclear security regime, and which opportunities are there available for terrorist organisations (cfr. durability; countermeasures)?[170] Finally, discussions on this theme also focus on the capabilities of a terrorist organisation to acquire nuclear technology and fissile material. These discussions often revolve around whether or not a particular terrorist organisation might have the necessary resources or might receive help from other cooperative organisations (cfr. resources; relation other organisations). Yet, these discussions also touch upon the terrorist organisation's operational experience (cfr. dynamics of the struggle; durability) or its technological awareness (cfr. openness to new ideas). Al Qaeda was, for instance, often considered to be a likely perpetrator of nuclear terrorism because of its size, lifespan, resources, and demonstrated awareness of nuclear weapons.[171]

Moving to the crux of the argument, however, it is remarkable that some aspects of the parameters with respect to innovation and technology acquisition by a terrorist organisation are not adequately covered by the three traditional nuclear terrorism variables. More specifically, discussions on the likelihood of nuclear terrorism do not systematically explore the role of the decision making dynamics (cfr. openness to new ideas), or the group's structure and the overall levels of internal disputes (cfr. group dynamics). Yet, as we have seen, these issues are expected to be of essential importance in effectively implementing a nuclear terrorism project. This nonroutine plot is expected to be characterised by a high task variability and low task analysability. One cannot but wonder how a terrorist organisation would need to go about in implementing such a project. For instance, who should make which decisions in a nuclear terrorism project, or how will the organisation deal with any unforeseen obstacles? These type of questions need to be targeted in nuclear terrorism threat assessments. Likewise, although being touched upon in traditional nuclear terrorism threat assessments, I believe discussions on this theme often underplay – or do not sufficiently systematically study – the role of a terrorist organisation's security environment (cfr. dynamics of the struggle) and the organisation's access to outside help or operational experience (cfr. human resources).

[169] See, e.g., Mark et al., "Can Terrorists Build Nuclear Weapons?"; Rodionov, "Could Terrorists Produce Low-Yield Nuclear Weapons?"; Bunn and Wier, "Terrorist Nuclear Weapon Construction: How Difficult?"
[170] E.g. Bunn et al., "Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline."
[171] E.g. Mowatt-Larssen, "Al Qaeda Weapons of Mass Destruction Threat: Hype of Reality."

This study therefore aims to more systematically explore the role and impact of such parameters throughout the implementation of a nuclear terrorism plot. Specifically, reflecting on these parameters, I believe these can all be categorised under one common denominator: *the organisational design*. This concept encompasses the aforementioned parameters of innovation and technology acquisition by a terrorist organisation. Henry Mintzberg - the godfather of organisational theory – defines organisational design as: "the sum total of the ways in which its labor is divided into distinct tasks and then its coordination is achieved among these tasks."[172] In other words, the organisational design refers to the assignment, control and coordination of different tasks, powers and responsibilities. Different types of design relate to different sources of control and coordinating mechanisms vis-à-vis the work.[173] It encompasses both the formal task and authority relationships and the more informal interactions between members of the organisation. The organisational design can thus be considered to be the common denominator of issues such as decision-making dynamics, group structure, internal disputes, operational security, and operational experience. It is essential in striking "a balance between external pressures from the organisation's external environment and internal pressures from, for example, its choice of technology."[174] This way, the organisational design can be expected to have an important impact on the likelihood that a terrorist organisation can effectively complete a nuclear terrorism project.

This study thus starts from the following research question: "What is the role of a terrorist group's organisational design in implementing the construction and detonation of an improvised nuclear device?" Clear links can be drawn to the individual parameters on terrorist innovation and technology acquisition throughout the following chapters. Yet, this study adopts this one encompassing independent variable. This strengthens the analytical clarity. By more systematically exploring the role of the organisational design, I aim to contribute to the comprehensive nature of any future nuclear terrorism threat assessment. It might shed new light on the three aforementioned traditional nuclear terrorism variables and enable a deeper understanding of the nuclear terrorism threat.

[172] Henry Mintzberg, *Structure in Fives: Designing Effective Organisations* (New Jersey: Prentice-Hall, 1983). 2
[173] Based on, e.g., Mintzberg, *Structure in Fives*; Freidson, *Professionalism: the Third Logic.* (Cambridge: Polity Press, 2001)
[174] Jones, *Organisational Theory, Design and Change,* 10.

3. Establishing some hypotheses

After having established the necessity of an organisational approach in nuclear terrorism threat assessments, and having formulated a research question on the role of the organisational design, this chapter will develop some hypotheses on the relation between the organisational design of a terrorist organisation and the nuclear terrorism threat. I will therefore draw on both broader terrorism literature and literature particularly focused on the role of the organisational design. Embedding this study in the relevant literature on this topic, I intent to substantiate my particular expectations with respect to the relation between the organisational design of a terrorist organisation and the nuclear terrorism threat. The empirical case studies that follow in the next chapters of this dissertation will subsequently shed more light on the plausibility of these expectations.

Specifically, this chapter will develop three intertwined hypotheses that – collectively - constitute an effectiveness-efficiency trade-off. The first hypothesis focuses on the type of organisational design that is expected to increase the likelihood that a terrorist organisation can effectively implement a project that is characterised by a nonroutine nature of *technology*. To be precise, I will argue that a more organic organisational design is likely to benefit the effective implementation of a nuclear terrorism project. Next, I will focus on two other organisational contingencies that are also relevant to a terrorist organisation: its operational *environment* and its *strategy.*[1] This refers respectively to the second and third hypothesis. The second hypothesis relates to the match between a terrorist group's organisational design and its clandestine operational environment. I expect that an organic type of organisational design is hard to reconcile with a terrorist group's clandestine operational environment. I expect that this organisational design is an inefficient way for a terrorist organisation to guarantee its security. Next, based on these two hypotheses, this chapter will develop a third hypothesis on what these expectations imply with respect to a terrorist organisation's strategy. Specifically, adopting an instrumental rational

[1] Lex Donaldson, *The Contingency Theory of Organisations* (London: SAGE Publications, 2001), 1.
These two particular contingencies are often mentioned in the literature in this field: Donaldson, for instance, refers to the environment, the organisational size, and the strategy. Gareth Jones names the environment, the strategy, the technology, and the internal processes that develop in an organisation over time. Mintzberg refers to the organisation's age and size, its technical system, the environment, and power. While this thus also includes other contingencies (e.g. age and size), reading through the literature leads me to believe that the organisation's environment and strategy will be most relevant to the nuclear terrorism threat. These two contingencies clearly link to the three other traditional nuclear terrorism variables – access to know-how and technology, to fissile material, and the motivation to go nuclear - and are thus necessary to reflect upon in order to better understand the diverse variables and their interplay. In other words, focusing upon these two contingencies will benefit a more encompassing analysis of the likelihood of nuclear terrorism.

approach, I expect an increasingly inefficiently functioning terrorist organisation with respect to the attainment of its political and organisational goals.

3.1. Organisational design and technology

This chapter will first explore the relationship between the organisational design and the technology that the organisation aims to adopt. It will argue that we might expect a terrorist organisation to be most likely to effectively complete a nonroutine nuclear terrorism project by means of an organisational design similar to an organic design. Such an organisational design is conducive to the effective implementation of an innovative project.

The organisational design can be considered a main determinant to the effective adoption of a particular type of technology. The way that work and resources are divided, controlled and coordinated influences the organisation's performance and the effective implementation of the different tasks and activities. This argument is called the *technology imperative*. It is attributed to the work by Joan Woodward but also confirmed by other authors such as Henry Mintzberg, Gareth Jones, or Dewar and Hage.[2] Some authors have criticised this idea based on, e.g., the measurement of technology.[3] The previous sections have however demonstrated that it is worthwhile to explore the relevance of the organisational design to the implementation of a nonroutine nuclear plot by a terrorist organisation.

Typologies of the organisational design have proliferated up to the point of confusion.[4] Yet, I agree with Gareth Jones that the principal challenge for any organisational design is to "allocate people and resources to organisational tasks and establish the task and authority relationships that allow the organisation to achieve its goals."[5] Any organisational design thus basically boils down to the issue of control and coordination of its resources. Brian Jackson – specifically reflecting upon a classification of terrorist organisations – similarly identifies the importance of "command and control authority

[2] The attribution to Woodward is suggested by Richard Burton and Borge Obel, *Strategic Organisational Diagnosis and Design: The Dynamics of Fit* (New York: Springer Science, 2004), 240. Yet, other authors also seem to (implicitly) confirm the importance of the technology variable: Henry Mintzberg, "Structure in 5's: A Synthesis of the Research on Organisation Design," *Management Science* 26, no.3 (1980): 327; Gareth Jones, *Organisational Theory, Design and Change: Text and Cases*, 4th ed. (Pearson Prentice Hall, 2003), 274; Robert Dewar and Jerald Hage, "Size, Technology, Complexity, and Structural Differentiation: Toward a Theoretical Synthesis," *Administrative Science Quarterly* 23, no. 1 (1978): 111.

[3] See, e.g., M.G. Rao & V.S.P. Rao, *Organisation Design, Change And Development* (New Delhi: Discovery Publishing House, 1999), 30.

[4] Eliot Freidson, *Professionalism: The Third Logic* (Cambridge: Polity Press, 2001), 4.

[5] Jones, *Organisational Theory, Design and Change,* 95.

relationships."[6] The typology that will be used in this study is consequently primarily based on this issue of control and coordination. Before elaborating on this typology and its building blocks, note however that I merely intent to use the concept of the organisational design as an analytical tool. This concept is a heuristic device that enables me to systematically explore the challenges to the implementation of a nonroutine nuclear terrorism plot.

This study reflects on three dimensions of the organisational design of a terrorist group that would like to implement a nuclear terrorism plot: the interconnectedness of the group, the level of hierarchical control, and the degree of specialisation. These dimensions shape the issue of control and coordination. Jacob Shapiro identified them as those "that matter for covert organisations."[7] First, the interconnectedness of the project group refers to both the number of connections between individuals in one cell in the group (=intra-cell) and the number of connections between these cell members with members of the project group (or other people) outside the cell (=inter-cell).[8] Interconnectedness is thus clearly linked to the issue of coordination and control. It refers to the way that information and resources are being shared.[9] Second, Shapiro identifies "control" as the salient issue to the level of hierarchy. The question in this context becomes: "who has control, and over what?"[10] Considering the first question, the center can be considered to be the political and ideological leadership. In contrast, those members who have to carry out the particular tasks and activities are situated on a decentralised position. Considering the second question, Shapiro distinguishes between control over the operations and control over the resources. This respectively refers to control over both the targeting and the procedures to carry out the operations and control over the group's financial resources, information and personnel.[11] Finally, the level of specialisation is an important dimension to the organisational

[6] Brian Jackson, "Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organisations and Its Application to Al Qaeda," *Studies in Conflict and Terrorism* 29, no. 3 (2006): 243.

[7] For this section, I build a lot on the work by Jacob Shapiro (Jacob Shapiro, "Organising Terror: Hierarchy and Networks in Covert Organisations," *unpublished paper,* 2005, 5-15). Yet, Shapiro develops these insights in the framework of prolonged terrorist campaigns (rather than in the framework of the implementation of one nonroutine attack). Note in this context subsequently that this section will often refer to literature that focuses on the organisational level (= the terrorist organisation as a whole; and its campaign of terror). This is a different focus than this study's focus (= the implementation of one particular plot by (potentially) a subgroup of the organisation). Yet, I believe that most of these insights with respect to the organisational level can also be expected to be at play at the level of one particular attack. In case I believe this different focus might change my hypotheses, I will explicitly outline this in the text.

[8] Shapiro defines a cell as a functional unit. This refers to "an individual or group of individuals that take consequential actions." He subsequently operationalised interconnectedness as "the average number of connections that minimal functional units in an organisation have with other such units." He thus primarily focuses on inter-cell connections. This study, however, wants to explicitly include intra-cell connections as well. These can be expected to be important during the implementation of an individual plot.

[9] Shapiro, "Organising Terror," 8-9.

[10] Ibid., 11.

[11] Ibid., 10.

design. While Shapiro primarily considers specialisation at the unit level,[12] this study primarily focuses on specialisation at the individual level. On the one hand, it can refer to task specialisation. This implies that "organisations divide the work in particular tasks that require little education or skills." On the other hand, it can refer to personal specialisation. This implies that the specific jobs require long periods of training to master the skills and knowledge of the occupation.[13] This latter issue is closely related to the difference between technical knowledge (techne) and practical knowledge (metis).[14] The type of specialisation, which represents different qualities of work,[15] has consequences for those who perform the job and the control and coordination over the different jobs. It will thus shape the organisational design.

Based on these dimensions, I distinguish between two ideal-types of a group's organisational design (or a sub section of the group): a mechanistic organisational design and an organic organisational design. Admittedly, such a rudimentary distinction does not do justice to hybrid structures or individual variations.[16] Yet, authors such as Ligon et al. and Mintzberg claim that organisations tend to vary across variables in systematic ways.[17] Moreover, and more importantly, reducing the typology of potential organisations to these two ideal-types benefits the analytical clarity of this exploratory project.[18] This subsequently leads to the following table 3.1.

---

[12] Shapiro, "Organising Terror," 12-15.

[13] Jerald Hage, "An Axiomatic Theory of Organisations," *Administrative Science Quarterly* 10, no. 3 (1965): 294. This also aligns with Freidson's distinction between "mechanical specialisation" – where individual discretion is minimised – and "discretionary specialisation" – where discretion or fresh judgement must often be exercised (Freidson, *Professionalism,* 23).

[14] See, e.g., Kathleen Vogel's emphasis on uncodified knowledge: Kathleen Vogel, *Phantom Menace or Looming Danger? A New Framework for Assessing Bioweapons Threats* (Baltimore: The John Hopkins University Press, 2013), 61; Michael Kenney, "'Dumb' Yet Deadly: Local Knowledge and Poor Tradecraft Among Islamist Militants in Britain and Spain," *Studies in Conflict & Terrorism* 33, no. 10 (2010): 911–32.

[15] Freidson, *Professionalism*, 22.

[16] For instance, Shapiro ("Organising Terror") focuses specifically on different variations. He furthermore argues that we should think about the organisational design as a matter of degree, not of kind.

[17] Gina Ligon et al., "Putting the 'O' in VEO's: What Makes an Organisation?," *Dynamics of Asymmetric Conflict* 6, no. 1-3 (2013): 115; Mintzberg, "Structure in 5's", 328.

[18] Notwithstanding the analytical purpose of this typology, it is also true that the utility of a typology is often judged on its applicability in practise. I therefore briefly elaborate on two arguments that demonstrate that this typology's is also applicable in practise.
(1) Reflecting up the literature in the field, it becomes clear that various scholar adopt a typology that - to a large extent - builds on this distinction between mechanistic and organic. Notwithstanding variation in the (detailed nature of the) classification, various typologies consider this to be an analytically and empirically useful starting point. Note that this dichotomous distinction clearly resonates with the work by Durkheim. Yet, some authors contest a one to one correspondence (e.g. Lex Donaldson, *in defense of organisation theory: a reply to the critics* (Cambridge: Cambridge University Press, 1985), 73). Moreover, Durkheim's primary focus was on society as a whole. The dichotomous distinction in organisational studies can thus – to my knowledge – be attributed to Burns and Stalker (Tom Burns and G.M. Stalker, *The Management of Innovation* (USA: Tavistock Publications, 1961). Other authors' work is, however, clearly in a similar line of thought. An organically designed organisation is, e.g. closely related to Freidson's understanding of a professional organisation, which he defines as "institutional circumstances in which the members of the occupations rather than consumers or managers control the work"

Table 3.1. Mechanistic versus organic organisational design

	Mechanistic organisational design	Organic organisational design
Level of interconnectedness	Low number of intra-cell and inter-cell connections	High number of intra-cell and inter-cell connections
Level of hierarchy	Tight control over operation and resources by the leadership	Tight control over operation and resources by the operators/experts
Level of specialisation	Low person specialisation (no specialisation or task specialisation)	High person specialisation

(Freidson, *Professionalism,* 12) Likewise, an organically designed organisation can be linked to what Mintzberg describes as an adhocracy, namely a configuration that "fuse(s) experts drawn from different specialties into smoothly functioning project teams" (Henry Mintzberg, *Structure in Fives: Designing Effective Organisations* (New Jersey: Prentice-Hall, 1983),254). This is in contrast to the other forms of organisational types that he identifies (a simple structure, a machine bureaucracy, a professional bureaucracy, and a divisionalized form). These other types of organisations (except for the simple structure) have more bureaucratic tendencies. They thus lean closer to a mechanistic type of design. With respect to the organisational approach in terrorism studies, Gina Ligon et. al ("Putting the 'O' in VEO's") explicitly start from this prototypical distinction between mechanistic and organic organisational types of organisations. Empirically building on groups with a white supremacist ideology, they subsequently distinguish between groups, simple organisations, mechanistic organisations, organic organisations and hybrid forms. Another example is Brian Jackson's distinction between groups, network and movements ("Groups, Networks, or Movements"). In this typology, tightly coupled groups can be linked to a mechanistic organisational design while movements can be linked to more organically designed groups.

(2) Second, while it is true that the design is always a matter of degree rather than kind, I will give three illustrative real-world examples of subunits of a terrorist group. This will further illustrate this typology's practical applicability. First, one could argue that the IRA's engineering department – which developed, e.g. advanced mortars - can be considered to be (more) organically designed. This group drew on both talented amateurs who developed their specialised personal skills over time and a limited number of highly-skilled technical personnel (such as professional engineers). The unit and its experts seems to have enjoyed a relatively high level of operational autonomy. Ackerman notes, for instance, "the ED enjoyed a degree of independence from frontline operations, and the decision to engage in the development and production of mortars may have been the PIRA leadership's way of "letting the movement's better technical intellects have their experiments." Finally, there are also seems to have been sufficient high level of connectedness. Ackerman notes, for instance, that "when things went wrong with an attack, the operatives conducting the attack would be debriefed by superiors." There was a commitment to learning. Second, the drone program by the Islamic State – which significance seems to lie less in its technical sophistication and more in the collection of simple, low-cost and replaceable devices… as well as the group's use of the drones in creative ways" – can be considered to be (more) mechanistically designed. Indeed, a CTC report states that "the Islamic State's centralised and bureaucratized approach to manufacturing provided the framework needed to bring the group's drone program to scale." Third, the Covenant, the Sword and the Arm of the Lord – a millenarian, survivalist Christian Identity organisation who attempted to employ cyanide – can also be considered to be (more) mechanistically designed. According to Ackerman, there was lack of specialised knowledge and skills to disseminate and employ the cyanide, and they were driven by non-rational and ideological tactical theories. James Ellison – the charismatic leader of the group – dominated decision-making, thereby contrasting operational autonomy and high interconnectedness (Gary Ackerman, "'More Bang for the Buck' Examining the Determinants of Terrorist Adoption of New Weapons Technologies," doctoral dissertation, King's College, 2014; Don Rasler, "The Islamic State and Drones: Supply, Scale, and Future Threats," *Combating Terrorism Center,* 2018).

On the one hand, a mechanistic design is meant to induce people to behave in a predictable and accountable way.[19] The tasks and activities of the project require little personal specialisation. Little discretion is needed for decision-making with respect to the particular tasks.[20] As Burns & Stalker state: "the problems and tasks facing the concern as a whole are broken down."[21] Given there is no need for personal specialisation, control and coordination of these members is likely to be centralised.[22] Leadership will directly impose decisions on who will do what, when and where. This increases the likelihood that an action will be taken as desired. Members of the terrorist group know what to target, how to target it, and their individual roles and responsibilities in the plot. There is a relatively low number of connections between individuals in one cell in the group and connections between cell members with members of the project group (or other people) outside the cell. The interaction between members of the group tends to be vertical rather than lateral, i.e. between superior and subordinate.[23] The organisation adopts formalised roles and rules to regulate and control the actions of its members.[24] There is thus a more "hierarchic structure of control, authority and communication."[25] This type of design relates to what Weber would describe as a bureaucracy.

I expect that this type of mechanistic organisational design would increase the effectiveness of the implementation of a particular terrorist attacks that falls within a group's standard operations (such as, e.g. the implementation of a simple military attack). Individual members can act independently from each other while the hierarchical elements of control (e.g. formal rules, monitoring activities, resource allocation, punishment) make sure that the individual agents' behavior is in line with the principal's preferences. Considering these clear command and control structures, there is an increased level of accountability. These type of mechanistic organisations are often considered to be more suitable to a terrorist organisation's production of standard violence.[26] The terrorist organisation's operational capacity seems to increase.[27]

---

[19] Jones, *Organisational Theory, Design and Change,* 115.

[20] Note, however, that most individual terrorists will need some extent of personal specialisation (e.g. how to make clandestine financial transactions is not something every civilian knows how to do). Yet, such activities can be considered to be standard operations for a terrorist organisation.

[21] Burns and Stalker, *The Management of Innovation*, 120.

[22] Ibid., 120.

[23] Ibid., 120.

[24] Ibid., 120.

Note that the terrorism literature also identifies similar characteristics in terrorist *organisations.* See, e.g., Ligon et al., "Putting the 'O' in VEO's."

[25] Burns and Stalker, "The management of Innovation", in ed. Michael Handel, *The Sociology of Organisations: Classic, Contemporary and Critical Readings* (USA: Sage Publications, 2003), 49.

[26] See, e.g. Lindsay Heger, Danielle Jung, and Wendy Wong, "Organising for Resistance: How Group Structure Impacts the Character of Violence," *Terrorism and Political Violence* 24, no. 5 (2012): 743–68.

[27] Note in this context that it is worth repeating that I am currently describing an ideal-type of organisational design. In real life, a terrorist organisation might, e.g., need to take into account security considerations related to

Yet, on the other hand, I do not expect this type of mechanistic organisational design to be suitable to the implementation of a nuclear terrorism plot. Although I expect that this type of design is beneficial to the production of violence *via standard operations*, I expect that the implementation of a nonroutine nuclear terrorism plot would benefit most from a more organic organisational design. This type of organisational design is the opposite of a mechanistic organisational design. According to Jones, an organic organisational design is meant to "promote flexibility, so people initiate change and can adapt quickly to changing conditions."[28] I therefore expect it to be more suitable to the contingencies and complexities related to a nuclear terrorism plot.

Indeed, the tasks and activities of a nonroutine nuclear terrorism plot require a high levels of personal specialisation (both techne and metis). A diversity of skills and expertise would be necessary in the identified nuclear terrorism scenario (e.g. clandestine procurement skills, nuclear skills, advanced military skills, explosives and ballistics experts, illicit trafficking experts, financial experts, etc.). These experts are expected to be a particular importance in such an innovative terrorism plot.[29] They would need to develop solutions to a variety of exceptional situations. These nonroutine problems are hard to systematically analyse in advance and can be caused by a diversity of factors, such as, e.g., unnoticed security measures, unexpected technical hick-ups, moral doubts, or any other contingent factor. Next, these experts also need to be able to function in the organisation in the best way possible. On the one hand, I expect that this implies that experts need to have sufficient discretion and decision-making authority with respect to the implementation of their tasks and activities.[30] Operational autonomy has been identified as an important factor throughout the implementation of complex engineering efforts by violent non-state actors. Ackerman et al. stated, for instance, that the responsibility for such projects is often given to a "specialist technical or logistical organ in the group."[31] It is expected that different hierarchical elements – such as strict formalisation, centralised decision-making, or tight planning and control systems - would thwart the necessary flexibility, creativity and adaptability by these experts.[32] Moreover, it is suggested by some organisational behavior literature that such hierarchical elements

---

such hierarchical elements. See, e.g. Jacob Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organisation* (Princeton: Princeton University Press, 2013).

[28] Jones, *Organisational Theory, Design and Change,* 116.

[29] See, e.g., Nicole Tishler, "Trends in Terrorists' Weapons Adoption and the Study Thereof," *International Studies Review* 20 (2018): 368-394.

[30] See, e.g., Charles Perrow, *Organisational Analysis: A Sociological View* (Great Britain: Tavistock Publications, 1970; Mintzberg, *Structure in Fives*; Freidson, *Professionalism;* Jones, *Organisational Theory, Design and Change;* Vogel, *Phantom Menace or Looming Danger?*

[31] Gary Ackerman, "Comparative Analysis of VNSA Complex Engineering Efforts," *Journal of Strategic Security* 9, no. 1 (2016): 126.

[32] Paul Gill et al., "Malevolent Creativity in Terrorist Organisations," *The Journal of Creative Behavior* 47, no. 2 (2013): 138; Ligon et al., "Putting the 'O' in VEO's," 115 & 126-128.

could hamper the experts' intrinsic motivation and dedication.[33] Control and coordination over the implementation of a nonroutine nuclear terrorism plot is therefore expected to be best decentralised. Yet, this does not mean that the leadership should be absent. Leadership can focus the group's efforts and provide strategic guidance. Moreover, the leadership can enhance the operational environment needed for the effective implementation of such a plot via, e.g., adequate resource support).[34] On the other hand, I also expect that a high level of interconnections (e.g. extensive (face-to-face) interactions and hands-on training) would improve the experts' functioning in the organisation.[35] Employees need to work together and coordinate their actions.[36] Intra-cell and inter-cell communication is expected to be necessary to cope with the nonroutine and interdependent nature of the different tasks and activities (e.g. the type of fissile material will influence the design and necessary components of the nuclear device). Burns and Stalker highlight in this respect "a lateral rather than a vertical direction of communication through the organisation, communication between people of different rank, also, resembling consultation rather than command."[37]

Such an organic organisational design is thus often considered to be more conducive to sophisticated innovation. It maximises flexibility and responsiveness to uncertainty.[38] I subsequently expect that this type of organisational design would increase the likelihood that a terrorist organisation can effectively implement the construction and detonation of an improvised nuclear device. Admittedly, the development of a less sophisticated and efficient nuclear explosion is technically less challenging. This potentially alleviates the nonroutine nature of the plot to some extent. Yet, considering the implementation of the plot as a whole, I nevertheless expect such a plot to be nonroutine. The first hypothesis (= H1) is thus:

> H1: A terrorist organisation is most likely to effectively complete a nuclear terrorism project by means of an organisational design similar to an organic design.

[33] See, e.g., Amabile et al. "Assessing the work environment for creativity," Academy of management journal, 39, no. 5 (1996): 1161-1162.
[34] See, e.g., Adam Dolnik, *Understanding Terrorist Innovation: Technology, Tactics, and Global Trends*, Contemporary Terrorism Series (London & New York: Routledge, 2007), 159 ; Gill et al., "Malevolent Creativity in Terrorist Organisations, 138-141; Jackson, "Groups, Networks, or Movements," 244.
[35] Brian Jackson, "Technology Acquisition by Terrorist Groups," 200.
[36] Jones, *Organisational Theory, Design and Change,* 115-116.
[37] Burns and stalker, "The management of Innovation," 49.
[38] Gill et al., "Malevolent Creativity in Terrorist Organisations," 138.
Note in this context that this type of design can be compared to what Mintzberg would call an adhocracy design, or what Freidson would call a professional organisation.

Technology is however not the only organisational contingency that reflects the situation of the organisation. As structural contingency theory claims, the organisational design simultaneously needs to match with other contingencies. Besides the need to match the organisational design with the technology that they aim to adopt, two of the most relevant contingencies are the organisation's clandestine environment and the organisational strategy.[39]

3.2. Organisational design and the environment

In order to develop the second (and third) hypothesis, I first need to draw attention to the diversity of goals for a terrorist organisation. In general, one can distinguish between tactical goals and strategic goals.[40] The tactical levels refers to each particular act of terrorism and its related measures (e.g. nuclear terrorism, beheadings, kidnapping, propaganda). Success on a tactical level can be measured by means of diverse criteria such as, e.g., operational success, publicity, or the undermining of opponents. Yet, these tactical events ultimately serve to benefit the overall strategic objectives of the organisation. As indicated in the adopted definition of terrorism, a terrorist organisation ultimately aims to influence the political behavior of a given target group. The organisation must link this tactical engagements together, so that they serve a broader purpose. Considering this strategic level, it is important to distinguish between the group's political goals and its organisational goals. On the one hand, terrorist organisations have political ambitions such as the consolidation of a Caliphate, the overthrown of a regime, or more territorial autonomy. Kydd & Walter state in this respect that "although the ultimate goals of terrorists have varied over time, five have had enduring importance: regime change, territorial change, policy change, social control, and status quo maintenance."[41] On the other hand, a terrorist organisation simultaneously want to "maximize its strength and ensure its survival."[42] Indeed, an organisation needs to endure to be able to achieve their political objectives. Any terrorist organisation therefore thus need to secure its operations from law enforcement intrusion or disruption.[43]

---

[39] Donaldson, *The Contingency Theory of Organisations*. 1.
As mentioned in footnote 1, I believe that focusing upon these two contingencies is particularly beneficial to a more encompassing analysis of the likelihood of nuclear terrorism.
[40] See, e.g., Richard English, *Does Terrorism Work: A History* (United Kingdom: Oxford University Press, 2016).
[41] Andrew Kydd and Barbara Walter, "The Strategies of Terrorism," *International Security* 31, no. 1 (2006): 52.
[42] Peter Krause, "The Political Effectiveness of Non-State Violence: A Two-Level Framework to Transform a Deceptive Debate," *Security Studies* 22, no. 2 (2013): 273.
[43] See, e.g., Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* (Princeton: Princeton University Press, 2009).

The second hypothesis relates directly to this latter issue. A terrorist organisation is a clandestine organisation. It needs to limit leaks and defections in order to secure its operations. Diverse variables will impact its capability to do so (e.g. the strength of counterterrorism forces, or – as Eli Berman elaborates on – the loyalty of members to the organisation).[44] Although this study elaborates further on these variables in the following chapters, it leaves them out of the account for now for reasons of analytical clarity. I focus specifically on the role of the organisational design in this section. To be precise, I will argue in what follows that I expect that an organisational design similar to an organic organisational design is hard to reconcile with a terrorist organisation's clandestine environment during the implementation of a nonroutine plot. Building on the available literature, I expect that such a design inherently implies increased security costs. It can be considered to be an inefficient way for a terrorist organisation to guarantee the security of its nuclear terrorism plot. These expected security risks are a result of each of the three aforementioned organisational design features.

First, it has been argued that a nonroutine nuclear terrorism plots requires people with a high level of personal specialisation. Different skills and expertise are expected to be necessary. Both techne and metis will be important to effectively implement such a plot. Yet, it is expected that the recruitment or allocation of these people in a clandestine operational environment inherently implies increased security risks. Not just everyone can complete the different tasks and activities. Any failed recruitment effort, or the mere involvement of these particular people with specialised skills, might imply detection by counterterrorism forces. A terrorist organisation would need to remain aware of mediocre (or plain bad) scientists and technicians, con men, or infiltration by counterterrorism forces. Note in this respect that resourceful and popular rebel groups can adopt expertise-oriented recruitment periods.[45] Although these organisations might often recruit opportunistic joiners that demonstrate little commitment to the common goals of the organisation,[46] they might also have the opportunity to be choosy and select people based on specific criteria.[47] The issue of espionage, defection or infiltration is however expected to remain particularly worrisome for a terrorist organisation trying to recruit people for a nuclear terrorism plot. Loyalty to the terrorist organisation might prove to be a particular important recruitment

[44] Eli Berman, *Radical, Religious and Violent: The New Economics of Terrorism* (Cambridge: MIT Press, 2009)
[45] Steven Windisch, Michael Logan, and Gina Scott Ligon, "Headhunting Among Extremist Organisations: An Empirical Assessment of Talent Spotting," *Perspectives on Terrorism* 12, no. 2 (2018): 19; Mia Bloom, "Constructing Expertise: Terrorist Recruitment and 'Talent Spotting' in the PIRA, Al Qaeda, and ISIS," *Studies in Conflict & Terrorism* 40, no. 7 (2017): 603–23; Brian Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict & Terrorism* 24, no. 3 (2001): 183–213."
[46] Jeremy Weinstein, "Resources and the Information Problem in Rebel Recruitment," *Journal of Conflict Resolution* 49, no. 4 (2005).
[47] See, e.g., Samuel T. Hunter et al., "Recruitment and selection in Violent Extremist Organisations: Exploring what Industrial and Organisational Psychology Might Contribute," *American Psychologist* 72, no. 3 (2017): 248.

criteria. Any security breach could potentially lead to the detection of the project. As Abrahms already indicated, it is essential that group members "act together to accomplish a common goal."[48]

Second, less hierarchical institutional circumstances are expected to increase the security risks for a terrorist group implementing a nuclear terrorism plot. This expectation seems to run against a common assumption in the terrorism literature. It is often claimed that this organic organisational design feature actually benefits a terrorist group's organisational security. Yet, this literature often focuses on the whole terrorist organisation over a longer period of time. It is often claimed, for instance, that a more hierarchical design inherently implies security costs for a terrorist organisation. Standardisation of rules and procedures makes an organisation more predictable and easier to monitor, manipulate and penetrate. It moreover increases the risks to leaving signatures and footprints.[49] Likewise, the monitoring or auditing of members of the organisation implies additional security vulnerabilities due to the increased communication and the establishment of links between leaders and individual members.[50] A less hierarchical design is therefore often considered to be beneficial to a terrorist organisation's security. As Max Abrahms put it, "in terms of defense, decentralisation supposedly makes militants harder to detect, infiltrate, isolate, prosecute, and ultimately defeat."[51]

Yet, also considering the whole terrorist organisation over a longer period of time, it should also be acknowledged that a more hierarchical structure of control, authority and communication has some particular security benefits. Mobley argued, for instance, that tightly structured organisations have the advantage of being capable to provide their members with better training in counterintelligence methods. They can be trained in improving securing while implementing operations.[52] Moreover, Abrahms argued that centralisation can prevent members from "shooting the cause in the foot." He argues that centralisation enables the leader to better communicate their tactical instructions, discipline wayward members, and improve the vetting of recruits.[53] A more hierarchical type of design thus enables the organisation to better manage members and prevent potentially divergent behavior. This

[48] Max Abrahms, *Rules for Rebels: the Science of Victory in Militant History* (Oxford: Oxford University Press, 2018), 115.
[49] Blake Mobley, *Terrorism and Counterintelligence: How Terrorist Groups Elude Detection* (New York: Colombia University Press, 2012), 231.
[50] Shapiro, *The Terrorist's Dilemma,* 26-63.
Shapiro identifies four variables that influence this trade-off: the extent that a terrorist organisation needs to be discriminate, the role of uncertainty for leaders and operatives, the preference divergence between leaders and operatives, and the extent of governmental counterterrorism activity.
[51] Abrahms, *Rules for Rebels,* 148.
[52] Mobley, *Terrorism and Counterintelligence,* 229-230.
[53] Abrahms, *Rules for Rebels,* 126-137.

prevention of divergent behavior improves the organisation's security. A more organic organisational design lacks these security benefits.

Extrapolating these mixed insights specifically to the implementation of a particular nonroutine plot, I expect that the latter type of arguments will prevail. While Abrahms' argument is oriented to the control and influence of activities being carried out in pursuit of the organisation's strategic goals,[54] I expect that more hierarchical elements would also improve the management over individual members throughout the implementation of a particular nonroutine plot. It would facilitate the prevention of divergent behavior by the individual team members and improve the security throughout the implementation of the plot. It follows then that the implementation of nuclear terrorism plot by an organisation that is less hierarchically designed lacks these security benefits. Indeed, notwithstanding the fact that the leadership of the organisation might provide strategic guidance and resource support, a less hierarchically designed organisation is expected to be characterised by higher levels of, e.g., unclear job definitions and authority relations, random and unplanned (personal) developments, and multiple lines of communication. In other words, such an organic organisational design is expected to create an increased level of "fluidity, confusion and ambiguity."[55] While this type of design increases the likelihood of the team effectively completing a nonroutine plot, it thus simultaneously implies an increased risk with respect to divergent behavior by any individual involved in the plot.[56] It is not necessarily true that the motivation and goals of the "rank-and-file" is similar to the incentive structure and objectives of the leadership.[57] A less hierarchical design implies less operational control over their actions. This could lead to, e.g., operational errors or frustrations, (moral) doubts with respect to the project, and/or leaks to counterterrorism forces. This is the reason why I expect such an organic organisational design to be an inefficient way to cope with a clandestine environment during the implementation of a nuclear terrorism plot.

Finally – and perhaps the most obvious reason – I expect that the increased level of intra-cell and inter-cell connections related to an organic organisational design will make this type of organisational design an inefficient security approach for a terrorist organisation that aims to implement a nuclear terrorism plot. Any organic organisational design implies increased communication and coordination efforts

[54] Abrahms, *Rules for Rebels,* 11.
[55] Mintzberg, *Structure in Fives,* 276.
[56] Note in this context that the use of the term 'divergent behavior' in this study does not necessarily refer to the same type of divergent behavior as meant by Max Abrahams. Abrahams focuses on divergent behavior on a strategic level. Divergent behavior thus also implies behavior that is not in line with the organisation's strategic goals. This study, however, focuses on the particular implementation of a nonroutine plot. Divergent behavior refers in this context to behavior that impedes the implementation of the plot.
[57] Abrahms, *Rules for Rebels,* 108-112.

between different cells and individual members of the group. This is necessary to effectively implement a nonroutine plot. In order to be flexible and problem-solving, people need to communicate and coordinate a lot. They often need to combine knowledge and information (e.g. via mutual adjustment within cells, or liaison devices between cells) to cope with different unexpected situations that cannot be analysed in advance. As mentioned earlier, I expect this design to be suitable to the implementation of a nuclear terrorism plot. Considering the nonroutine and interdependent nature of the different tasks and activities of such a plot (e.g. the type of fissile material will influence the design and necessary components of the nuclear device), I expect a lot of communication and coordination to be necessary between the different cells and individual members of the project team. Yet, this high level of connections inherently implies increased security risks to the terrorist organisation. It provides an opportunity for counterterrorism forces to detect (parts of) the ongoing operation. Each communication and coordination tool might be intercepted by counterterrorism forces. Moreover, the lower level of compartmentalisation implies that any security breach might allow counterterrorism forces to intrusively penetrate the plot (and the organisation). This could aggravate the consequences of a potential security breach.

Taking into account each of the three organisational design features, I thus expect that an organic organisational design would be hard to reconcile with a terrorist organisation's clandestine operational environment during the implementation of a nuclear terrorism plot. Admittedly, a mechanistic design would also imply security risks (via, e.g. hierarchical elements). Security risks are ultimately self-evident for any clandestine organisation. Moreover, other factors such as, e.g., the group's popular support will also influence its security environment. Yet, considering the expected increase in recruitment requirements, divergent behavior and intra- and inter-cell connections, I expect an organic design to imply increased security risks when such other factors are kept constant. Note in this context that the discovery of anything that might be connected to a nuclear terrorism plot might imply a surge in efforts to stop such a plot. The defense system might provide a warning.[58] Although this type of design would increase the likelihood that they can effectively complete a nuclear terrorism plot, it can thus simultaneously be considered to be an inefficient way for a terrorist organisation to guarantee the security of this plot. The second hypothesis (=H2) is thus:

> H2: An organisational design similar to an organic design implies increased security risks to a terrorist organisation and its nuclear terrorism project.

[58] Michael Levi, *On Nuclear Terrorism* (Cambridge & London: Harvard University Press, 2009), 98-99.

Considering this hypothesis, note again that there might be some variation in the degree that an organisation is organically designed. The development of a less sophisticated and efficient nuclear explosion might require a less organically designed organisation. This might thus also alleviate the security costs to this organisational design. Yet, even a less organically designed organisation implies increased security costs. These security costs, on its turn, could endanger the survival of the organisation. This leads me to some particular expectations with respect to this organisational design and a terrorist organisation's strategy.

3.3. Organisational design and the organisational strategy

The third and final hypothesis builds on the previous two hypotheses. It reflects upon the match between the organisational design and the strategy of a terrorist organisation. While the first and second hypothesis specifically focus on the actual implementation of a nuclear terrorism plot, this final hypothesis goes beyond this tactical level by reflecting upon the strategic level.[59] In short, adopting an instrumental rationality approach, I will argue that I expect that a terrorist organisation pursuing a nuclear capability via an organic organisational design would imply an increasingly inefficiently functioning organisation with regards to the attainment of its political and organisational goals.

The development of the third hypothesis starts by assuming that a terrorist organisation would adopt an instrumental rationality with regards to nuclear terrorism.[60] This implies that I consider terrorist organisations as strategic actors that assess options, consider their interests, and aim to make decision that match their actions with their goals.[61] The decision by a terrorist organisation to go nuclear might be understood "in the broader process of strategic calculation and not simply as a one-off decision."[62] This approach is in line with the adopted definition of a terrorist organisation and seems particularly appropriate to analyse the likelihood of nuclear terrorism. Given the stakes at play and the resources involved in such a plot, a terrorist organisation can be expected to thoroughly reflect strategically upon

[59] Note that this section relates closely to the motivation of a terrorist organisation to go nuclear. As previously noted, these different contingencies are selected in order to benefit the encompassing nature of nuclear terrorism threat assessments. It clearly links to one of the three traditional nuclear terrorism variables.
[60] Max Weber, *Economy and Society: An Outline of Interpretive Sociology* (Berkeley, Los Angeles, London: University of California Press, 1978), 26. He refers to this as "rational consideration of alternative means to the end, of the relations of the end to the secondary consequences, and finally of the relative importance of different possible ends."
[61] Christopher McIntosh and Ian Storey, "Between Acquisition and Use: Assessing the Likelihood of Nuclear Terrorism," *International Studies Quarterly* 62, no. 2 (2018), 2.
[62] McIntosh and Storey, "Between Acquisition and Use," 5.

a nuclear attack.[63] Yet, notwithstanding this assumption, reflection upon the strategy behind a nuclear terrorism act still inherently struggles with two problems. First, the costs and impact of a nuclear attack can vary. The required resources, impact and expected reaction to a nuclear explosion of a few tons (e.g. a fizzle) might differ from that of the detonation of a 15kT bomb. Second, and closely related, it is difficult to assess what constitutes "success" for a terrorist organisation. For instance, it might be the case that a fizzle that does not result in many casualties would lead to a less vigorous response by law enforcement agencies. Such reduced backlash might be politically and organisationally beneficial to a terrorist organisation. It is however hard to know what a terrorist organisation really wants. Political scientist James DeNardo notes in this context that "at best, we can evaluate whether they got what they claimed to want."[64] Yet, notwithstanding that we should take into account these comments, I will try to generally reflect upon the expected gains and losses of such a nuclear terrorism plot.

On the one hand, a nuclear terrorism plot might entail various benefits. On a tactical level, a nuclear terrorism plot can lead to substantial levels of physical destruction and economic costs. This would have a considerable psychological effect on the organisation's different target audiences. It could enable the terrorist organisation to attract more media attention, boost membership and morale, outbid competitors, sabotage peace talks, demonstrate their operational capacity to the enemy, etc. On a strategic level, it is also conceivable that a successful nuclear terrorism plot would benefit a terrorist organisation's broader demands. It could be perceived as appropriate for – what Kydd and Walter call - a terrorist organisation's strategy of attrition, intimidation, spoiling or outbidding.[65] This way, it could for instance be perceived as a useful tool to compel the United States to withdraw from the Middle-East or eliminate the state of Israel. These are just two examples of strategic goals that might be considered attainable by a nuclear terrorism plot.

On the other hand, however, a nuclear terrorism plot might also entail substantial costs. On a tactical level, it would cost the terrorist organisation a considerable amount of time, people and material resources (e.g. financial resources). A terrorist organisation is, however, often limited in its resources. On a strategic level, it is important not to think of the utility of such an attack in a vacuum. First, a

[63] McIntosh and Storey, "Between Acquisition and Use," 2; Thomas Schelling, 'Whatever Happened to Nuclear Terrorism?' *Publisher unknown.* Available at: https://d3qi0qp55mx5f5.cloudfront.net/cpost/i/docs/Schelling-Nuclear-Terrorism.pdf?mtime=1397148761, (accessed April 9, 2019)

[64] James DeNardo, "Power in Numbers: The Political Strategy of Protest and Rebellion," cited in Max Abrahms, *Rules for Rebels: the Science of Victory in Militant History* (Oxford: Oxford University Press, 2018), 8.

[65] Kydd and Walter, "The Strategies of Terrorism."
Note that Kydd and Walter also identify a strategy of 'provocation'. Given that the reaction to a nuclear attack is however not likely to be perceived as an overreaction by many people, I do not consider this strategy to be applicable to nuclear terrorism.

terrorist organisation would need to reflect upon the direct consequences on its strategic goals. For instance, a terrorist organisation with territorial aims might be reluctant to detonate an improvised nuclear device in that territory. Second, a terrorist organisation would also need to reflect upon the further strategic horizon. A nuclear attack might threaten the organisation's continued existence. It could reduce the organisation's popular support, thereby leading to internal threats of disintegration. Moreover, external threats could threaten its continued operations and survival. There is a relatively high likelihood that a nuclear terrorism attack would lead to a unified international community (and the removal of tacit state support) against the terrorist organisation and a substantial reaction by the targeted country. For instance, even though a nuclear attack might precipitate a US withdrawal from the Middle East, there is than "no credible scenario under which the united States would simply "give up," capitulate to those demands, and cease hostilities against the organisation responsible."[66] Abrahms convincingly argued in this context that greater civilian target selection (as would undeniably be the case for a nuclear terrorism plot) leads target countries to infer that the terrorists want to destroy their society and beliefs. Policy concessions becomes very unlikely.[67] This thus leads to the question which type of political goals could only be achieved by this type of nuclear weaponry and not by more conventional attacks. Adopting an instrumental-rational approach, one could ask the question which terrorist organisation would allocate so many resources to such an attack?[68]

Notwithstanding the group's organisational design, one could thus question the strategic value of a nuclear terrorism plot. Yet, taking into account the previous hypotheses, I expect that a more organic organisational design will tilt the cost-benefit balance even more in favour of a negative decision. Even though that an organically designed terrorist organisation might increase the likelihood that it can effectively implement a nuclear terrorism plot, it simultaneously would imply the investment of substantial resources and an increased risk of failure. As Zanders noted in the context of CBW armament, the "terrorist organisation must get it right at every single stage."[69] Any error, detection or defection could potentially lead to a less than optimal weapon or a failure of the plot. This would most-likely imply substantial tactical and strategic costs (e.g. lost investment of resources or a crackdown on the organisation). The likelihood that any strategic gains will be achieved is thus reduced by an organisational design similar to an organic organisational design. Adopting an instrumental rationality approach, hypothesis 3 (=H3) thus becomes:

---

[66] McIntosh and Storey, "Between Acquisition and Use," 9.
[67] Max Abrahms, "Why Terrorism Does Not Work?," *International Security* 31, no. 2 (2006).
[68] See, e.g., Jean Pascal Zanders, "Internal Dynamics of a Terrorist Entity Acquiring Biological and Chemical Weapons: Insights for the Study of Possible Nuclear Weapon Acquisition," in Brecht Volders & Tom Sauer (eds.) *Nuclear Terrorism: Countering the Threat*, Global Security Studies (London & New York: Routledge, 2016), 40.
[69] Zanders, "Internal Dynamics of a Terrorist Entity Acquiring Biological and Chemical Weapons, " 36.

H3: An organisational design more similar to an organic design implies an increasingly inefficiently functioning terrorist organisation with respect to the attainment of its political and organisational goals.

Yet, with respect to this hypothesis, it is essential to note that there are limits to adopting an instrumental-rationality approach to terrorist organisations.[70] Although this hypothesis starts from this approach, it is also known in the literature on this topic that a mere utility-functions perspective is often too simplistic to explain decisions and strategies. Rational and strategic thinking is based on objectivity and deliberation. This is not always the case.

First, it is clear that benefits and losses are not uniformly valued. The reference point and desirability of various prospects impacts decision-making as well.[71] This touches upon a different category of "rationality" identified by Max Weber. He introduced the idea of value-rationality. This refers to a type of social action that is "determined by a conscious belief in the value for its own sake of some ethical, aesthetic, religious, or other form of behavior, independently of its prospects of success."[72] A terrorist organisation pursuing a nuclear capacity might, for instance, be driven by a religious motivation to punish all non-believers, an obsession with nuclear technology, or just a mere desire of revenge. In this context, it is interesting to refer to Hymans' claim that fear and pride play an important role in a national state's decision to pursue a nuclear capacity.[73] Related to this, and as will become relevant in what follows, Weber also distinguishes between devotion "oriented toward a purpose, a common cause, a

[70] See, e.g., Gordon McCormick, "Terrorist Decision Making," *Annual Review of Political Science* 6 (2003): 473–507; Jacob Shapiro, "Terrorist Decision-Making: Insights from Economics and Political Science," *Perspectives on Terrorism* 6, no. 4–5 (2012); Brian Jackson, "Organisational Decision-making by Terrorist Groups", in Paul K. Davis and Kim Cragin, eds., *Social Science for Counterterrorism: Putting the Pieces Together* (Santa Monica, CA: RAND, 2009); Jerrold M. Post, *Prospects for Nuclear Terrorism: Psychological Motivations and Constraints*, in Leventhal and Alexander (eds.), "Preventing Nuclear Terrorism: The Report and Papers on the International Task Force on Prevention of Nuclear Terrorism" (Massachusetts; Lexington Books, 1987).

[71] Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, 1979.

[72] Weber, *Economy and Society,* 24-25.
Note that he also refers to 'traditional' types of social action. This refers to social action which is determined by ingrained habituation. Yet, as nuclear terrorism (nor something similar) has never happened, this does not seem to be relevant to our study. Moreover, Weber also refers to an affectual social action. This refers to social actions that are "determined by the actor's specific affects and feeling states." This might also be an interesting perspective to look at the potential motivation for nuclear terrorism. Yet, Weber also stated that "it may, for instance, consist in an uncontrolled reaction to some exceptional stimulus." This type of rationality seems more useful to reflect upon ad-hoc instances of social behavior. This is hard to reconcile with a nuclear terrorism project that takes several months to implement.

[73] Jacques Hymans, *The Psychology of Nuclear Proliferation: Identity, Emotions, and Foreign Policy* (Cambridge: Cambridge University Press, 2006).

rationally intended goal" and devotion to "a person as such."[74] The meaning of action is not necessarily determined by the actual achievement of the result.[75]

Second, Martha Crenshaw argued that it is also simply wrong to assume that "terrorists necessarily act in terms of a consistent rationality based on accurate representations of reality."[76] A terrorist organisation might make particular decisions despite disconfirming information. Moreover, the decisions that terrorist organisations make will not always be good ones, even from their own point of view.[77] Max Abrahms, for instance, shows that terrorists have often overrated the political effectiveness of terrorism.[78] Their decision can be influenced by a wrong strategic calculus of the leader (or a faction) of the organisation. The organisation can, for instance, make wrong assessments about how its external audience and constituency will respond to any type of tactical attack.[79] Moreover, closely related, internal group dynamics can also skew the strategic logic of a terrorist organisation. Internal loyalties or pressures might, for instance, impede members or leaders of the organisation to make correct strategic considerations. Likewise, processes such as groupthink – where critical evaluations of alternatives options of behavior are undervalued - can bias decision-making by a terrorist organisation.[80] These dynamics might interfere with instrumental rationality.

Nevertheless, in spite of the fact that different interwoven factors will influence decision-making by a terrorist organisation, there is an inherent analytical value in starting from an instrumental-rationality approach. This exploratory study aims to enable analysis rather than obfuscate it. I will, however, come back to these different factors in the empirical chapters and following analyses. Specifically, I will particularly reflect upon the plausibility of this third hypothesis by means of the two last empirical case studies of actual nonroutine terrorism operations. This will be clarified in more depth in the following chapter on the research design.

Before moving to the research design, I will however briefly recapitulate the two previous chapters that embedded this study in the existing literature on the nuclear terrorism threat. First, I have argued that an organisational approach is necessary in today's nuclear terrorism threat assessments. This claim was substantiated by the development of a nuclear terrorism scenario and a review of the literature on

[74] Weber, *Economy and Society,* 1150.
[75] Ibid.*,* 25.
[76] Martha Crenshaw, *Explaining Terrorism: Causes, Processes and Consequences* (London & New York: Routledge, 2011), 88.
[77] Jackson, "Organisational Decision-making by Terrorist Groups," 222.
[78] Abrahms, *Rules for Rebels,* 46.
[79] Jackson, "Organisational Decision-making by Terrorist Groups," 223-227.
[80] See, e.g., Crenshaw, *Explaining Terrorism,* 106 – 108.

nuclear terrorism. Moreover, cross-referencing this latter strand of literature with the literature on innovation by terrorist organisations highlighted that particular attention needs to be given to the role and impact of the organisational design. Next, I have consequently developed three hypotheses with respect to the relation between the organisational design of a terrorist organisation and the likelihood of nuclear terrorism. These expectations revolve around an effectiveness – efficiency trade-off for any terrorist organisation that considers pursuing a nuclear capacity. I expect that an organisational design similar to an organic organisational design will increase the likelihood that a terrorist organisation can effectively implement a nuclear terrorism project. Yet, I also expect that such an organic design would simultaneously imply an increasingly inefficiently functioning terrorist organisation with regards to its security position and its strategic-political goals. The following table provides an overview of these hypotheses.

Table 3.2. Overview of the hypotheses

H. 1	A terrorist organisation is most likely to effectively complete a nuclear terrorism project by means of an organisational design similar to an organic design.
H. 2	An organisational design similar to an organic design implies increased security risks to a terrorist organisation and its nuclear terrorism project.
H. 3	An organisational design more similar to an organic design implies an increasingly inefficiently functioning terrorist organisation with respect to the attainment of its political and organisational goals.

By exploring the plausibility of these hypotheses, I hope this study enables a deeper understanding of the nuclear terrorism threat. It might shed new light on the three aforementioned nuclear terrorism variables. Yet, the question remains how to study an event that has not yet happened? There is no terrorist organisation that has constructed and detonated an improvised nuclear device. This complicates any assessment of this phenomenon. The following chapter will therefore elaborate on how I have approached this problem.

4. Research design

This study starts from the following research question: "What is the role of a terrorist group's organisational design in implementing the construction and detonation of an improvised nuclear device?" It is one of the first studies on nuclear terrorism with this particular focus. This perspective is not incompatible with previous discussions on the three traditional nuclear terrorism variables.[1] In contrast, by systematically exploring this critical gap in the work on the nuclear terrorism threat, this dissertation aims to enable a deeper understanding on the likelihood of the nuclear terrorism threat. It should be clear, however, that this research question is exploratory in nature.

First, it is an initial study on some hypotheses emanating from the literature on (nuclear) terrorism and the literature on the role of the organisational design. These ideas have not been systematically developed in today's nuclear terrorism threat assessments. I therefore intend to explore the application of these theoretical propositions onto the nuclear terrorism threat; I intend to explore the plausibility of these hypotheses. The emphasis lies more at generating theory rather than verifying it.[2] This theory-building orientation seems to contradict the use of hypotheses. Yet, this is because hypothesis testing is often used in a "hard" sense. It is often associated with hypothethico-deductive explanation and prediction. In this study, however, I follow Flyvbjerg's "soft" interpretation. Although drawing on relevant literature, this dissertation ultimately revolves around exploring the plausibility of these hypotheses and testing the theoretical propositions.[3] I am more interested in expanding the theory (analytical generalisation) than enumerating frequencies (statistical generalisation).[4] This type of exploration is an essential scientific endeavour. It is the preferred approach when there is little or no scientific knowledge on the process that needs to be examined.[5] This way, this study constitutes the basis for confirmatory research at a later stage.[6]

---

[1] (1) terrorist motivations to use nuclear devices, (2) the availability of nuclear know-how and technology, and (3) clandestine organisations' opportunities to obtain fissile material

[2] See, e.g. Barney Glaser and Anselm Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research* (New Brunswick & London: AldineTransaction, 1967).

[3] Bent Flyvbjerg, "Five Misunderstandings About Case-Study Research," *Qualitative Inquiry* 12, no. 2 (2006): 227; Robert Yin, *Case Study Research: Design and Methods*, Applied Social Research Methods Series (London: SAGE Publications, 2003), 28-29.

[4] Yin, *Case Study Research,* 10.

[5] Robert Stebbins, *Exploratory Research in the Social Sciences*, Qualitative Research Methods Series 48 (London: SAGE Publications, 2001). 6.

[6] Stebbins (*Exploratory Research in the Social Sciences*, 5) notes in this context that exploration is a process that unfolds "not only within individual studies but also across several studies." When no significant new ideas arise, exploration can come to an end and confirmation can start.

Second, there are no empirical cases of a terrorist organisation successfully constructing and detonating an improvised nuclear device.[7] This implies that this study is necessarily exploratory rather than confirmatory. The lack of direct empirical evidence of this phenomenon impedes any confirmatory study. Admittedly, there are two terrorist organisations that reportedly have tried to set up a nuclear program: Al Qaeda and Aum Shinrikyo. Yet, these programs are generally not considered to have been well-developed. Thus, notwithstanding that the study of these programs might provide us with some interesting insights, it will not provide us with a good understanding of the challenges throughout the implementation of an entire nonroutine project. Moreover, more pragmatically, the reliability of the available empirical evidence on these programs is often hampered by the sensitive nature of these events.

I thus have looked for alternative ways to empirically study this phenomenon. Specifically, in order to do so, I have opted to study four cases that were facing a similar nature of technology as the *nonroutine* technology in the adopted nuclear terrorism scenario. I will extrapolate relevant insights with respect to a nuclear terrorism plot by building on this shared organisational feature (infra). The exploratory nature of drawing on such alternative empirical data is not troublesome. Rather than proving anything, the goal is to explore and learn about an underdeveloped dimension in today's nuclear terrorism threat assessments. This way, I hope to better understand the probability of the nuclear terrorism threat as the output of analysis. Hans Eysenck formulates this neatly: "sometimes we simply have to keep our eyes open and look carefully at individual cases—not in the hope of proving anything, but rather in the hope of learning something!"[8] This, however, does not imply that this study should not be conducted in a systematic manner.

4.1. Case selection

The key criterion for the selection of cases in this study is their theoretical relevance (and not their structural circumstances).[9] Each case must be theoretically appropriate to explore the plausibility

[7] One could imagine various reasons why nuclear terrorism did not yet occur. For instance, to date, terrorist organisations may have simply failed to acquire the nuclear material they seek (= availability of fissile material). Moreover, terrorist rhetoric might be just that, meant to frighten their perceived enemies and/or remain relevant (= motivation of terrorist organisation). As with all non-events, there is discussion with respect to the causal mechanism behind the non-occurrence of the phenomenon. As outlined, however, this project will particularly focus on the impact of the organisational design. This variable has not been sufficiently developed, and needs to be better explored in nuclear terrorism threat assessments. This is not to argue, however, that the organisational design is an omnipotent cause.

[8] Hans Eysenck, *Case studies in behaviour therapy,* cited in Flyvbjerg, "Five Misunderstandings About Case-Study Research," 224.

[9] Glaser and Strauss, *The Discovery of Grounded Theory,* 45-77.

of the hypotheses and test the theoretical propositions of this study. Considering case selection is an essential step in any scientific study, this section will explicitly elaborate in more depth on how I have selected cases for a theoretically relevant data collection. An overview of the exact case selection process and the criteria can be retrieved in the annex at the end of this manuscript.

First and foremost, each case must be homogenous with respect to the nature of technology in order to be theoretically relevant. The research question focuses on a better understanding of the implementation of a potential nuclear terrorism plot. As we have seen, the adopted nuclear terrorism scenario is characterised by a nonroutine nature of technology. Considering the diverse technical tasks and the organisation's clandestine operational environment, I expect the implementation of this plot to be entangled by many exceptional problems that are hard to systematically analyse in advance. The organisational design is expected to impact the effective implementation of such technology. Thus, in order to extrapolate any meaningful insights about the nuclear terrorism threat and the role of the organisational design, the selected cases must be characterised by a similar nonroutine nature of technology. Each case must be characterised by a similar high task variability and low task analysability. This enables me to build on this shared feature to extrapolate relevant lessons to the nuclear terrorism threat. Only cases with a similar nature of technology enable a better understanding of the potential implementation of a nuclear terrorism plot and the role of the organisational design. The data must apply to a similar theoretical category in order to be able to reflect upon the plausibility of the formulated hypotheses and theoretical propositions.[10] Next, case selection was also based on the availability of reliable information and two other factors (invested resources and timing) that might impact the theoretical extrapolations to a nuclear terrorism plot (see annex).

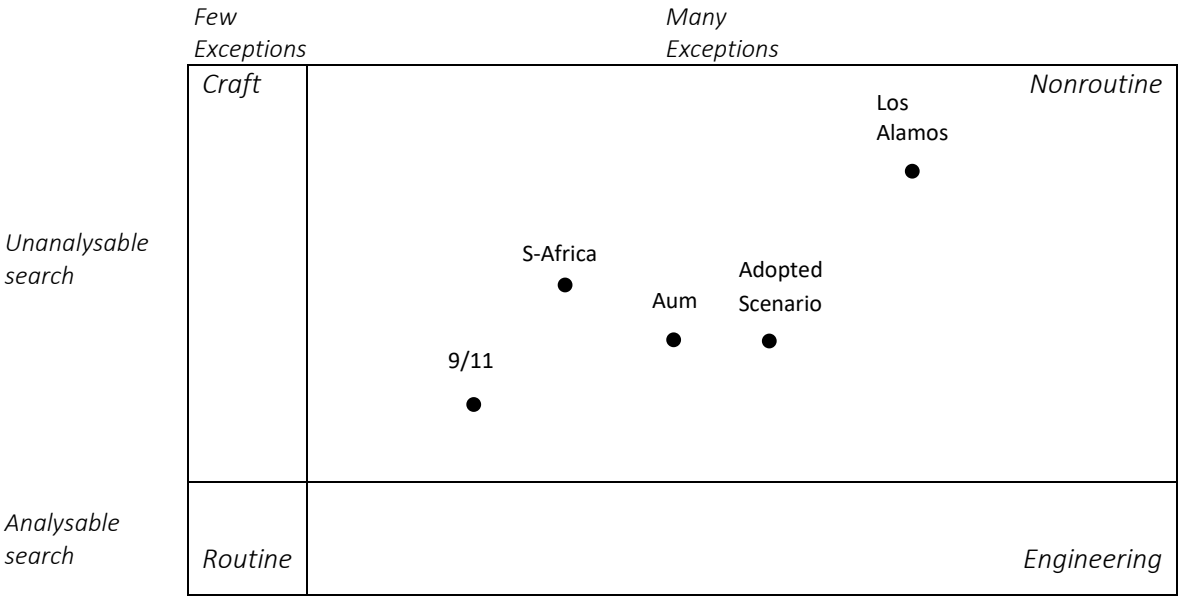
Given these selection criteria, I have selected four cases to study: (1) the construction of the first atomic bombs at Los Alamos, (2) the South African development of a nuclear device, (3) Aum Shinrikyo's chemical and biological armament activities, and (4) the implementation of 9/11 by Al Qaeda. Each of these cases is characterised by a high task variability and low task analysability. It is true that a wider variety of case studies is possible (see annex).[11] Yet, I have opted to limit the number of case studies to four. On the one hand, a limited number of cases is necessary to be able to develop an in-depth and valid understanding of each case. Such a thorough understanding of each case is necessary to reflect upon the plausibility of the hypotheses and theoretical propositions yet simultaneously remain open to

[10] Glaser and Strauss, *The Discovery of Grounded Theory,* 55.

[11] A variety of cases might be eligible to be selected as a case study (see the annex at the end of this manuscript). This could also enable an intermediate N-analysis via, e.g., QCA. Yet, considering the explorative character of this study, and the subsequent need to develop a thorough understanding of each case, I have opted to limit myself to four in-depth case studies.

the more inductive identification of new elements.[12] On the other hand, studying four cases makes it easier for the analysis to go beyond the individual cases. It enables me to extrapolate insights that are applicable across the different cases. This advances the generation of analytical generalisations.[13] The following figure 4.1 positions these cases on a two-dimensional graph with respect to the nature of technology.[14]

Figure 4.1. The nonroutine nature of the selected case studies



As becomes clear, each of these cases is characterised by a high task variability and low task analysability. The collected data for these cases will apply to a similar category. This enables comparison between these cases. Yet, it simultaneously becomes clear that there is some degree of heterogeneity. On the one hand, I have opted for a relatively robust typology with respect to the technology variable. Although this benefits this study's analytical clarity, it simultaneously implies that there is some differentiation in the nonroutine nature of each case. On the other hand, going beyond the exact theoretical categorisation, it is also true that there is some differentiation with respect to other

[12] Alexander George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (Cambridge & London: MIT Press, 2005). Note that this is essential to any explorative study. It could, for instance, be the case that my literature review did not cover every relevant aspect to this study's focus. I thus need to remain open to the more inductive identification of other relevant issues. The empirical chapters might highlight issues that are not touched upon in the relevant literature.

[13] Yin, *Case Study Research,* 47.

[14] This graphic is based on Charles Perrow's technology variable (see figure 2.7), but visually adapted in order to be more clear. It is important however to be clear in the fact that this is a means to visually represent the different cases and - what I believe - was the nature of technology that they were facing. It is based on both the clandestine operational environment and the exact operational tasks and activities. Yet, this positioning on a graph is inherently arbitrarily. It is clearly no exact science. It primarily functions as a way to structure my reasoning.

contingencies such as the resources invested in the project and its timing (see annex).[15] Yet, this is not a problem. Holding other variables constant is of primary importance in confirmatory research. In exploratory research, such differences are considered to be potentially important qualifying conditions. These differences should be made an essential part of the analysis.[16] I will therefore now elaborate in more-depth on each case, why it was selected, and what are the most important differences. More information can also be found in the empirical chapters:

1. *Los Alamos* was the first unified research and development program with respect to nuclear weapons. While most of the American development of the bomb focused on endogenously acquiring the fissile material, Los Alamos was the part of the Manhattan project that was tasked with actually designing and constructing the bomb. This first case of nuclear proliferation is an excellent example of a project characterised by a nonroutine nature of technology. On the one hand, a whole range of unexpected situations arose throughout its implementation. Some examples are the occurrence of radiation accidents,[17] technical surprises (e.g. the discovery that plutonium could not be used in a gun-type weapon),[18] or problems with the procurement of material.[19] On the other hand, there were not a lot of known ways to resolve these unexpected problems. For instance, a technical history of Los Alamos describes the project as characterised by "an empirical problem-solving methodology based on systematic trial and error rather than thorough analysis."[20] Moreover, even though that this high level of task variability and low level of task analysability was the most important selection criterion, case selection was also affected by the availability of reliable information. The implementation of this clandestine project happened more than 70 years ago. Various primary and secondary sources of data are available in English by now (infra). This enables the first explorations via this first case study to be substantiated by as much reliable empirical evidence as possible.

   Reflecting upon the differences between this case and the adopted nuclear terrorism scenario, it is obviously true that the exact operational tasks and activities of both cases are not identical

[15] Considering the available literature, the adopted nuclear terrorism scenario would take at least 6 months and it would entail the participation of at least 20 persons (but probably more). The budget for this project would circle around 10 million dollar. This assessment is, however, inherently arbitrarily. These criteria are of secondary importance. Please see the annex for more information.
[16] Glaser and Strauss, *The Discovery of Grounded Theory,* 49-52.
[17] See, e.g., David Hawkins, "Manhattan District History: Project Y, The Los Alamos Project" (Los Alamos Scientific Laboratory, December 1, 1961), 186.
[18] Lillian Hoddeson et al., *Critical Assembly: A Technical History of Los Alamos During the Oppenheimer Years, 1943-1945* (United Kingdom: Cambridge University Press, 2004), 191.
[19] Hawkins, "Manhattan District History," 51.
[20] Hoddeson et al., *Critical Assembly,* 9.

to each other. Los Alamos was, e.g., not involved in the enrichment of fissile material (i.e. an important step in the nuclear terrorism scenario). This does not, in essence, undermine the theoretical relevance of this case. Both cases share a *nonroutine* nature of technology.[21] This study builds on this organisational analogy to extrapolate lessons with respect to the nuclear terrorism threat. Yet, it does lead to a degree of heterogeneity with respect to the exact nonroutine nature of technology. Considering Los Alamos' clandestine environment and – especially – the technical challenges related to this first development of atomic weapons, it can safely be assumed that this project was characterised by a higher task variability and lower task analysability than the adopted nuclear terrorism scenario (see figure). This intense nonroutine nature of technology facilitates the exposure of organisational dynamics related to this nature of technology. This fits the purpose of this first explorative case study. Yet, it will simultaneously force me to consider this as a potentially qualifying condition during the following analyses. Not all these dynamics are necessarily applicable to a potential nuclear terrorism plot. Likewise, Los Alamos was characterised by a substantially higher amount of invested resources and a longer project time. These factors need to be taken into account when reflecting upon the theoretical implications of this case study. Note in this context that the other cases will assist me in assessing the qualifying conditions. Studying four cases enables me to extrapolate insights that go beyond the individual cases.

2. South Africa clandestinely developed nuclear explosives and weapons throughout the 70's and 80's. This second case study will primarily focus on its first development and construction of a nuclear capability: the so-called Peaceful Nuclear Explosives (PNE) program. This program was not responsible for the production of highly enriched fissile material. It only focused on the construction of South Africa's first nuclear capacity. It is an excellent example of a project with a nonroutine nature of technology. Moreover, this case is simultaneously a case more analogous to the adopted nuclear terrorism scenario with respect to both the degree of the nonroutine nature of technology and the other contingencies. This enables this study to better assess and understand the extrapolations and qualifying conditions identified in the first case study.

   The PNE program was characterised by a nonroutine nature of technology. André Buys compared it to "reinventing the atom bomb."[22] On the one hand, while arguably not to the same

[21] Remember that this study adopts a broad interpretation of "technology."
[22] André Buys, research engineer at the Reactor Engineering sub-division of the RD division, e-mail correspondence with author, June 24, 2017.

degree as during the implementation of Los Alamos, the implementation of the South African program was characterised by diverse unexpected situations. Some examples of the high task variability are the technical difficulties in some design and engineering areas (e.g. handling tungsten reflector material or obtaining the reliable seating of different components during firing),[23] the loss of top secret documents,[24] or the detection of the Vastrap test site in 1977.[25] On the other hand, some search activity was often necessary to cope with these unexpected situations. This level of task analysability was not as low as during the implementation of Los Alamos; more information on the gun-type design was already available. Yet, the work has nevertheless been described as a "learning exercise based on systematic theoretical and experimental research, technology development, prototype design and extensive test and evaluation."[26] The exact operational tasks and activities of this case and the adopted nuclear terrorism scenario are not identical. Yet, as also indicated in figure 4.1, the nonroutine nature of technology seems to be closer to one another. This benefits the analogy between this case and the adopted nuclear terrorism scenario.[27]

Likewise, although neither identical, the South African PNE program is more analogous to the adopted nuclear terrorism scenario with respect to the invested resources. The number of persons involved was, for instance, more comparable to the adopted nuclear terrorism plot (infra chapter). Thus, although the time invested in the project was substantially longer than envisaged in the adopted nuclear terrorism scenario, this case can generally be considered to be a state nuclear project more akin to the adopted nuclear terrorism scenario. Although I need to remain thoughtful about the differences between this case and the adopted nuclear terrorism scenario, this case seems therefore appropriate to reflect upon the extrapolations that followed from the first case study. To which extent were similar dynamics at play throughout the implementation of the South African nuclear project, and how does this influence my expectations with respect to the adopted nuclear terrorism scenario?

---

[23] Mark Hibbs, "South Africa's secret nuclear program: from a PNE to a deterrent', cited in Darryl Howlett and John Simpson, "Nuclearisation and Denuclearisation in South Africa," *Survival* 35, no. 3 (n.d.): 156-157.

[24] Johan Slabber, head of Reactor Engineering sub-division of the RD division, e-mail correspondence with author, August 17, 2017; André Buys, research engineer at the Reactor Engineering sub-division of the RD division, e-mail correspondence with author, April 15, 2017

[25] Hannes Steyn, Richard Van der Walt, and Jan Van Loggerenberg, *Nuclear Armament and Disarmament: South Africa's Nuclear Experience* (New York: iUniverse, Inc., 2007), 41.

[26] André Buys, June 24, 2017.

[27] Note that I expect that the impact of the clandestine operational environment would be more pressing for a terrorist organisation than it was for the South African nuclear project. I therefore expect more exceptional situations to occur for terrorist organisations implementing such a plot. Yet, I simultaneously expect a higher task analysability for a terrorist organisation, given that the technical requirements for the adopted nuclear scenario are probably less demanding.

Moreover, going beyond the theoretical relevance of this case, case selection was again influenced by the availability of reliable information. Considering that South Africa has given up on its nuclear arsenal, access to reliable information on the implementation of the PNE program became less challenging. Access to relevant and reliable information is more difficult in other small nuclear proliferation programs such as, e.g., North Korea's nuclear program. I have corresponded, for instance, with two people that were directly involved in the actual implementation of the PNE program (infra).

3. Aum Shinrikyo launched 17 terrorist plots that included chemical and biological weapons or agents between 1990 and 1995.[28] This was clearly a nonroutine program. While its 1994 attack in Matsumoto led to 7 deaths, its most lethal attack was its March 1995 Sarin attack. This led to 13 lethal casualties and the wounding of more than thousand people.[29] Going beyond the cases of state nuclear proliferation, this third case study will reflect upon whether the previous extrapolations remain plausible during the implementation of a nonroutine plot by an actual terrorist organisation. The analysis of the organisational dynamics in an actual terrorism plot might reveal qualifying conditions to the previous theoretical extrapolations. Moreover, this case study is of particular importance in assessing the plausibility of the third hypothesis. This hypothesis with respect to a terrorist organisation's strategy is best reflected upon via the study of an actual terrorist organisation.

   The most important selection criterion was the nonroutine nature of technology of Aum's CBW project. Admittedly, the exact operational tasks and activities are not identical to the adopted nuclear terrorism scenario. The challenges to weaponising different forms of WMD's cannot be lumped together. Yet, notwithstanding substantial differences, the efficient weaponisation of chemical and biological weapons in a clandestine environment can be considered to be a nonroutine project. Indeed, the implementation of the various chemical and biological armament activities by Aum Shinrikyo faced diverse unexpected situations. Some examples are the use of an harmless and nonvirulent strain of a biological agent,[30] the wind blowing in the

[28] Tim Ballard et al., "Chronology of Aum Shinrikyo's CBW Activities" (Monterey: James Martin Center for Nonproliferation Studies, August 26, 2005).
[29] Holly Fletcher, "Aum Shinrikyo", *Council on Foreign Relation.* http://www.cfr.org/japan/aum-shinrikyo/p9238#p2 (accessed October 18, 2016).
[30] Adam Dolnik, "Aum Shinrikyo's path to Innovation", in *Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators,* edited by Maria Rasmussen and Mohammed Hafez (Defense Threat Reduction Agency, 2010), 128.

wrong direction during the Matsumoto attack (thereby reducing the number of casualties),[31] or the dismantlement of Aum's Sarin production facility after precursor chemicals were detected by law enforcement authorities.[32] Notwithstanding the latter example, note that Aum generally enjoyed some level of protection against law enforcement intrusion due to its status as a religious cult. I therefore expect less exceptional situations compared to the adopted nuclear terrorism scenario. Next, there were not always known ways to resolve these unexpected problems. The efficient weaponisation of chemical and biological weapons is no straightforward exercise.[33] Moreover, a particular example related to its security environment is that the dismantlement of Aum's Sarin production facility led to the Sarin strain being used in the 1995 Tokyo attack to be weaker than intended. Their unpreparedness with respect to such an incident led them to rush the attack.[34] Thus, although I again need to remain thoughtful about the differences between this case and the adopted nuclear terrorism scenario (e.g. Aum's protected status as a religious cult), the CB armament activities by Aum provide a good case to reflect further upon the previously made extrapolations.[35] In this context, it should be noted that Aum was characterised by an organisational design with various mechanistic features. This case allows us therefore to reflect upon – what the hypotheses would suggest to be – a mismatch between the organisational design and the technology that the organisation aims to adopt. What can this teach us about the plausibility of the formulated hypotheses and theoretical propositions?

Moreover, similar to the selection of the previous cases, this case was also selected due to the availability of reliable information. Rosenau was correct in stating that some information has emerged, yet "crucial information is missing or remains hidden."[36] Nevertheless, having only access to publicly available information, this case is one of the best-documented cases of a terrorist organisation implementing a WMD program. Rosenau indeed further elucidates that "it is possible to use unclassified information to hypothesize some informed, albeit tentative,

[31] Nadine Gurr and Benjamin Cole, *The New Face of Terrorism: Threats from Weapons of Mass Destruction* (London & New York: I.B. Tauris, 2000). 64.
[32] Gavin Cameron, "Multi-Track Microproliferation: Lessons from Aum Shinrikyo and Al Qaida," *Studies in Conflict & Terrorism* 22, no. 4 (1999), 294; Anthony Tu, "What Were the Real Objectives of Aum Shinrikyo?" *CBRNE terrorism newsletter* 41, (2012): 6.
[33] Gurr & Cole (68), situate this threat, for instance, in the same category of threat as the use of a nuclear device by a terrorist organisation (namely the "least common threats").
[34] Cameron, "Multi-Track Microproliferation," 294; Parachini and Furukawa, "Japan and Aum Shinrikyo", 543. Tu, "What Were the Real Objectives of Aum Shinrikyo," 6.
[35] Note in this context that other contingencies (e.g. invested resources, timing) come close to the adopted nuclear terrorism scenario (see annex). This strengthens the analogy between both cases.
[36] William Rosenau, "Aum Shinrikyo's Biological Weapons Program: Why Did It Fail?," *Studies in Conflict & Terrorism* 24, no. 4 (2001) 293.

judgements about why the cult did not achieve its objectives."[37] This is in line with the explorative purposes of this particular study.

4. The 9/11 plot refers to the implementation of four coordinated terrorist attacks against the United States of America by Al Qaeda. Similar to the previous case study, this case study enables me to reflect upon the applicability of the previous theoretical extrapolations throughout the implementation of an actual nonroutine terrorism plot. It is also of particular relevance in assessing the plausibility of the third hypothesis. Yet, more importantly, this case study simultaneously functions according to the logic of a least-likely case. The nonroutine nature of technology was less outspoken than the adopted nuclear terrorism scenario. Likewise, the invested human and material resources are considered lower compared to those that would be invested in the adopted nuclear terrorism scenario. This implies that the extrapolations with respect to the formulated hypotheses and theoretical propositions about the adopted nuclear terrorism scenario become more plausible in case similar dynamics can be identified throughout the implementation of 9/11.

   The implementation of 9/11 did not entail the manufacturing of a complex weapon. The aircrafts itself were used as a weapon. Moreover, the implementation of this plot occurred before the so-called Global War on Terror. Various security layers were seriously flawed.[38] Yet, the implementation of 9/11 can nevertheless be characterised by a nonroutine nature of technology. Besides determining the tactics to successfully hijack the planes, which included the use of multiple case runs to revise and improve the operational plan,[39] this plot also required Al Qaeda to have people with specialised skills and training to successfully fly these multi-engine aircrafts into the selected targets. Moreover, this plot required an uncommon level of patience and detailed planning in a clandestine operational environment. Multiple and diverse tasks needed to be attuned to each other throughout the implementation of this plot (e.g. communication to enable the planning and guidance of the operatives; recruit, vet, indoctrinate and train the pilots and muscle hijackers; understand the security strengths and weaknesses of the target; move the operatives; and raise and transfer the necessary money).[40] Terrorist organisations have not often succeeded in this type of coordinated attacks with multiple targets.

[37] Rosenau, "Aum Shinrikyo's Biological Weapons Program," 293.
[38] National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, 1st ed. (New York: Norton, 2004), 83. (hereafter cited as the 9/11 Commission Report).
[39] This enabled the hijackers, e.g., to determine which seat was best suited to quickly overrun the cockpit once the passenger belt sign was switched off.
[40] The 9/11 Commission Report, 172-173.

It went beyond Al Qaeda's standard operations. Bruce Hoffman stated in this context that this is "less of a choice than a reflection of the logistical and other organisational hurdles and constraints."[41]

Not surprisingly, notwithstanding the lower level of technical sophistication and the counterterrorism flaws, the implementation of this plot faced a number of exceptional situations. This is illustrated by, e.g., the fact that two of the originally selected suicide operatives proved to be ill-prepared for a mission in the United States. They had no aptitude for English and could consequently not learn how to fly.[42] Likewise, Ramzi Binalshibh – whom was originally envisaged as the fourth pilot - did not acquire a U.S. visa. He was suspected to be an undocumented alien seeking work.[43] Next, it turned out that it was not always clear for Al Qaeda on how to cope with these unexpected situations. The leadership, for instance, originally hoped to have 25 or 26 operatives during the plot. Yet, they ultimately ended up with 19 operatives.[44] Moghadam refers in this context of the final 9/11 plot as the end point of a trial-and-error process since 1993, when Ramzi Youssef bombed the WTC.[45] The implementation of 9/11 can thus be considered to be a nonroutine terrorism plot.

Moreover, going beyond the theoretical relevance of this case, there are a high number of reliable sources on the actual implementation of this plot (infra). This unique terrorism attack received a lot of governmental and scholarly attention. Taking into account this availability of relevant and reliable sources, and the logic of a least-likely case study, this final case study is thus considered to be appropriate as a final case study to critically reflect upon the plausibility of the formulated hypotheses on the probability of nuclear terrorism and the role of the organisational design.

Each of these cases is homogenous with regards to its nonroutine characterisation. Yet, the exact degree of the nonroutine nature of technology and the other contingencies are simultaneously to some extent heterogeneous. This is a function of, for instance, the exact operational tasks and activities that need to

[41] Bruce Hoffman, "Lessons of 9/11",Testimony submitted for the Committee Record to the United States Joint September 11, 2001 Inquiry Staff of the House and Senate Select Committees on Intelligence on October 8, 2002 (2002): 8-9.
[42] The 9/11 Commission Report, 215-223
[43] "Staff Statement No.1: Entry of the 9/11 Hijackers into the United States" (National Commission on Terrorist Attacks Upon the United States, n.d.).
This staff statement mentions that at least 4 individuals implicated in the 9/11 failed in obtaining visas.
[44] The 9/11 Commission Report, 235; Terry McDermott, *Perfect Soldiers: The 9/11 Hijackers: Who They Were, Why They Did It* (e-book: Harper Collins e-books, 2008), 229.
[45] Assaf Moghadam, "How Al Qaeda Innovates," *Security Studies* 22, no. 3 (2013): 486.

be carried out. This is, however, not considered troublesome. Each case can be considered to be a piece of the puzzle in this explorative study. Together, these cases enable us to explore the potential implementation of a nuclear terrorism plot and the role of the organisational design. This way, this study addresses a critical gap in the nuclear terrorism literature. It aims to improve our understanding of the probability of nuclear terrorism as the "output of analysis." It goes beyond examining the individual tasks and activities in a potential nuclear terrorism plot (such as reflecting upon the probability that a terrorist organisation might acquire fissile material), yet is not incompatible with this approach. In contrast, my approach might result in particular insights applicable to such individual steps. This way, this study ultimately hope to enable a better understanding of the nuclear terrorism threat. It is the first time that this type of systematic comparison is being done in the nuclear terrorism literature.

4.2. Data collection and analysis

The emphasis of this study is more on generating theory rather than verifying it. It is about assessing the plausibility of the formulated hypotheses and theoretical propositions; not about providing a hard test for these hypotheses. In contrast to confirmatory and verifying research, this implies that it is not troublesome if some of the empirical evidence is not entirely accurate. Although we naturally want to be as sure as possible about evidence, explorative research is not about the facts upon which we stand, but about the theoretical abstractions that were generated from it. This also implies that falsification should not be considered a function of individual empirical observations. In contrast, the theoretical abstractions remain valid until proven theoretically refuted (by, e.g. extra case studies).[46]

It thus follows that we do not compare evidence for its own sake. A variety of sources might be relevant. While this might be bewildering if we wanted to evaluate the data as accurate evidence for verification, this variety of data can yield more insightful information on the theoretically relevant categories in this type of explorative research. The result is not unbounding relativism. Instead, biases in particular sources tend to reconcile themselves as the analyses proceed.[47] Moreover, it enables us to get a thorough understanding of each individual case and the cross-case implications. This way, I have aimed to prevent a bias towards preconceived notions. Table 4.1. provides a schematic overview of the primary and secondary sources that I have used.

[46] Glaser and Strauss, *The Discovery of Grounded Theory,* 23-24.
[47] Ibid.*,* 66-69.

The specific data collection was controlled and guided by the adopted organisational perspective and the individual cases being studied.[48] Different kind of sources were potentially relevant (e.g. expert interviews, seminal literature, interviews with participants in the respective cases, etc.). Taken this into account – and also considering the delicate and often classified nature of the information – I have collected my data up to the point of saturation via the snow-ball method. I have scanned a great deal of potentially relevant references to primary or secondary literature, experts, or participants in any of the suggested cases. Each potential data source was screened to check its relevance with respect to the research question (e.g. considering Alamos, there were various testimonies available of participants in the project that were overly technically oriented. I did not read these in-depth).[49]

Table 4.1. Overview of data sources

Nuclear terrorism scenario	• Seminal literature on the topic (see references in the chapter) • Semi-structured and open-ended round-table conversation with: Tom Bielefeld (independent consultant; physicist and specialist on nuclear security, non-proliferation and terrorism) Gilbert Eggermont (retired physicist; specialist on nuclear safety and security) Roland Carchon (retired physicist; specialist on nuclear safety) • Semi-structured and open-ended interview with: Tom Bielefeld Roland Carchon Zia Mian (Princeton University; physicist specialised in nuclear weapons and nuclear energy policy) Moritz Kutt (Princeton University; physicist, specialised in nuclear warhead verification technologies) Frank Von Hippel (Princeton University; physicist, specialised in nuclear weapons) Alexander Glaser (Princeton University; physicist, specialised in nuclear energy and nuclear-weapon proliferation • (indirect or brief) email correspondence with particular questions for: a respondent working in a nuclear weapons laboratory, Alex Wellerstein (historian of science, specialised in nuclear weapons history)
Los Alamos	• Seminal literature on the topic (see references in the chapter) • Firsthand accounts by scientists and participants that were actively involved in Los Alamos (available via Badash et al. *Reminiscences of Los Alamos, 1943-1945*.) *John Dudley* (a graduate of West Point, Massachusetts Institute of Technology, and the Army War College, served in the Engineer Corps. In 1942-1943 he played a key role in selecting a site for the secret weapons laboratory and was responsible for the initial construction there) *Edwin McMillan* (physicist; worked at nuclear weapons at Los Alamos) *John Manley* (physicist; in 1942 and 1943 he was attached to the Manhattan Project's Metallurgical Laboratory in Chicago; from 1943 he was at Los Alamos, principally as Oppenheimer's aide in creating the new laboratory) *Elsie McMillan* (wife of Edwin McMillan) *George Kistiakowsky* (chemist; he was chief of the Explosives Division at Los Alamos,) *Joseph Hirschfelder* (physicist; he was a group leader in both the Ordnance and the Theoretical Divisions at Los Alamos)

[48] Glaser and Strauss, *The Discovery of Grounded Theory,* 45.

[49] Electronically available data was stored in Nvivo (infra). Interview transcripts (not 100% ad verbatim, as this is not necessary for theoretical abstractions) were also stored electronically. Literature that was not electronically available (e.g. books) was stored in my office.

	Laura Fermi (wife of Enrico Fermi, physicist at Los Alamos and creator of the world first's nuclear reactor) *Richard Feynman* (theoretical physicist at Los Alamos between 1942 and 1945) *Bernice Brode* (worked as a computer at Los Alamos between 1943-1945) *Norris Bradbury* (physicist: during the final year of the war, he was in charge of the implosion field-test program at Los Alamos and responsible for the assembly of all non-nuclear components of the plutonium bomb) • Interviews with people involved in Los Alamos via 'voices of the Manhattan Project.' *Robert Oppenheimer* (scientific director Los Alamos) *Hans Bethe* (physicist; head of the theoretical division at Los Alamos) *Robert Serber* (physicist; explained the basic principles and goals of the project to all incoming scientific staff) *Harry Allen and Robert Van Gremert* (worked in procurement at Los Alamos) *Norris Bradbury* (supra) • Autobiographical books: Leslie Groves, *Now It Can Be Told: The Story of the Manhattan Project* (director of the Manhattan Project) Luis Alvarez, *Adventures of a Physicist* (physicist; responsible for conduction implosion tests) • A first draft of this chapter has been read and briefly reviewed by, e.g., Charles Ferguson (at that time director of the Federation of American scientists), Siegfried Hecker (FSI-CISAC), and anonymous reviewers of 'Terrorism & Political Violence.'
South Africa's nuclear devices	• Seminal literature on the topic (see references in the chapter) • Semi-structured and open-ended written correspondence with people directly involved in the PNE program: *Andre Buys* (Reactor Engineering sub-division of the RD division) *Johan Slabber* (Reactor Engineering sub-division of the RD division) • (Brief) semi-structured and open-ended personal written correspondence with people closely involved in the broad South African nuclear endeavour. *Waldo Stumpf* (chief executive officer of the AEC) *Nic Von Wielligh* (Uranium Enrichment Corporation; led the South African team interfacing with the IAEA during SA's declaration of its past program) • Literature by people directly involved in the broad nuclear program *Steyn* (physicist and general manager of Research and Development at Armscor), *Van der Walt* (physicist, and general manager of the AEC) and *Van Loggerenberg* (pilot; chief of the South African Air Force); *Waldo Stumpf* (supra) *Nic Von Wielligh* (supra) • Open-ended expert interviews (both experts on South Africa's nuclear history): *Anne-Mart Van Wyk* (adjunct professor Monash South Africa) *Peter Liberman* (associate professor Queens college, city university of New York) • A first draft of this chapter draft has been read and reviewed by Nic Von Wielligh (supra), and anonymous reviewers of 'Dynamics of Asymmetric Conflict'
Aum Shinrikyo CB armament activities	• Seminal literature on the topic (see references in the chapter) • Online available interview with Tomomasa Nakagawa, a member of Aum's biological armament activities • Literature based on primary resources Richard Danzig et al., "Aum Shinrikyo Insights Into How Terrorists Develop Biological and Chemical Weapons (chairman CNAS) • Semi-structured and open-ended expert interviews with *Jean Pascal Zanders* (independent consultant 'the Trench'; specialises in questions of armament and disarmament, covering chemical, biological, radiological and nuclear weapons *Marc Sageman* (former CIA officer; senior Fellow in the Foreign Policy Research Institute's Center for the Study of Terrorism) *Sonia-Ben Ouagrham-Gormley* (Associate Professor in the Schar School of Policy and Government at George Mason University) *Daniel Smith* (Senior Faculty Specialist, START)

	• A first draft of this chapter has been read and briefly reviewed by Marc Sageman and Daniel Smith, and anonymous reviewers of 'Terrorism & Political Violence.'
9/11	• Seminal literature on the topic (see references in the chapter) • Excerpts of interviews (available via Fouda & Fielding, "masterminds of terror") with people directly involved in the 9/11 plot: Khalid Sheikh Mohammed Ramzi Binalshibh • The 9/11 commission report and its individual staff statements • The Joint inquiry conducted by the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence

In order to analyse this variety of data, I have first dedicated my time to mapping each individual case. This was a necessary precondition to gain a good understanding on the implementation of these plots. Next, I have thematically identified key-issues at play in the respective case studies. While this research project is explorative in nature, I have aimed to strengthen its reliability and validity by developing a set of questions as my heuristic approach. These questions were drawn up based on the literature review in chapter two. Considering this explorative study's focus on the role of the organisational design – which is underdeveloped in today's nuclear terrorism threat assessments – these questions ultimately revolve around the issue of control and coordination. Particular focus is given to the three essential organisational design parameters: the interconnectedness of the group, the level of hierarchical control, and the degree of specialisation. Yet, I obviously remained aware of potential new elements arising from the data:

1. Which type of skills and expertise were required to effectively implement the project?
2. How many resources were invested in the implementation of the project?
3. Were members of the project well-trained?
4. Were member of the project indoctrinated by the goals of the organisation?
5. Were there various subunits, and how were these subunits organised throughout the implementation of the project?
6. How did the organisation set up the planning of the implementation of the project?
7. How was information-sharing organised throughout the implementation of project?
8. To which extent could scientists and technicians make autonomous operational decisions ?
9. Were there any security breaches throughout the project's implementation? Why did these occur?

Guided by these questions, I have identified key organisational themes at play throughout the implementation of each of these four cases. Next, assisted by Nvivo (in case data could be electronically stored), I have examined the data relevant to each theme to reflect upon its incidence, variance and impact. I have adopted a positivistic stance in doing so. This way, I was able to systematically explore the role of the organisational design in implementing each of these nonroutine projects. As mentioned earlier, these insights function as the basis for my extrapolations with respect to the role of a terrorist group's organisational design in implementing the construction and detonation of an improvised nuclear.

Finally, a cross-case analysis brings together all the previous explorative insights and extrapolations. There is some degree of heterogeneity with respect to these cases. Yet, this is not a problem. These differences might entail important qualifying conditions and should therefore be an essential part of the final analysis. By assessing and comparing the similarities and differences via this cross-case analysis, I hope this study contributes to a better understanding of the nuclear terrorism threat as the output of analysis.

4.3. Data reporting

Each individual case study will constitute a separate chapter. These individual chapters will follow the same theory-generating narrative; after elaborating on the relevance of the particular case, I will reflect upon four key organisational dimensions – and corresponding challenges - to the implementation of these nonroutine projects. These dimensions are: the resource support, the level of autonomy, the level of information-sharing, and clear and compelling goals. Each of these dimensions was to at least some degree relevant during the implementation of each of these nonroutine cases.[50]

[50] The observant reader will note that three of these four dimensions are identified by Jacques Hymans, *Achieving nuclear ambitions: scientists, politicians, and proliferation* (United States: Cambridge University Press, 2012). Notwithstanding the theory-generating purpose of my study, I am ineluctably guided by the available literature and theory on this topic. Where appropriate, I thus rehabilitate existing ideas. Given Hymans' focus on state nuclear proliferation, it comes as no surprise that these ideas are also to some extent relevant to this study. To my knowledge, Malfrid Braut-Hegghammer, *Unclear Physics: Why Iraq and Libya Failed to Build Nuclear Weapons* (Ithaca and London: Cornell University Press, 2016) is one of the few authors that explicitly proclaims to challenge Hymans' findings. Yet, as Hymans convincingly argues, there seems to be a general congruence between both perspectives. (J. Hymans, "review on unclear physics: why Iraq and Libya failed to get the bomb" *ISSF roundtable 9-22*. https://networks.h-net.org/node/28443/discussions/189010/issf-roundtable-9-22-unclear-physics-why-iraq-and-libya-failed-get#_Toc489128157 (accessed November 9, 2018.) I thus believe Hymans' work to be an excellent starting point for my study. Yet, this does not undermine the contribution of this study. Indeed, while Hymans to my knowledge did not study Los Alamos or South Africa, he neither reflected upon the applicability and utility of these ideas to the development of a nuclear capacity by a terrorist organisation. Yet, this particular approach led me, for instance, to explicitly include 'information-sharing' as an essential organisational dimension.

They are instrumental to a better understanding of the issue of control and coordination. I will include exemplifying quotes in these sections to demonstrate my observations. Next, I will turn from description to exploration. Each chapter will specifically elaborate on the role of the organisational design. As mentioned earlier, the organisational design is expected to influence the adoption of a particular nature of technology. The organisational design is the common thread that shapes the four aforementioned organisational dimensions – and corresponding challenges – to the implementation of these nonroutine projects. Finally, each chapter will end by extrapolating insights with respect to the formulated hypotheses on the probability of nuclear terrorism.

This iterative structure functions to facilitate the development of the cross-case analysis in chapter nine. It benefits the comparison of similarities and differences between the different cases. Each case forms a piece of the puzzle. Each of these cases is homogenous with regards to its nonroutine characterisation. Yet, the exact degree of the nonroutine nature of technology and the other contingencies are to some extent heterogeneous. This might imply important qualifying conditions. Both these similarities and differences need to be an essential part of my analysis. Moreover, this ninth chapter will also reflect upon other potential nuclear terrorism scenarios. As previously outlined, the adopted nuclear terrorism scenario merely provides a framework for reasoning on this phenomenon. This implies that the insights that follow from this study are not necessarily applicable to all nuclear terrorism scenarios. This study consequently also reflects upon some other scenarios, and how my insights might or might not apply to these scenarios. This way, I ultimately aim to shed new light on today's nuclear terrorism debates and enable a deeper understanding of the nuclear terrorism threat.

Moreover, as will become clear, this particular approach also led me to reflect upon the effectiveness- efficiency trade-off in such a plot. These issues are – to my knowledge – not elaborated on by Hymans or others.

5. Case study: constructing the first nuclear bombs at Los Alamos

The first case study that I have selected to explore the plausibility of the hypotheses is the design and construction of the first nuclear bombs in the 1940s.[1] The development of these first nuclear weapons took place at the Los Alamos National Laboratory in the United States. This project – which was also nick-named Project Y - resulted in the first detonation of an implosion-type nuclear device at the 16th of July 1945 (= Trinity Test), the 6th of August 1945 explosion of a gun-type nuclear device over Hiroshima, and the 9th of August 1945 detonation of an implosion-type nuclear device over Nagasaki.[2]

While the structure of atoms was widely studied throughout the 1930s, scientists only discovered the process of nuclear fission by the end of 1938. As this news broke through, many scientists immediately recognised the potential danger of atomic energy. On August 2, 1939, Albert Einstein – with the help of Leo Szilard – wrote a letter to the American President Roosevelt. He informed him "that the element uranium may be turned into a new and important source of energy in the immediate future." He then added that "it may become possible to set up a nuclear chain reaction in a large mass of uranium, by which vast amounts of power and large quantities of new radium-like elements would be generated (…) this new phenomenon would also lead to the construction of bombs, and it is conceivable – though much less certain – that extremely powerful bombs of a new type thus maybe constructed." Einstein believed that Germany was already exploring this option. He consequently requested the American government to speed up their nuclear efforts.[3] Originating from this letter, the United States of America incrementally established a project that would result in the only successful atomic bomb effort during the second World War. More specifically, after numerous reports on the possibility of an atomic bomb – including e.g. the influential British MAUD report – and a series of military defeats in the Pacific (e.g. Pearl Harbour), Washington tentatively decided to proceed with the construction of the atomic bomb by early 1942.[4] This project became known as the Manhattan Project.

A major part of this Manhattan project was directed at the endogenous production of enriched fissile material. The nonroutine nature of this endeavour implies theoretical relevance to this study's focus.

---

[1] Large sections of this chapter are published in: B. Volders, "Nuclear Terrorism: What can we Learn from Los Alamos," *Terrorism & Political Violence,* 2017.

[2] The yield of these devices was somewhere in the range between 10 and 25 kT.

[3] Albert Einstein, 'Letter to Roosevelt', Available at: https://www.osti.gov/opennet/manhattan-project-history/Resources/einstein_letter_photograph.htm#1 (accessed September 1, 2016).

[4] For more details, please have a look at the Department of Energy's website on the Manhattan project. Available at: https://www.osti.gov/opennet/manhattan-project-history/Events/1942/1942.htm (accessed September 1, 2016).

The Manhattan project as a whole would thus be an appropriate case study for this research project. Yet, I have opted to focus this case study particularly on the work at the Los Alamos National Laboratory. This part of the Manhattan Project was tasked with the actual design and construction of the atomic bomb. While research on this theme was first spread over various universities, the government decided by the end of 1942 to establish a unified bomb research and development program. This isolated laboratory was erected at the Los Alamos boys ranch school in the remote mountains of northern New Mexico. As the scientific director of this project - Robert Oppenheimer - stated, work at Los Alamos focused on "work on the bomb itself."[5] Compared to the Manhattan project as a whole, this project was smaller in size and technically less demanding. This makes this project a bit more similar to the adopted nuclear terrorism scenario (infra).

In what follows, this chapter will adopt a theory-generating narrative. After elaborating on the relevance of this particular case, I will reflect upon four key organisational dimensions – and the corresponding challenges - to the implementation of Los Alamos. These dimensions are: the resource support, the level of autonomy, the level of information-sharing, and clear and compelling goals. Next, turning from description to exploration, I will elaborate on the role and impact of the organisational design. This is the common thread that permeates these organisational dimensions and challenges. Finally, I will build on these findings to extrapolate relevant insights about the formulated hypotheses and theoretical propositions with regards to the probability of nuclear terrorism.

5.1. The relevance of Los Alamos

The main selection criterion for this case was its theoretical relevance. Los Alamos was characterised by a *nonroutine* nature of technology. This is similar to the adopted nuclear terrorism scenario. Considering the combination of various technical challenges and the project's clandestine operational environment, Los Alamos had to cope with a high task variability and low task analysability. This shared organisational feature between Los Alamos and the adopted nuclear terrorism scenario is the basis for my extrapolations with respect to the nuclear terrorism threat:

Robert Wilson – a physicist at Los Alamos – illustratively notes the nonroutine nature of technology by stating that: "we were constantly plagued by worry about some unpredicted or overlooked mechanism

[5] Robert Oppenheimer cited in United States Atomic Energy Commission 1954, *In the Matter of J. Robert Oppenheimer* (Cambridge: MIT Press, 1971), 12.

of nuclear physics which might render our program unsound."[6] One particular example is the occurrence of a small measurement error – which was well within the limits of error according to Oppenheimer – that implied an increase by 40% in the fissile material required.[7] Other examples are some radiation incidents, or the unexpected technical surprise that plutonium could not be used in a gun-type weapon. These type of unexpected problems were often a consequence of the fact that the diverse divisions that worked on this issue – e.g. the chemistry and metallurgy division, the ordnance division, the theoretical division and the experimental physics division – faced a variety of new tasks that needed to be completed and attuned to each other. The nature of the search procedure to deal with these unexpected problems has been described as "an empirical problem-solving methodology based on systematic trial and error rather than thorough analysis."[8] Moreover, these unexpected problems could also result from – or be exacerbated by – the clandestine nature of the project. Los Alamos was a top-secret atomic weapons laboratory. The geographical isolation of the town is indicative of this project's secret character.[9] Yet, security concerns often complicated the implementation of the project. For instance, the unfamiliarity with the work being done at the laboratory by the procurement offices often led to mistakes in the procurement of material.[10] Thus, to synthesize, Los Alamos was characterised by a nonroutine nature of technology.

It is clear, however, that the implementation of the adopted nuclear terrorism scenario – and the exact problems that would arise - would not be identical to the implementation of Los Alamos. Los Alamos was characterised by the implementation of breakthrough technology. This was technically more challenging than the adopted nuclear terrorism scenario and implied the investment of more time and resources. Moreover, Los Alamos only focused on the development and construction of a nuclear device. The adopted nuclear terrorism scenario, in contrast, also entails other steps (e.g. the acquisition of fissile material). These differences in the exact tasks and activities inherently lead to a degree of heterogeneity with regards to the exact nonroutine nature of technology. To be precise, taking into account its clandestine environment and, particularly, the challenges to the implementation of breakthrough technology, it can safely be assumed that the nonroutine nature of technology at Los Alamos was more intense than it would be in the adopted nuclear terrorism scenario. Los Alamos was

[6] Robert Wilson, "Nuclear Physics," cited in Lillian Hoddeson et al., *Critical Assembly: A Technical History of Los Alamos During the Oppenheimer Years, 1943-1945* (United Kingdom: Cambridge University Press, 2004), 191.
[7] Hoddeson et al., *Critical Assembly,* 191.
[8] Ibid., 9-10.
[9] Leslie Groves, *Now It Can Be Told: The Story of the Manhattan Project*, 2nd ed. (United States of America: Da Capo Press, 1983), 66-67.
[10] David Hawkins, "Manhattan District History: Project Y, The Los Alamos Project" (USA: Los Alamos Scientific Laboratory, 1961), 56.

characterised by a higher task variability and lower task analysability than that expected in the adopted nuclear terrorism scenario (see figure 4.1).

These differences will need to be integrated in the analyses that follows. They might potentially become important qualifying conditions. Yet, considering this is the first case in this exploratory study, its intense nonroutine nature of technology can simultaneously be considered to be an advantage. Organisational dynamics related to the nonroutine nature of technology might manifest themselves more clearly. Not every dynamic necessarily applies to the adopted nuclear terrorism scenario. Yet, such an intense nonroutine nature of technology does provide us with a broad starting point for this study's explorative focus. Moreover, case selection was also based on the fact that there is a lot of reliable information available on the actual implementation of Los Alamos (for an overview, please see table 4.1). This strengthens the explorations that follow from this first case study. Further refinements and nuances will remain necessary. Yet, the other three cases will assist me in doing so. Indeed, studying four cases enables me to extrapolate insights that go beyond the individual cases.

5.2. Organisational challenges

This section aims to describe the main organisational challenges at Los Alamos. To be precise, I will elaborate on four key organisational dimensions – and the corresponding challenges - to the implementation of this nonroutine project. These dimensions are: the resource support, the level of autonomy, the level of information-sharing, and clear and compelling goals. Each of these dimensions was at least to some extent relevant during the implementation of each of the selected cases. As will be illustrated, the organisational design is the common thread that permeates these organisational dimensions.

5.2.1. Resource support

Both human and material resources were – notwithstanding some challenges - successfully acquired, allocated and employed throughout the implementation of Los Alamos. People with both the necessary techne and metis were of vital importance to the effective implementation of Los Alamos. These individuals succeeded in completing this technically complex project while operating in a clandestine operational environment. Moreover, adequate material resource support benefitted the

functioning of these well-skilled people. It accommodated their improved functioning by enabling them to dedicate themselves to their vocation.[11]

Los Alamos was generally characterised by the successful recruitment and employment of some of the brightest minds at that time (e.g. John Manley, Robert Serber, Hans Bethe, Enrico Fermi, Emilio Sègre, Seth Neddermeyer, George Kistiakowsky, et al.). Yet, there were some challenges to the availability and motivation of these people. Recruitment began in the fall of 1942. Originally, no one involved in another war time effort (such as the development of advanced radar technology) could be approached. Strict adherence to this policy was nearly impossible. It was thus relaxed when it could be demonstrated that this person would be essential to Los Alamos.[12] Moreover, the secret nature of the project continuously entailed the "problem of how much one could say."[13] Not everybody did join the project. Participation entailed various personal and professional sacrifices. Potential participants needed to be convinced to move to an isolated, well-secured area, and would be cut off from the rest of the scientific world.[14] Oppenheimer recalled in this context that: "the notion of disappearing into the desert for an indeterminate period and under quasi-military auspices disturbed a good many scientists and the families of many more."[15] Leadership consequently wanted to avoid that people that decided not to participate in the project would know too much about it.

Yet, notwithstanding these challenges, an adequate number of specialised individuals with both the necessary techne and metis were recruited and employed throughout the implementation of this plot. Considering the project's secret nature, it comes as no surprise that the nucleus of the organisation came from several groups working for or with Oppenheimer.[16] Approaching people from your own network might alleviate security considerations. Oppenheimer recruited these very first men (e.g. Manley, Bethe, Serber,…) by travelling from university to university that worked on the topic of nuclear fission.[17] Scientific interest in the innovative nature of the job and the acknowledgement of its importance are often mentioned as grounds for successful recruitment efforts (infra: clear and

[11] Jacques Hymans' work primarily focuses on the management of state nuclear projects. While I believe he implicitly acknowledges (or implicitly assumes) the importance of well-skilled individuals, his focus leads him to primarily focus on the material resource support (Jacques Hymans, *Achieving Nuclear Ambitions: Scientists, Politicians, and Proliferation* (United States: Cambridge University Press, 2012).
[12] Hoddeson et al, 58-59.
[13] Stephane Groueff, *Interview with J. Robert Oppenheimer* (1965). Available at: https://www.manhattanprojectvoices.org/oral-histories/j-robert-oppenheimers-interview (accessed April 12, 2019).
[14] Groves, *Now It Can Be Told*, 150.
[15] J. Robert Oppenheimer cited in Los Alamos Scientific Laboratory Public Relations, "Los Alamos: Beginning of an Era 1943-1945: Part 2" (USA: Los Alamos Scientific Laboratory, 2008).
[16] Groves, *Now It Can Be Told,* 149.
[17] Groueff, *Interview with J. Robert Oppenheimer*.

compelling goals). Although this project was originally conceived as a small community of research scientists,[18] the "total laboratory personnel increased steadily from 250 in July, 1943, to 2,500 in July, 1945."[19] The project moreover enjoyed outside help (e.g. the British mission and consultants of different universities). Together, these individuals were the driving force behind effective progress at Los Alamos. Physicists, chemists, and metallurgists were "expected to gather new information at the limits of understanding."[20] For example, metallurgists knew little about the element plutonium. They reasonably, but incorrectly, assumed that plutonium would metallurgically be similar to uranium. This hindered the production of plutonium metal, until they – via a variety of overlapping plutonium production schemes - found that plutonium has a lower melting point than uranium.[21] By adopting a 'trial-and-error' methodology, these people succeeded in surmounting various of the nonroutine situations that occurred throughout the implementation of this project.[22] One particular advantage of an adequate number of specialised human resources was that these people could be flexibly deployed. Luis Alvarez stated:

> Los Alamos was fortunate to have a full complement of high-caliber nuclear physicists. Because it did, a physicist of Emilio's (Sègre) skills could be diverted from apparently more essential tasks to measure the rates of spontaneous fission in samples of uranium and plutonium, constants we thought we already knew. His discovery of the high spontaneous-fission background of reactor-bred plutonium was the most important single event at Los Alamos in the first months after I arrived. It had fateful consequences for bomb design and for the work of Kistiakowski's X-division.[23]

The effective functioning of these well-skilled people was facilitated by satisfactory material resource support. First, federal funding and a competent and flexible procurement office allowed for the satisfactory flow of non-nuclear components and fissile material.[24] This enabled the minimisation -

[18] Hawkins, "Manhattan District History," 39.
[19] Los Alamos Scientific Laboratory Public Relations, "Los Alamos: Beginning of an Era 1943-1945: Part 3" (USA: Los Alamos Scientific Laboratory, 2008), 23. This number includes a broad range of people involved in Los Alamos. It includes, e.g., administrative services, scientists, and technicians.
[20] Hoddeson et al., *Critical Assembly: A Technical History of Los Alamos During the Oppenheimer Years, 1943-1945*., "*Critical Assembly,"* 409.
[21] Ibid., 409.
[22] Ibid., 9.
[23] Luis Alvarez, *Adventures of a Physicist*, Alfred P. Sloan Foundation Series (New York: Basic Books inc. Publishers, 1987), 126.
[24] The United States did not need to fight a war on the home front. This probably benefitted its commitment of resources towards the nuclear weapons program. Hoddeson, for instance, notes that the political leadership did ensure "essentially unlimited funding and material support" to projects in line with the mission. Hoddeson et al., *Critical Assembly: A Technical History of Los Alamos During the Oppenheimer Years, 1943-1945*., "*Critical Assembly,"* 6; Hawkins, "Manhattan District History."

though not the complete elimination - of human frustrations, operational delays, and engineering errors. Considering the procurement of materials, scientists and technicians at the laboratory were not allowed to have direct contact with manufacturers and dealers due to security considerations. In case of questions about the design or fabrication, "these questions had to be transmitted through the New York or Chicago Purchasing Office to the Los Angeles Purchasing office, from there to the Los Alamos Procurement Office, and finally to the using groups."[25] This sometimes resulted in delays, engineering errors and human frustrations. Yet, Kistiakowsky mysteriously stated that they often "found ways of getting around them."[26] Moreover, although prospects sometimes looked dim, the organisation succeeded in the timely delivery of fissile material. This was essential to carry out some necessary experiments.[27] Second, going beyond the material to build the bomb, Hymans illustrated that it is important to create an operational environment in which scientists and technicians can "dedicate themselves fully to their scientific vocation."[28] Concerns about physical and psychological safety and security can distract people. This was well understood during the implementation of Los Alamos. The isolated and clandestine character of Los Alamos often negatively impacted the living conditions.[29] Yet, people at Los Alamos tried to make life as pleasant as possible. More than thirty recreational and cultural organisations were established throughout the implementation Los Alamos.[30] Physical resources should support the creation of such a favourable operational environment. It optimises the functioning of the organisation's experts.

5.2.2. Level of autonomy

Hymans argued that it is important that the experts involved in the implementation of a nuclear program maintain sufficient scientific autonomy and decision-making power with respect to their field of expertise.[31] Even if this was not self-evident due to the military and clandestine nature of Los Alamos, there was ultimately sufficient respect for the expertise of the people involved. This benefitted the creative application of individual knowledge, stimulated team work, and strengthened objective operational decision-making. Yet, it simultaneously imply particular security risks.

---

[25] Hawkins, "Manhattan District History," 54.
[26] Lawrence Badash, Joseph Hirschfelder and Herbert Broida (eds.), *Reminiscences of Los Alamos, 1943-1945*, Studies in the History of Modern Science (USA: Reidel Publishing Company, 1980), 65.
[27] Los Alamos Scientific Laboratory Public Relations, "Los Alamos: Beginning of an Era 1943-1945: Part 4" (USA: Los Alamos Scientific Laboratory, 2008), 31.
[28] Hymans, *Achieving Nuclear Ambitions,* 51.
[29] For instance, the people involved at Los Alamos were limited in their use of telephones, surrounded by a chain-link fence and faced poor housing conditions.
[30] Los Alamos Scientific Laboratory Public Relations, "Los Alamos: Beginning of an Era 1943-1945: Part 2," 17.
[31] Hymans, *Achieving Nuclear Ambitions,* 51.

Los Alamos was originally intended to be operated as a military laboratory. Compartmentalised units would, for instance, only receive information that they "needed to know."[32] This type of institutional set up was meant to ensure more rigid top-down control over the implementation and security of the project. Yet, when Oppenheimer was trying to recruit Robert Bacher and Isidor Rabi (MIT) to join Los Alamos, they argued that "the execution of the security and secrecy measures should be in the hands of the military ... the decision as to what measures should be applied must be in the hands of the laboratory."[33] Oppenheimer agreed on that point, "because I believe it is the only way to assure the cooperation and the unimpaired morale of the scientists."[34] Many of the scientists and technicians disavowed a military chain-of-command. It was considered to be ill-suited for scientific decision-making.[35] People wanted a civilian laboratory where scientists could discuss their work with peers and the "center of gravity remained in the scientific staff."[36] This was beneficial in stimulating creative progress, team work and more objective operational decision-making. For instance, once it became clear that a gun-type design would not work with plutonium, Oppenheimer decided to reorient the laboratory more to the implosion-type design.[37] While Major General L.R. Groves had over-all executive responsibility – and securing the isolated area where the laboratory was built was the responsibility of the military - Oppenheimer, a scientist himself, supervised all the scientific work.[38] This system succeeded in reducing subjective interference by military or political institutions while simultaneously guaranteeing the security of the project. For instance, Kistiakowsky - who was in charge for the explosive lenses of the implosion-type design - recalled that Lord Cherwell, the scientific advisor to Winston Churchill, came to Los Alamos in 1944.

> I took him around Los Alamos and gave him absolutely the whole story. He listened to me and told me that Baratol was going to be no good for the lenses, that I should use commercial dynamite. I explained to him why, on theoretical grounds, dynamite couldn't work and we parted friends. A little later Oppenheimer called me in to tell me about Churchill's personal cable to Roosevelt saying that certain people, specifically Kistiakowsky at Los Alamos, are barking up the wrong tree, since Baratol is not going to work, and that they should use dynamite.... So I went through a rather large X (Explosives) Division personnel list, singled out individuals who hadn't

[32] John Manley, "A new laboratory is born," in Badash, Hirschfelder and Broida (eds.), *Reminiscences of Los Alamos, 1943 - 1945,* 35.
[33] Richard Rhodes, *The Making of the Atomic Bomb* (New York: Simon & Schuster, 2012), 454.
[34] Ibid*.,* 454.
[35] National Security Histories Series, "The Manhattan Project: Making the Atomic Bomb" (United States: US Department of Energy, 2010), 80.
[36] Hawkins, "Manhattan District History," 37.
[37] Rhodes, *The Making of the Atomic Bomb*, 549.
[38] Hawkins, "Manhattan District History," 4.

> contributed anything, constituted a group out of them, and so dynamite didn't delay the project in the slightest.[39]

This case study, however, simultaneously illustrated that such levels of scientific autonomy also entail particular security risks to the organisation. To be precise, it became clear that scientific autonomy might sometimes lead to some of the experts not acting in line with the preferences of the organisation. This is a classic example of the principal-agent problem. It led to some human frustrations and operational delays during the implementation of Los Alamos. This held the potential to undermine the effective implementation of the project and, on its turn, lead to increased security risks.

First, the lack of strict top-down control did sometimes lead to frictions between scientists. For instance, Bethe and Oppenheimer were greatly annoyed by Edward Teller. The latter was head of the implosion theory group, but decided to work on the thermonuclear bomb rather than the implosion design. Because a thermonuclear bomb had a low priority, Oppenheimer ultimately decided to limit Teller's autonomy by replacing him.[40] This type of friction holds, e.g., the potential to induce (moral) doubts about a person's participation in the project. Second, scientific autonomy did sometimes lead to the "we know best syndrome." This refers to the phenomenon where autonomous specialists develop strong convictions within their expertise which they refuse to alter.[41] David Busbee, for instance, designed the first S-site plant following his own naval ordinance concepts at the time. Kistiakowsky, however, recalls that the plant was "a monstrosity from our point of view" and "never used afterwards."[42] This phenomenon holds the potential to cause operational delays or errors. Third, the lack of an outside opinion increased the risk of "group-think."[43] This refers to a concurrence-seeking tendency that is driven by social pressure in a cohesive group. For instance, Neddermeyer's first theoretical analysis of the implosion design of a nuclear bomb faced stiff opposition by Oppenheimer, Fermi and Bethe. Manley stated that "nobody else really took it very seriously."[44] Later, however, Bohr went beyond their incredulity to pursue this truly original idea. As it would turn out, the implosion design was a more efficient way to detonate an atomic bomb.[45] Group-think might also lead to operational delays or errors.

---

[39] George Kistiakowsky, "Reminiscences of wartime Los Alamos," in Badash, Hirschfelder and Broida (eds.), *Reminiscences of Los Alamos, 1943-1945,* 52-53.
[40] Hoddeson et al., *Critical Assembly*, 162.
[41] Hymans, *Achieving Nuclear Ambitions,* 52.
[42] Hoddeson et al., *Critical Assembly*, 167.
[43] Irving Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascos* (New York: Houghton Mifflin, 1982), 9.
[44] Manley, "A new laboratory is born", in Badash, Hirschfelder and Broida (eds.), *Reminiscences of Los Alamos, 1943-1945,* 34.
[45] Rhodes, *The Making of the Atomic Bomb*, 479-480.

Any instance of human frustrations, operational delays or engineering errors might undermine the effective implementation of the project or might lead to particular security risks. Indeed, any delay, error or (moral) doubt holds the potential to give rise to the detection or interruption of the project by adversaries. Yet, these risks ultimately did not trump the advantages during the implementation of Los Alamos. Scientific autonomy allowed for better operational decision-making while simultaneously strengthening the flexible and creative functioning of the team.

5.2.3. Information-sharing

Scientific autonomy goes hand-in-hand with high levels of information-sharing. A relatively free flow of information during the implementation of Los Alamos stimulated the combination of knowledge and enhanced a sense of common purpose. Yet, the different communication and coordination mechanisms inherently entailed increased security risks. Any information breach could reveal the ongoing activities at Los Alamos. This thus held the potential to undermine the effective implementation of the plot and the American strategic advantage that followed from the construction of the first nuclear weapons.

Various communication and coordination tools were established during the implementation of Los Alamos. The decision to locate the Los Alamos National Laboratory at one place was instrumental in facilitating communication and coordination. Its physical isolation – and the guarded barbed-wire fence around the laboratory – made it possible to set up formal and informal consultation between scientists and technicians. Even though there were different divisions, there was no strict compartmentalisation between these different units. There was a relatively free flow of information: the heads of the operating groups were in contact with each other through the coordinating council; individual divisions and groups had their own meetings, seminars, published reports, and informal talks; the Los Alamos library reproduced and distributed progress reports by various groups at the laboratory; and weekly colloquiums with all the laboratory employees with a scientific degree or equivalent were organised to discuss the technical program.[46] These channels were both informative and deliberative. This intense flow of information stimulated creativity and flexibility. It encouraged thinking outside the box. Moreover, it also fostered a "sense of common effort and responsibility."[47] It illuminated the joint nature of this effort. John Manley – one of the principle assistants at Los Alamos – stated for instance that:

[46] Hawkins, "Manhattan District History," 32.
[47] Ibid., 33.

> Each scientist could discuss his work with his peers … these discussions brought forth ideas and were excellent morale boosters. I'm sure the work went faster and more effectively as a result. After all, a reason to create Los Alamos was to improve the communication between all those engaged in the weapon problem.[48]

Moreover, different liaison contacts were established between Los Alamos and the other units of the Manhattan Project. In order to develop the bomb, it was, for instance, important for scientists and technicians "to know when (fissile) materials would become available from the production plants at Oak Ridge (Site X), the form in which the material would be received, and the processing which it would have undergone.[49] Liaison officers thus held an important role in coordinating the overall project. Additionally, they also improved safety throughout the implementation of the plot. Richard Feynman, describes a Los Alamos scientist going to Oak Ridge. When he was walking through the plant, he saw them wheeling a tank carboy with an uranium nitrate solution. They were planning to handle it in a similar manner if it would be purified more. Yet, they did not know that the neutrons would be more effective when slowed down in water. This could lead to a reaction that makes radioactivity, thereby becoming very dangerous. If it was not for this scientist visiting Oak Ridge, they would have not paid any attention to this.[50]

Yet, the abundant flow of information also came with an inherent disadvantage. This organisational design feature implied increased security risks throughout the implementation of this clandestine project: notwithstanding the type of organisational design, it is generally hard to secure a project of this size and complexity. Richard Rhodes noted, for instance, that: "Soviet physicists realized in 1940 that the United States must also be pursuing a program when the names of prominent physicists, chemists, metallurgists and mathematicians disappeared from international journals: secrecy itself gave the secret away."[51] Yet, this case study made clear that a high level of information-exchange heightens these security risks. Regular presence at the various formal and informal meetings - which were open to many members of Los Alamos - provided that person with a "generally complete and accurate picture of the problems and progress of the laboratory."[52] Various security measures were established (e.g. the

[48] Manley, "A new laboratory is born", in Badash, Hirschfelder and Broida (eds.), *Reminiscences of Los Alamos, 1943-1945,* 35.
[49] Hawkins, "Manhattan District History," 34.
[50] Richard Feynman, "Los Alamos from Below," in Badash, Hirschfelder, and Broida (eds.), *Reminiscences of Los Alamos, 1943-1945,* 119-121.
[51] Rhodes, *The Making of the Atomic Bomb*, 501.
[52] Hawkins, "Manhattan District History," 33.

isolation of the laboratory, the institution of formal censorship in personal mails, or the prohibition of talking about work in the nearby town Santa Fe). Yet, this could not prevent leaks from occurring. There were many instances of a security breach.[53] For instance, Joseph Hirschfelder – active in the ordnance and engineering division at Los Alamos – recollected that "every once in a while there would be some young loud-mouth who would go down to the La Fonda Bar and shoot his mouth off."[54] This could endanger the project's security. Moreover, even worse, the flow of information made the project vulnerable to infiltration. The most illustrative example is the case of Klaus Fuchs. Klaus Fuchs was a theoretical physicist who managed to participate in different discussions and meetings at Los Alamos. He joined the project via the British mission. Yet, it was unknown that he had communist sympathies and that he forwarded a great deal of the gathered information to Russia. Although it remains unclear what damage he actually caused, some believe he "probably shortened the Russian atomic bomb development by two years."[55] While his intentions were not necessarily focused on undermining the effective implementation of Los Alamos, his actions did damage the greater strategic interests of the United States.[56]

5.2.4. Clear and compelling goals

Hymans argued that the effective implementation of a state nuclear project benefits from the formulation of clear and compelling goals. A clear goal sharpens the focus of the project. A compelling goal inspires the project team in rallying around the common goals of the project.[57] This was also true for Los Alamos. Clear and compelling goals were an important tool in coping with some of the aforementioned organisational challenges to the implementation of this nonroutine plot. Yet, this case study simultaneously illustrated that an unsuccessful attempt to formulate clear and compelling goals might actually increase the security risks related to defection and/or detection.

The mere establishment of Los Alamos was instrumental to the creation of a clear goal. Indeed, it was Los Alamos, and no other laboratory, that would make the first bomb.[58] Los Alamos was mission-oriented.[59] All scientists received Robert Serber's lecture *The Los Alamos Primer* when arriving at Los

[53] Hoddeson et al., *Critical Assembly,* 96.
[54] Joseph Hirschfelder, "Scientific Technological Miracle at Los Alamos," in Badash, Hirschfelder and Broida (eds.), *Reminiscences of Los Alamos, 1943-1945,* 86.
[55] Ibid.*,* 85.
[56] Another famous example of a suspected spy is Theodore Hall. He passed along information to the Soviet Union about the implosion-type bomb and on the processes for purifying plutonium.
[57] Hymans, *Achieving Nuclear Ambitions,* 53.
[58] Los Alamos Scientific Laboratory Public Relations, "Los Alamos: Beginning of an Era 1943-1945: Part 3."
[59] Hoddeson et al., *Critical Assembly,* 5-6.

Alamos. This brought them up to speed with the principles and goals of the project. Rhodes notes in this respect that "the scientists' euphoria at finally learning in detail what they had only previously guessed or heard hinted, measures the extent to which secrecy had contorted their emotional commitment to the work."[60] The group strived to accomplish a common goal. This allowed the project team to steadily progress and remain focused. Continuous formal and informal meetings throughout the project subsequently enhanced clarity on the project's (intermediary) goals. This stimulated both the focus and dedication of scientists and technicians. Burke – a member of the Chemistry and Metallurgy Division – noted, for instance, that:

> Looking back, I am impressed with how simply we did our planning there. There were no PERT charts, no milestones and no long proposals to be made and reviewed. When a need was established, the requirements were spelled out as clearly as possible and the people involved tried to make what was needed. They generally succeeded. I suppose so much was accomplished in such a short time because we all agreed that the very clear goal was a proper one and because everyone was so highly competent and so highly motivated by patriotism.[61]

This quote simultaneously illustrates the compelling nature of Los Alamos' goals. Both factors are closely intertwined. Establishing coming goals is facilitated by the formulation of clear goals. Considering the perceived German nuclear threat, experts were readily emotionally attracted to the clear and common goal of this project. The second World War stimulated the scientists and technicians' motivation to build the nuclear bomb. This alleviated some of the aforementioned forms of divergent behavior. The personal conflicts between, e.g., Teller and Bethe or Kistiakowsky and Neddermeyer, demonstrate the susceptibility to conflict. Yet, a common goal implied that strong individuals were more likely to subordinate their individual goals and standards of their profession to the needs of the group. There was, in general, little dissent about fighting against the Axis powers. Establishing such a common goal was actively pursued by the leadership. For example, President Roosevelt had Oppenheimer read a personal letter at a colloquium organised in 1943:

> I wish you would express to the scientists assembled with you my deep appreciation of their willingness to undertake the tasks which lie before them in spite of the dangers and the personal sacrifices. I am sure we can count on their continued wholehearted and unselfish labors.

[60] Rhodes, *The Making of the Atomic Bomb*, 460.
[61] J. Burke, "Recollections of Processing Uranium Hydride and Plutonium at Wartime Los Alamos," *Journal of Nuclear Materials* 100 (1981): 12.

Whatever the enemy may be planning, American science will be equal to the challenge.[62]

Clear and compelling goals thus enhance the organisation's coherence, focus, and perseverance. Yet, it simultaneously might entail particular security risks. First, a clandestine organisation is vulnerable if the formulation of goals is clear but not compelling. The example of Klaus Fuchs demonstrates the security risks that follow from an uncompelled worker who is informed about the goals and progress of the project. Moreover, another example can be found by looking at Szilard or Rotblat. When it became clear that Germany was nearly defeated, these people argued against the use of atomic weapons. Moral doubts about the common goal of the project might lead to defection or disruption of the effective implementation of the plot. Second, the leadership of the project needs to ensure that the formulation of clear goals does not evolve into top-down meddling in day-to-day affairs. As mentioned earlier, this might undermine the scientists and technician's operational decision-making capability. It might hamper their adaptive and creative functioning. This might be counterproductive to the project's effective implementation and might imply particular security risks.

The latter remark points to the overall importance of good leadership. Although the organisation needed to cope with a clandestine operational environment, the leadership succeeded in providing sufficient resources and formulating clear and compelling goals while simultaneously preserving scientific autonomy and establishing sufficient tools for information-exchange between the various members of the project. Not surprisingly, both the synergy between Groves and Oppenheimer and Oppenheimer's role in effectively building the bomb is often praised.[63] Although any (moral) doubt or security breach could have undermined the effective implementation of the project, the leadership succeeded in uniting the diverse individuals in a high-performing and multidisciplinary team.

5.3. Los Alamos: similar to an organic organisational design

Turning from description to exploration, I will now elaborate specifically on the role and impact of the group's organisational design. I have adopted a definition of the organisational design as "the sum total of the ways in which its labor is divided into distinct tasks and then its coordination is achieved among these tasks."[64] This case study underlined that the organisational design shapes some of the

[62] Letter from Franklin D. Roosevelt to Robert J. Oppenheimer, 29th of June 1943. Available at: http://www.loc.gov/teachers/classroommaterials/presentationsandactivities/presentations/timeline/depwwii/wwarii/fdr.html (accessed April 13, 2019).
[63] National Security Histories Series, "The Manhattan Project: Making the Atomic Bomb," 79.
[64] Henry Mintzberg, *Structure in Fives: Designing Effective Organisations* (New Jersey: Prentice-Hall, 1983), 2.

main organisational challenges to the implementation of such a project. The following section will link the aforementioned organisational dimensions – and its corresponding challenges – to the organisational design. In doing so, this section will elaborate explicitly on how the organisational design influenced the implementation of Los Alamos. I will not yet extrapolate insights to the adopted nuclear terrorism scenario.

In short, it became clear that Los Alamos can be characterised by an organisational design that has many organic organisational design features (see table 5.1). This type of design was beneficial to the effective implementation of this plot. Yet, it simultaneously implied a substantial investment of resources and increased security risks.

Table 5.1. Organisational design of Los Alamos

	Organisational design of Los Alamos
Level of interconnectedness	Relatively high number of intra-division and inter-division connections
Level of hierarchy	Relatively high level of control over the operations by the experts themselves + high resource support to the experts.
Level of specialisation	High level of personal specialisation (high level of both techne and metis)

* Note that this table is inherently arbitrarily to some extent. It is difficult to assign exact and uniform values to these design parameters.

We first reflect upon the type of specialisation. This is chosen as a starting point because it has consequences for both those who perform the job and the control and coordination over the different jobs. It is clear that the implementation of this project required high levels of personal specialisation. The experts involved needed to have both technical knowledge (= techne) and practical knowledge (= metis) to cope with the nonroutine problems that arose throughout the development of this breakthrough technology. The project required an adequate people with the necessary training and experience. As I have illustrated throughout the previous sections, the organisation's success in recruiting and employing some of the nation's greatest minds and outside help was of great importance to the effective implementation of this project.

Second, these experts were given the opportunity to operate at a high functional capacity. This improved the effective implementation of the plot. On the one hand, the (political) leadership provided the project team with a lot of material resource support. They moreover formulated clear and

compelling common goals.[65] On the other hand, this implied that the organisational design allowed for an appropriate level of operational autonomy and decision-making power by the experts involved. Los Alamos' institutional disposition gave the experts – rather than the political or military leaders - control over their work. There were several groups and divisions. There were thus also various scientific leaders in hierarchical positions. Yet, Los Alamos was generally not characterised by a strictly centralised hierarchical control system.[66] Coordination and control over the diversity of nonroutine tasks and activities is hard to establish via carefully predetermined rules and specifications. The leadership did not centrally specify exactly who will do what, when and where.[67] There was no strict behavioural formalisation and there were no tight planning and control systems. More organic means (e.g. mutual adjustment and direct supervision) were often used to control and coordinate the work of the scientists and technicians. This was beneficial to the latter's flexibility, creativity and adaptability. Moreover, it stimulated the experts' intrinsic motivation and dedication to their tasks and activities.

Finally, and closely related, Los Alamos was characterised by a relatively high number of intra-division and inter-division connections. Various communication and coordination tools were established throughout the implementation of Los Alamos (e.g. formal and informal meetings, access to outside help, liaison positions between different groups and divisions, weekly colloquiums, etc.). Considering it was not centrally specified exactly who would do what, when and where, people needed to work together and coordinate their actions. This was necessary in order to effectively cope with the nonroutine problems that arose throughout the implementation of this plot. Communication (and consultation) therefore tended to be more lateral than vertical. This organisational design feature was beneficial to both the motivation and effectiveness of the experts involved in the project.

Los Alamos was thus characterised by an organisational design with many organic organisational design features. This benefitted the effective implementation of the plot. It promoted the creativity,

[65] Hymans already underlined the "need for a clear top-down political decision to go nuclear as a prerequisite for getting the project in gear." Jacques Hymans, "review on unclear physics: why Iraq and Libya failed to get the bomb" *ISSF roundtable 9-22.* Available at: https://networks.h-net.org/node/28443/discussions/189010/issf-roundtable-9-22-unclear-physics-why-iraq-and-libya-failed-get#_Toc489128157 (accessed November 26, 2018.)

[66] Different job positions were united in different groups. These groups were, on its turn, united into various divisions. For instance, the ordnance division comprised of several groups (e.g., Proving Ground, Instrumentation, Fuse Development, Projectile, Target, and Source, Implosion Experimentation, Engineering, Delivery Interior Ballistics, High Explosive Development, S Site, RaLa and Electric Detonator). These groups and divisions were functionally differentiated (Charles Thorpe and Steve Shapin, "Who Was J. Robert Oppenheimer? Charisma and Complex Organisation," *Social Studies of Science* 30, no. 4 (2000): 561).

[67] Admittedly, at the final phase of Project Y, Oppenheimer launched the powerful Cowpuncher Committee to "ride herd" on the implosion program. The committee oversaw eight major programs. At weekly meetings, "this committee relentlessly defined and redefined the assignments to individual groups, while constantly adjusting scheduled milestones." This appears to come closer to more strict planning of the different tasks and activities. Yet, in my understanding, this still implied a relatively high level of operational discretion by the experts itself.

adaptability and flexibility to cope with the nonroutine technology at hand. Yet, it simultaneously implied some organisational challenges. As suggested by the organisational design literature,[68] this case study supports the idea that this type of design does not constitute - in general - an efficient way of organising. It implied a substantial investment of resources and increased security risks.

On the one hand, the implementation of Los Alamos required a substantial investment of both human and material resources. As mentioned before, the total number of personnel increased steadily from 250 to 2,500 in July 1945. This included some of the brightest minds at that time. They were dedicated to the invention of the atomic bomb. Considering the material resources, Hoddeson stated that the political leadership did ensure "essentially unlimited funding and material support" to projects in line with the mission.[69] This was beneficial to the creation of a favourable operational environment that benefitted the functioning of the experts.

On the other hand, control and coordination over the implementation of Los Alamos was hard to standardise. The adopted organic organisational design features brought about increased security risks. First, Los Alamos required various experts (and outside help). The availability of an adequate number of well-skilled people benefitted the effective implementation of the plot. Yet, it was no efficient way to guarantee security. As mentioned earlier Rhodes stated that the mere disappearing of these experts from publishing in international journals made the Soviets aware that the U.S. was pursuing a nuclear program. Moreover, a higher number of persons involved inherently implies an increased risk for detection. Second, the lack of strict hierarchical control entailed some level of fluidity and ambiguity with respect to the tasks to be performed and the coordination between these different tasks. Scientists and experts were allowed the necessary operational discretion. They adopted a "trial-and-error" methodology. Yet, this also led to some divergent behavior. This, on its turn, could undermine the security of the project. Any defection, delay or error holds the potential to give rise to detection or interruption by adversaries. More strict control and coordination could potentially alleviate this concern. Finally, this institutional design required a great deal of information-exchange and coordination. Combining knowledge and expertise enabled the people involved to deal with the nonroutine problems that arose. Yet, it simultaneously entailed increased security risks. Klaus Fuchs is probably the best example of such a risk. Not surprisingly, there were indeed various security breaches

[68] See, e.g., Henry Mintzberg, *Structure in Fives,* 277
[69] Hoddeson et al., *Critical Assembly*, 6.

throughout the implementation of Los Alamos.[70] Yet, notwithstanding these challenges, Los Alamos successfully developed and constructed the first nuclear bombs.

Considering the focus of this study, the question now becomes to what extent these organisational dynamics and challenges would also be applicable to a nuclear terrorism project. Taking into account the potentially qualifying conditions, the following section will draw upon the insights that follow from this case study to reflect upon the previously formulated hypotheses on the probability of nuclear terrorism.

5.4. Extrapolations to the nuclear terrorism threat

This section will be framed around the idea of an effectiveness-efficiency trade-off. To be precise, I will first elaborate on the type of organisational design of which I expect that it would increase the likelihood that a terrorist organisation can *effectively* implement a nuclear terrorism project (= H1). Second, I will elaborate on why I expect that that particular type of organisational design would simultaneously be an *inefficient* way for a terrorist organisation to guarantee the security of its nuclear terrorism plot (=H2). Third, I will make some provisional comments with respect to the match between a nuclear terrorism plot and a terrorist organisation's strategic-political goals (=H3).

5.4.1. Effectiveness…

Considering the fit between the organisational design and the nonroutine nature of technology, this first explorative case study generally confirms the plausibility of the first hypothesis. It remains plausible to expect that "a terrorist organisation is most likely to effectively complete a nuclear terrorism project by means of an organisational design similar to an organic design." (= H1)

First, the Los Alamos case underlined the importance of individuals with the necessary techne and metis. It stresses the need for sufficient personally specialised people throughout the implementation of any nonroutine plot.[71] This can thus be expected to also hold true for the implementation of a nuclear

[70] For instance, considering the different cases of espionage, please have a look at the Department of Energy's website on the Manhattan project. Available at. https://www.osti.gov/opennet/manhattan-project-history/Events/1942-1945/espionage.htm (accessed November 22, 2018).

[71] My research does not allow me to further quantify the term 'sufficient.' The exact number will ultimately be a function of the exact nuclear terrorism scenario and its nonroutine nature of technology (see chapter 9).

terrorism plot. Admittedly, the implementation Los Alamos placed higher demands on the skills, perseverance, and creativity of the experts involved. Yet, the adopted nuclear terrorism scenario (and all its different steps) is also expected to be characterised by a nonroutine nature of technology. A terrorist organisation would need an adequate number of individuals with the necessary techne and metis. The tasks can be as diverse as, e.g., reconnoitring a nuclear facility, designing the nuclear device, illicitly funnelling financial means, casting fissile material, smuggling non-nuclear components, or coordinating the attacking team. Any unnoticed security measure, (moral) doubt, technical hick-up, personal disagreement, detection of a part of the plot, or any other contingent factor can substantially complicate matters. These type of unexpected situations are hard to analyse in advance and require particular techne and metis by the people involved. Note in this context that the development of a 15kT nuclear explosion would also imply higher demands in terms of the required specialised skills than the development of a 100 ton nuclear explosion (see chapter 2).[72] We should think about the nonroutine nature of technology as a matter of degree, not of kind.

Second, we can theoretically generate from this case study that the functional capacity and effectiveness of the experts is likely to rise if they can operate in an organisation with an appropriate organisational design. This idea often remains underdeveloped in the literature on the nuclear terrorism threat. On the one hand, it implies that the leadership should provide appropriate material resource support to the project team. Moreover, they should formulate clear and compelling common goals. This does not imply that the political and ideological leadership should be absent. They can focus and support the group's implementation efforts. Yet, on the other hand, it does imply that the organisational design should also allow for an adequate level of scientific autonomy and information-sharing. The adopted nuclear terrorism scenario is a nonroutine project. Operational control should be situated at the level of the experts (rather than at the level of the political leaders). The terrorist leadership needs to refrain from centralised, top-down meddling. Impeding horizontal communication and coordination, imposing (pet) solutions at the expense of practical progress, or adopting stringent action planning is expected to increase the risks with respect to operational delays, errors, and frustrations. For instance, as Lord Cherwell pushed for the use of commercial dynamite at Los Alamos, unduly (ambitious) demands by a terrorist leader could induce an expert to disregard some essential engineering considerations in a nuclear terrorism project or to neglect diverse security issues (e.g. entering the nuclear black market without sufficient regards for security). Moreover, various intra-group and inter-group connections and information-sharing is likely to benefit the effective implementation of the project. For instance,

[72] Note that - considering a nuclear explosion with a lower yield - an organisation would still need the expertise and skills to identify the potential of such a weapon and how to obtain it.

terrorists that need to design and construct the nuclear device will need to be aware of the type of fissile material that has been acquired, and might, on its turn, need to inform illicit traffickers about the characteristics of the required nuclear and non-nuclear components. Adequate levels of scientific autonomy and information-sharing are thus expected to benefit the effective implementation of a nonroutine nuclear terrorism plot.

5.4.2. Versus efficiency

Various organic organisational design features are expected to strengthen a terrorist organisation's potential to cope with the nonroutine technology of a nuclear terrorism project. Yet, second, I will elaborate on why I expect that this particular type of organisational design would simultaneously be an *inefficient* way for a terrorist organisation to guarantee the security of a nuclear terrorism plot (=H2). Moreover, I will build upon these insights to place some provisional comments with respect to the match between a nuclear terrorism plot and a terrorist organisation's strategic-political goals (=H3).

Considering the fit between the organisational design and the group's clandestine operational environment, this case study generally supports the plausibility of the hypothesis that an organisational design similar to an organic design implies increased security risks to a terrorist organisation and its nuclear terrorism project (=H2). Three issues underline and demonstrate this argument.

First, the Los Alamos case study demonstrated that the recruitment of experts is not necessarily a straightforward process. Even though this project enjoyed a relatively high level of domestic and international legitimacy (supra), it was nevertheless charactised by some minor recruitment challenges. This implied particular security challenges. One always needs to be cautious in sharing information to outsiders. Given that a nuclear terrorism plot can be expected to enjoy less popular legitimacy, it seems plausible to expect that the recruitment of an adequate number of people with the with the necessary techne and metis (e.g. clandestine procurement skills, nuclear physics experts, advanced military skills, financial experts, etc) might be a challenging task. Resourceful and popular rebel groups might adopt expertise-oriented recruitment periods.[73] Yet, the risks of espionage, infiltration or fraud remains a

[73] Steven Windisch, Michael Logan, and Gina Scott Ligon, "Headhunting Among Extremist Organisations: An Empirical Assessment of Talent Spotting," *Perspectives on Terrorism* 12, no. 2 (2018): 19; Mia Bloom, "Constructing Expertise: Terrorist Recruitment and 'Talent Spotting' in the PIRA, Al Qaeda, and ISIS," *Studies in Conflict & Terrorism* 40, no. 7 (2017): 603–23; Brian Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict & Terrorism* 24, no. 3 (2001): 183–213."

particular concern for terrorist organisations. Loyalty to the terrorist organisation might prove to be a particular important recruitment criteria. In this context, it is interesting to note that the nucleus of the group at Los Alamos came from several groups working for or with Oppenheimer. His familiarity with various researchers catered to some extent to these security constraints.

Second, the Los Alamos case study underscored that higher levels of scientific autonomy entail an increased level of fluidity, confusion and ambiguity. A less hierarchical design implies less operational control over the experts' actions. This could lead to, e.g., operational errors or frustrations, (moral) doubts with respect to the project, and/or leaks to counterterrorism forces (e.g. as a result group think processes, friction between scientists, or the "we know best syndrome"). It is thus plausible to expect that the impact of such levels of operational autonomy might also be at play during the implementation of a nuclear terrorism plot. As Abrahms argued, it is not necessarily true that the motivation and goals of the "rank-and-file" is similar to the incentive structure and objectives of the leadership.[74] An increased likelihood of divergent behavior by the experts involved entails an increased risk that the nuclear terrorism plot would be detected or disrupted. Adopting a terrorist organisation's perspective, any instance of an operational error, delay or defection holds the potential to undermine the implementation of a nuclear terrorism plot. This again touches upon the issue of the loyalty of the experts involved.

Finally, the Los Alamos case study highlighted that higher levels of information-exchange also imply increased security risks. The multiple communication lines and coordination tools between different divisions and individual members increased both the likelihood of detection and the likelihood that any security breach would be a substantial security breach. Theoretically extrapolating these insights to the implementation of a nuclear terrorism plot, it seems plausible to expect that an increase in communication and coordination tools would also imply an increased likelihood that any of these information-exchanges might be intercepted by counterterrorism forces. Each exchange of information provides an opportunity for counterterrorism forces to detect (parts of) the ongoing operation. Moreover, a lower level of compartmentalisation would also imply that any security breach might allow counterterrorism forces to intrusively penetrate the plot. The different individuals and units in the plot are connected to each other. This could aggravate the consequences of any potential security breach. The terrorist equivalent of Klaus Fuchs might prove to be disastrous for a terrorist organisation and its nuclear terrorism plot.

[74] Max Abrahms, *Rules for Rebels: the Science of Victory in Militant History* (Oxford: Oxford University Press, 2018), 108-112.

Yet, Los Alamos and the adopted nuclear terrorism scenario are not identical. I need to take into account the degree of heterogeneity between Los Alamos and the adopted nuclear terrorism scenario. Los Alamos' intense nonroutine nature of technology, substantial size, and project time should be taken into account as potentially qualifying conditions. Indeed, even if this first explorative case study was ideal to facilitate the exposure of different organisational dynamics, not all of them are necessarily applicable to a potential nuclear terrorism plot.

Each of the aforementioned heterogeneous issues (the intense nonroutine nature of technology, the project's substantial size, and its long implementation period) probably increased each of the three aforementioned security risks. For instance, the likelihood of detection (via, e.g., espionage) is heightened when a large group takes a long time to implement a project characterised by very high levels of scientific autonomy and information-sharing. These security risks might thus be less pressing in, e.g., a scenario where a terrorist organisations would aims to develop a nuclear device with a 100 ton yield. Indeed, the development of a less sophisticated and efficient nuclear explosion might require a less organically designed organisation. This might thus also alleviate the security costs to this design. Yet, notwithstanding that the degree of security risks might vary, I do not see any reason to theoretically refute the abstraction that was generated from this case study. I believe it remains plausible to expect that an organisational design with various organic features will increase the likelihood of an inefficiently functioning terrorist organisation with respect to its security (=H2). Considering the illegitimate nature of a terrorist organisation – and the size and consequences of such a nuclear terrorism plot – a terrorist organisation might be particularly sensitive to these security risks.

Before moving to the other cases studies, I will now also briefly reflect upon these insights to make some provisional comments with respect to the match between a nuclear terrorism plot and a terrorist organisation's strategic-political goals (=H3). Considering the inherent differences between a state and non-state actor, it should be emphasised that the latter two case studies of actual nonroutine terrorism plots will be of primary importance with respect to the assessment of this third hypothesis. Nevertheless, it is worthwhile to note that the implementation of Los Alamos enjoyed a relatively high level of domestic and international legitimacy. This project took place in the context of the second World War. Due to a series of military defeats in the Pacific, the German threat, and the military and strategic value of an atomic bomb, there was a relatively high level of support for the development of such a weapon. This had some intertwined consequences relevant to the focus of this study. First, it benefitted the human and material resource support to this project. Mobilisation of resources for this project became a less daunting task. Second, and closely related, it facilitated the creation of a common and compelling goal to the members involved. The instrumental rationality and inherent value behind this

project was clear. Finally, it alleviated some of the security concerns. Indeed, notwithstanding various and substantial security breaches, the progress of this project was not undermined by any adversaries that were aware of the program. No adversary did not halt the American nuclear program. This level of legitimacy and support thus enabled Los Alamos to overcome various of the aforementioned concerns. This is not necessarily true for a terrorist organisation. This might subsequently have particular consequences on its strategic considerations. Yet, this lines of thought will be developed in more-depth in the final two case studies.

5.5. Conclusion

Los Alamos was the first case study to explore the plausibility of the suggested theoretical propositions and hypotheses with respect to the likelihood of nuclear terrorism. It was appropriate to expose various organisational dynamics and challenges relevant to this study's focus due to its intense nonroutine nature of technology, its substantial size, and its long project time. Yet, these differences with the adopted nuclear terrorism scenario simultaneously imply that this provisional analysis should be treated with caution. Indeed, it might be the case that these heterogeneous issues increased each of the three aforementioned security risks.

Nevertheless, that being said, this case study does in general affirm the relevance of the organisational design variable in adopting a particular type of technology. The organisational design had an impact on the implementation of Los Alamos. It is subsequently plausible to expect that it will also impact the implementation of a nuclear terrorism plot. Moreover, more specifically, this case study does not provide us with any reason to theoretically refute the plausibility of the suggested effectiveness-efficiency trade-off. On the one hand, it became clear that an organisational design similar to an organic organisational design increases the likelihood that the organisation can effectively complete a nonroutine project. The (political) leadership can focus and support the group's implementation efforts. Yet, the experts should be able to operate at a high functional capacity. They should enjoy an adequate level of operational autonomy and sufficient opportunities to exchange information. This will increase the likelihood that they can effectively cope with the nonroutine problems at hand. On the other hand, however, this case study also supports the idea that this type of organisational design would simultaneously be an *inefficient* way for a terrorist organisation to guarantee the security of its nuclear terrorism plot. Each of the three organic design features implies particular security risks.

These insights are only first explorations. The differences between the Los Alamos case and the adopted nuclear terrorism scenario might imply that, e.g. our inferences are blown out of proportion. Moreover, other contingent factors (e.g. the role of counterterrorism efforts) will also play a role. Thus, in order to strengthen my extrapolations, I now turn to the second case study: the South African PNE program. This program was also a nonroutine project, but it is often perceived as a state nuclear project more akin to a nuclear terrorism project. It is therefore interesting to reflect upon whether or not there were similar organisational dynamics and challenges at play throughout the implementation of this project?

6. Case study: the South African PNE program

The second case study that has been selected to explore the plausibility of the hypotheses is the South African design and construction of a nuclear device by means of the Peaceful Nuclear Explosives (PNE) program.[1] This program is more analogous to the adopted nuclear terrorism scenario with respect to both the degree of the nonroutine nature of technology and the other contingencies. This enables this study to assess the extrapolations and qualifying conditions that were identified in the first case study. It generally allows us to strengthen our understanding of the nuclear terrorism threat.

The origins of South Africa's nuclear program date back to the closing days of the Second World War.[2] Considering South Africa harbored abundant natural uranium resources, the country was an essential player in establishing a stable supply of uranium to the American (and British) nuclear program.[3] Yet, due to the enormous amount of reserves of this valuable material, a "more active participation in nuclear matters" could not be excluded for long.[4] The Atomic Energy Board (AEB) – which was established in 1948 - launched a civilian nuclear research and development program at the Pelindaba site in 1959. They recruited and trained scientists and technicians, acquired nuclear and nuclear-related information, constructed and procured equipment, and built research and support facilities.[5] In doing so, they enjoyed the benefits of civilian nuclear cooperation agreements with, e.g., the United States and Britain. For instance, Eisenhower's "Atoms for Peace" program led to various opportunities to overseas training for the experts involved and the construction of the research reactor Safari-1.[6]

In 1967, the AEB succeeded in establishing a self-sustaining chain reaction at their power reactor at Pelinduna.[7] Even though this program was terminated in 1969 in favour of a parallel project on uranium enrichment, it did improve and establish South Africa's confidence in its indigenous expertise on reactor

[1] Large sections of this chapter are published in: B. Volders, "Nuclear Terrorism: What can we Learn from the South African Development of Nuclear devices," *Dynamics of Asymmetric Conflict*, 2019.
[2] Andre Buys, "Proliferation risk assessment of former nuclear explosives/weapons program personnel: the South African case Study," *Research Report University of Pretoria* (2007): 6.
[3] Roy Horton, "Out of (South) Africa: Pretoria's Nuclear Weapon Experience," *USAF Institute for National Security Studies Occasional Paper* 27 (1999), 5; Nic Von Wielligh and Lydia Von Wielligh-Steyn, *The bomb: South Africa's nuclear weapons programme* (Pretoria: Litera Publications, 2015), 97.
[4] Hannes Steyn, Richard Van der Walt, and Jan Van Loggerenberg, *Nuclear Armament and Disarmament: South Africa's Nuclear Experience* (New York: iUniverse, Inc., 2007), 30
[5] David Albright and Andrea Stricker, *Revisiting South Africa's Nuclear Weapons Program: Its History, Dismantlement, and Lessons for Today* (Washington: Institute for Science and International Security, 2016), 4.
[6] Von Wielligh and Von Wielligh-Steyn, *The Bomb,* 104-110.
[7] Steyn, Van der Walt and Van Loggerenberg, *Nuclear armament and disarmament*, 33; Nuclear Threat Initiative, "South Africa nuclear chronology" (Washington: Center for Nonproliferation Studies, 2009); Von Wielligh and Von Wielligh-Steyn, *The bomb*, 110.

physics and manufacturing critical facilities. This was important in the future development of the PNE program. Indeed, influenced by the international community's interest in using nuclear explosives for civil applications,[8] and in an attempt to keep the interest of a "team of reactor physicists…deemed essential for the future work of the AEB",[9] the AEB launched an internal committee to research the technical and economic aspects of PNE's after the termination of the Pelinduna project.[10] Carl de Wet, the Minister of Mines, subsequently approved a secret program for the development of peaceful nuclear devices in March 1971.[11] Although different types of nuclear devices were identified, the PNE program primarily focused on the gun-type design. They focused on building a nuclear explosive device without a delivery system. This device was meant for testing and demonstrative purposes. The responsibility over this program was given to the AEB's Reactor Development Division (RD Division).[12] This division already existed during the Pelinduna power reactor program but was reorganised to this task. It only had to focus on the construction of the bomb; not the enrichment of fissile material.[13]

This RD Division consisted of 9 functional subdivisions.[14] Although this group was still situated on the Pelindaba site, facilities were erected in a secluded area on this site.[15] Albright & Stricker mention that the entire group "was growing to about 50-100 people."[16] There were substantial suspicions by the international community about Pretoria's nuclear project. Yet, the RD Division produced a first gun-type device without a HEU core by mid-1977. The device was 2.79 meter in length, and had a diameter of 480 mm (excluding the protective steel case). The total weight was 3450 kg.[17] A cold test – which would not result in an actual yield-producing explosion - was first planned for August 1977 at the Vastrap site in the Kalahari Desert, but was detected by the international community. Yet, after a successful cold test in 1978, the RD Division succeeded in building a complete nuclear device that included an HEU core.

---

[8] Steyn, Van der Walt, and Van Loggerenberg, *Nuclear Armament and Disarmament,* 36.
[9] Ibid., 36.
[10] Nuclear Threat Initiative, "South Africa Nuclear Chronology."
[11] Von Wielligh and Von Wielligh-Steyn, *The Bomb,* 122.
[12] Steyn, Van der Walt, and Van Loggerenberg, *Nuclear Armament and Disarmament*, 36.
[13] This was the responsibility of a separate organisation, UCOR. This organisation was established to produce the uranium hexafluoride feed material for an indigenously developed and erected uranium isotopic separation plant. This plant was known as the Pilot (or Y) Plant.
[14] Steyn, Van der Walt, and Van Loggerenberg, *Nuclear Armament and Disarmament,* 37. Written correspondence with André Buys, April 15, 2017.
These nine subdivisions are: the nuclear engineering group, the theoretical reactor physics group, the theoretical nuclear physics group, the experimental reactor physics group, the reactor engineering group, the electronic engineering group, the process metallurgy group, the physical metallurgy group, and the nuclear chemistry group.
[15] Written correspondence with Nic Von Wielligh, October 17, 2017. He led the South African team that interfaced with the IAEA during South Africa's declaration of its past program. The Reactor Engineering subdivision was seconded to the Propulsion Laboratory of the National Institute for Defence Research (NIDR) of the Council for Scientific and Industrial Research (CSIR) at Somerset West – a small city close to Capetown (1972 to 1976).
[16] Albright and Stricker, *Revisiting South Africa's Nuclear Weapons Program*, 29; Confirmed by written correspondence with André Buys, June 24, 2017.
[17] Von Wielligh and Von Wielligh-Steyn, *The Bomb,* 134-135.

This device was called Video.[18] This civilian-led PNE program was afterwards taken over by the Armaments Corporation of South Africa (Armscor), which was part of the South African Department of Defence. They produced five other gun-type nuclear devices. Although this chapter will sometimes touch upon these later phases in the South African nuclear program, it will primarily focus attention to the implementation of the PNE program.

This chapter will be structured according to a similar theory-generating narrative to the previous chapter (supra: research design). Following a similar structure facilitates the cross-case analysis in chapter nine. After first elaborating on the relevance of the PNE program, this chapter will reflect upon the four previously identified organisational dimensions. These were also relevant throughout the implementation of the PNE program. Next, turning from description to exploration, this chapter will focus on the role and impact of the organisational design. This variable shapes these four organisational dimensions and its corresponding challenges. Finally, this chapter will extrapolate relevant insights to the formulated hypotheses on the probability of nuclear terrorism. Were there similar (or new) organisational dynamics and challenges at play throughout the implementation of this project?

6.1. The relevance of South Africa's PNE program

The main selection criterion for studying the South African PNE program was its theoretical relevance. Similar to the adopted nuclear terrorism scenario and Los Alamos, this case study was characterised by a *nonroutine* nature of technology. While the exact tasks and activities are not identical to the adopted nuclear terrorism scenario, this shared organisational feature is the basis for my extrapolations with respect to the nuclear terrorism threat. In addition, this case constitutes a project more analogous to the adopted nuclear terrorism scenario with respect to both the degree of the project's nonroutine nature of technology and the other contingencies. This enables this study to better assess and understand the extrapolations and qualifying conditions identified in the first case study.

First, considering the combination of various technical challenges and the project's clandestine operational environment, the PNE program was characterised by a high task variability and low task analysability. Although this project did not implement breakthrough technology, André Buys compared it to "reinventing the atom bomb."[19] On the one hand, this was a product of the technical complexity of

[18] Von Wielligh and Von Wielligh-Steyn, *The Bomb,* 149. This device was later replated, and named Melba. It was used as a demonstration-device.
[19] Written correspondence with André Buys, June 24, 2017.

the tasks that needed to be completed and attuned to each other.[20] The South Africans did not adopt a pure "trial-and-error" strategy.[21] Yet, the work has been described as a "learning exercise" that was "based on systematic theoretical and experimental research, technology development, prototype design and extensive test and evaluation."[22] This project went beyond the standard operations of its personnel. For instance, little was known about ballistics, explosives and pyrotechnics. The reactor engineering group of the RD Division was therefore sent to Somerset West to work on the mechanical and pyrotechnical subsystems of the gun-type device.[23] This team faced "several challenges, including achieving the repeatability of projective velocity and symmetry requirements when the projectile flies into the core."[24] On the other hand, these unexpected problems could also result from – or be exacerbated by – the clandestine nature of the project. The PNE program was a secret project. Some examples of nonroutine problems that occurred due to the program's clandestine nature are the loss of top secret documents,[25] the challenging procurement of non-nuclear components,[26] or the detection of the Vastrap test site in 1977. The latter forced a "crash program to dismount and remove critical equipment that could not be explained for military use."[27] Thus, even though not to the same extent as during the implementation of Los Alamos (see figure 4.1), the PNE program was characterised by the occurrence of exceptional problems that are hard to systematically analyse in advance.

Second, going beyond the more analogous nonroutine nature of technology, other contingent factors were also more analogous to the adopted nuclear terrorism scenario. There was a relatively low number of people involved in the PNE program (infra). Moreover, it was completed in a clandestine operational environment and directed to the construction of a relatively simple gun-type device.[28] The first nuclear device – codenamed Video – would be the type of crude device we might expect in the adopted nuclear terrorism scenario. We still need to keep in mind the differences between the PNE program and the adopted nuclear terrorism scenario in the analysis that will follow (i.e. it remains a state nuclear project and the exact tasks and activities are not identical). Yet, this case does seems appropriate to critically reflect upon the extrapolations that followed from the first case study. To which extent were similar (or new) dynamics at play throughout the implementation of the South African PNE program, and what

[20] Various of my respondents (Nic Von Wielligh, Andre Buys, Anna-Mart van Wijck, Johan Slabber) agreed that building the nuclear device was a very demanding technical challenge.
[21] Written correspondence with Johan Slabber, August 17, 2017.
[22] Written correspondence with André Buys, June 24, 2017.
[23] Ibid.
[24] Albright and Stricker, *Revisiting South Africa's Nuclear Weapons Program,* 27.
[25] Written correspondence with Johan Slabber, August 17, 2017; Written correspondence with André Buys, April 15, 2017.
[26] Written correspondence with Johan Slabber, August 17, 2017.
[27] Steyn, Van der Walt and Van Loggerenberg, *Nuclear armament and disarmament*, 41.
[28] Jessica Stern, *The Ultimate Terrorists* (Cambridge and London: Harvard University Press, 1999), 58-60.

does this imply with respect to our understanding of the nuclear terrorism scenario? This way, this second case study forms a new piece of the puzzle.

Finally, case selection was also based on the availability of reliable data. Access to reliable information on the implementation of the PNE program became less challenging due to the fact that South Africa has given up on its nuclear arsenal. Security considerations often hamper access to reliable information on smaller and clandestine nuclear proliferation programs. I have, for instance, managed to correspond with Andre Buys[29] and Johan Slabber;[30] two people directly involved in the implementation of the PNE program. This would have been impossible for, e.g., the North Korean nuclear program. Please see table 4.1 for a complete overview of the data that I have used.

6.2. Organisational challenges

The following section will describe, explain and interpret the main organisational challenges at play during South Africa's PNE program. First, this section will elaborate on the previously identified organisational issues: resource support, level of autonomy, information-sharing, and clear and compelling goals. As mentioned earlier in the methodological chapter, this iterative structure facilitates the comparison of similarities and differences between the different cases. It allows this study to advance the accumulation of knowledge on this understudied dimension. Next, this chapter will turn from description to exploration. I will elaborate on the role of the organisational design and on the extrapolations that follow from this case study with respect to the nuclear terrorism threat. This way,

[29] Andre Buys joined the Atomic Energy Board (AEB) in January 1971. He was appointed a research engineer in the Reactor Engineering (RE) Sub-division of the Reactor Development (RD) Division of the AEB at Pelindaba. The RE Sub-division was responsible for the engineering design of the nuclear explosive devices (the nuclear design was done by other subdivisions). He was one of the people transferred to Somerset West in 1972. He returned to Pelindaba in 1976, where he was appointed Head of the RE Sub-division. After the Vastrap nuclear test site was discovered in 1977, the government instructed the AEB to prepare a device for an underground nuclear explosion as a demonstration of South Africa's nuclear capability. He was the leader of the team that designed and built this device that was ready for use in 1979. He personally did the final assembly of the device. He resigned from the AEB and joined ARMSCOR in January 1982. He was appointed Engineering Manager at Kentron Circle and led the team that designed and built the first interim nuclear weapon that was ready for use at the end of that year (1982). He was also the systems engineer for the series-production nuclear weapons that were designed and manufactured during 1982 - 1985 and the Plant Manager of Kentron Circle from 1983 - 1985. After 1985 he was promoted to senior management positions in ARMSCOR.

[30] Johan Slabber went through a number of responsibilities during the entire project. He was the Head of the Reactor Engineering Division which was responsible for the entire mechanical engineering aspects of the device such as the physical design. He tested the structural integrity and internal ballistics during firings of non-nuclear simulations. He machined delicate components including the fissile material taking into consideration the criticality aspects. All these activities were carried out in close collaboration with the Reactor Physics group. Later on, he was made responsible for the entire development that included the various groups i.e., reactor physics, mechanical- , electrical/electronic- , chemical and civil engineering as well as the manufacturing workshops.

this chapter aims to verify the previous insights and to reflect in more depth upon the formulated hypotheses on the relation between the organisational design and the nuclear terrorism threat.

6.2.1. Resource support

This case study supports the idea that sufficient individuals with the necessary *techne* and *metis* are essential in coping with a plot with a high task variability and low task analysability. Even though there were minor allocation and employment challenges, South Africa's specialised and motivated experts were indispensable in effectively completing this technically challenging and clandestine project. Moreover, the personnel enjoyed the support of adequate material resources (e.g. money and non-nuclear components). This was beneficial to their optimal functioning.

The RD division initially consisted of a small group of native South African nuclear scientists and engineers (and a few people seconded from other divisions of the AEB).[31] This group gradually expanded to about 50-100 people over the following years.[32] This number of people is substantially lower than the number of people involved at Los Alamos and comes closer to the size of the adopted nuclear terrorism scenario. Some of these people originally enjoyed training in nuclear science and technology in the U.S. and Europe.[33] Although any unclassified information would in principle not fall under any nuclear agreement for cooperation,[34] some reports suggest that this actually did lead to the acquisition of sensitive information on nuclear explosives by the South Africans.[35] A 1984 CIA report mentions, for instance, that they knew about "at least one South African scientist [who] was in the United States studying the application of PNE's."[36] These people further developed their skills over time via, e.g., the

[31] Andre Buys, "Proliferation risk assessment of former nuclear explosives/weapons program personnel, 8-9; written correspondence with Waldo Stumpf, April 27, 2017. Waldo Stumpf is the former chief of the Atomic Energy Corporation.
[32] Albright and Stricker, *Revisiting South Africa's nuclear Weapons program,* 29.
[33] Written correspondence with André Buys, April 15, 2017; written correspondence with Johan Slabber, August 17, 2017.
[34] Written correspondence with Johan Slabber, August 17, 2017.
[35] Albright and Stricker, *Revisiting South Africa's Nuclear Weapons Program,* 6.
[36] Director of Central Intelligence, *Trends in South Africa's Nuclear Security Policies and Programs,* Declassified version (1984), 8. Available at: https://www.cia.gov/library/readingroom/docs/DOC_0000107420.pdf (accessed on May 18, 2017); Albright and Stricker, *Revisiting South Africa's Nuclear Weapons Program,* 28 mention in this context that: "In 1974 unable to answer certain pressing questions about the gun-type device, an engineer working on it at Somerset West went to the United States to attend a high explosive conference where leading US nuclear weapons experts were to deliver talks. Posing as an employee working on civil high explosives at the Council for Scientific and Industrial Research, South Africa's leading civilian scientific and technology research organisations, he had ample opportunities to ask detailed questions of the US nuclear weapons experts. He was pleased that these experts engaged in discussions with him in which they were frank and helpful." It is not entirely clear whether or not both sources are referencing to the same incident.

Pelinduna project. They were the top nuclear experts in the country at that time.[37] Their high level of specialisation proved to be essential in effectively coping with various nonroutine situations.[38] For instance, little was known about ballistics, explosives and pyrotechnics. Yet, the reactor engineering group succeeded in coping with the "several challenges" that it was confronted with.[39] Moreover, another example is when Johan Slabber's *metis* once foiled a criticality accident. He thereby prevented a potential disruption of the project.[40] Nic von Wielligh explains:

> It was possible to make the assembly more reactive by inserting a control rod into an aperture. The rod was inserted slowly, and, as expected, the locally manufactured counter tubes showed higher counts … the count suddenly started levelling off. One of the researchers slowly pushed the rod in deeper, millimeter by millimeter, but with no result. On impulse, Johan Slabber decided to stop the experiment immediately. This was providential because closer examination revealed that the counter tubes were saturated and had simply stopped counting.[41]

The acquisition, allocation and employment of well-trained and motivated personnel is however not as straightforward as often assumed. There were some minor problems. The RD division personnel was "simply informed" about the PNE program. Yet, there were some people "unwilling to work in this program and transferred to other divisions of the AEB or resigned."[42] This reluctance towards the project is also illustrated by some informed outsiders at the AEB that were critical of the PNE program and the following program led by Armscor.[43] Professional sacrifices, moral doubts, or strategic doubts about the program are often mentioned as reasons for resistance. Moreover, the employment of personnel was complicated by a sensitivity to selecting "responsible and mild-mannered" people. Deploying fanatics might undermine effective coordination and control of the program.[44] The domestically perceived legitimacy of this state endeavor - and a sense of pride in overcoming the multiple obstacles - have catered to these challenges (infra). Yet, these examples do illustrate that the allocation and employment of experts is not without a challenge. This finding was also suggested by the Los Alamos case study.

---

[37] Written correspondence with André Buys, April 15, 2017; written correspondence with Johan Slabber, August 17, 2017.
[38] Interview with Anna-Mart Van Wyk, May 4, 2017. Anna-Mart van Wyk is a senior researcher at Monash University South Africa.
[39] Albright and Stricker, *Revisiting South Africa's Nuclear Weapons Program,* 27.
[40] Von Wielligh and Von Wielligh-Steyn, *The bomb*, 256.
[41] Ibid*.,* 256.
[42] Written correspondence with André Buys, April 15, 2017.
[43] Ibid.
[44] An Armscor manager cited in Albright and Stricker, *Revisiting South Africa's nuclear weapons program,* 98.

In addition, the effective functioning of these experts was facilitated by a satisfactory material resource support. First, there was a satisfactory flow of non-nuclear components. Although security considerations led them to build specialised facilities in a secluded area of the Pelindaba site, they did not move away the machine shop from this large site. This enabled them to draw upon the infrastructure of the main site.[45] Moreover, when South Africa had not already imported non-nuclear components before arms embargoes became effective (e.g. casting furnaces), or these materials were not locally available (e.g. explosives), they often had the skills and support to design and manufacture them locally. This implied the need to improvise.[46] Specifically considering the procurement of non-nuclear components, Johan Slabber noted mysteriously that "there are many ways to skin a cat."[47] Yet, as was also the case during the implementation of Los Alamos, a satisfactory flow of non-nuclear components is not as straightforward as often assumed. Security considerations are continuously at play. Buys, for instance, stated that:

> We were particularly wary of unsolicited offers to supply us with nuclear weapon-specific materials and items (we received many such offers). It cost us a lot more, but we manufactured these items ourselves rather than risk a breach of security.[48]

Second, South Africa's nuclear project also received adequate domestic financial support.[49] This was beneficial to the creation of a favorable operational environment. For instance, while there were various security measures in place (e.g. employees were not permitted to socialize after hours or to give any sign in public that they knew each other),[50] there was also room for a recreational center for the people to relax. These type of measures enable the experts to dedicate themselves to their scientific vocation in a physical and psychological secure and safe manner. Adequate material resource support minimises human frustrations, operational delays, and errors.

[45] Albright and Stricker, *Revisiting South Africa's nuclear weapons program,* 30.
[46] Von Wielligh and Von Wielligh-Steyn, *The bomb*, 268; written correspondence with André Buys, April 15, 2017.
[47] Written correspondence with Johan Slabber, August 17, 2017.
[48] Written correspondence with André Buys, April 15, 2017.
[49] Interview with Anna-Mart Van Wyk, 4th of May 2017. It is illustrative in this context that Von Wielligh, *The Bomb*, 132 notes that South Africa's expenditure on defence made up one-fifth of the total national budget in 1975. Notwithstanding that South-Africa had several (military) projects (e.g. the conventional army, military helicopters, etc.), Anna-Mart Van Wyk clarifies that sufficient money was channelled to the secret nuclear project.
[50] Von Wielligh and Von Wielligh-Steyn, *The Bomb,* 167.

6.2.2. Level of autonomy

Scientists and technicians at the PNE program retained sufficient operational decision-making power while simultaneously complying with the established security measures. This case study supports the idea that experts having control over the operational implementation of the project stimulates the creative and flexible application of knowledge. This is necessary to effectively cope with the nonroutine situations that arise throughout the implementation of this type of project. Yet, while the Los Alamos case suggested that high levels of operational autonomy implied increased divergent behavior by these experts, no similar observation was made while studying the South African PNE program.

The AEB was initially a "research institution and organised like a scientific laboratory."[51] Various security measures were set in place when the PNE program was launched (e.g. the physical isolation of the program, the limited contact with outsiders, or the transport to the facility via blinded vans). Yet, the culture of the RD Division remained "by and large that of a research laboratory."[52] The nine sub-divisions were functionally grouped according to scientific discipline. Scientists and technicians had a lot of discretionary power to select what and how to do their work.[53] There were no tight deadlines.[54] Considering the PNE program was primarily about demonstrating their capability, Johan Slabber noted that "the only objectives were that all the development should be completed when the core (fissile) material became available."[55] There was a clear top-down political decision that approved the development of PNE's, but there was little military or political interference in the RD Division's execution of its work. Laurence Alberts, the AEB Vice President between 1971 and 1977, identified the 1960s and 1970s as years where the "priest with the white coat had more impact than the priest with the black coat." Likewise, Piet Koornhof, minister of minerals and energy from 1972 to 1976, stated that it "would have been unthinkable for him and the other politicians to question the scientists' advice on such technical matter."[56] This level of scientific autonomy fostered creativity and precision. Rational scientific judgement prevailed over strict and autocratic control. As a U.S. State Department official stated: "they came up with their own home-spun technology."[57] André Buys acknowledged that innovation thrives

[51] Written correspondence with André Buys, April 15, 2017.
[52] Ibid.
[53] Ibid.
[54] Interview Anna-Mart Van Wyk, 4th of May 2017; Albright and Stricker, *Revisiting South Africa's Nuclear Weapons Program,* 17.
[55] Written correspondence with Johan Slabber, August 17, 2017; Interview with Anna-Mart Van Wyk, May 4, 2017; Albright and Stricker, *Revisiting South Africa's nuclear weapons program,* 17.
[56] Laurence Alberts and Piet Koornhof cited in Peter Liberman, "The Rise and Fall of the South African Bomb," *International Security* 26, no. 2 (2001): 65; confirmed by written correspondence with Nic Von Wielligh, April 22, 2017.
[57] U.S. State Department official cited in Al Venter, *How South Africa Built Six Atomic Bombs* (South Africa: Ashanti Publishing, 2008), 109.

when people are given the freedom to come up with their own original idea. He gave an illustrative example:

> We needed a state-of-the-art 3D numerically controlled milling machine to manufacture some of the nuclear components that had an extremely complex geometry. We could import such a machine at a very high price. Instead, we gave the problem to the machine shop operators to see if they could find a way of manufacturing the components. To our surprise they came up with a very ingenious solution that cost almost nothing. They were able to modify their current machines to enable it to manufacture the parts. It was a wonderful example of *necessity is the mother of invention.*[58]

The Los Alamos case study suggested that such increased levels of operational autonomy imply an increased risk for friction between scientists, the "we know best syndrome," or "group-think" processes. Allowing for operational control at the level where expertise cumulates was expected to imply a loss of control by the leadership. This could imperil the group's operational effectiveness and security. Yet, remarkable, these dynamics were not observed throughout the implementation of the PNE project. Some issues do hint to the potential risks related to higher levels of operational autonomy (e.g. the aforementioned attention that was given to evading the recruitment of fanatics, or the statement by Buys that "we were just worried as human beings that you make this thing of such tremendous power and you give it to somebody who's not going to be responsible with it").[59] Yet, in general, it seems that little divergent behavior found place throughout the implementation of this nonroutine project. Buys illustratively stated that "we were a small close-knit group that got along very well with each other."[60] Three potential explanations come to mind to explain the lack of divergent behavior.

First, it might have been a result of the resource support for the project and its clear and compelling goals (infra). Both factors might have played a mitigating role with regards to potentially divergent behavior by the experts involved. Second, unlike scientists at Los Alamos, these experts did not invent the technology; more information was available about the required tasks and activities. This potentially alleviated the level of operational ambiguity and fluidity, thereby also alleviating the risk for diverging behavior. Third, the PNE program's relatively small size implies that there are simply less individuals that might display divergent behavior. Notwithstanding the exact reason, this observation thus nuances the

[58] Written correspondence with André Buys, June 24, 2017.
[59] Interview with André Buys by Michael Montgomery, 'Building the South African Bomb' (2008). Available at: https://www.revealnews.org/article/building-the-south-african-bomb/ (accessed on June 7, 2017).
[60] Written correspondence with André Buys, April 15, 2017; written correspondence with Johan Slabber, August 17, 2017.

previous claims that operational autonomy leads to an increased risk for divergent behavior (which could imperil the group's operational effectiveness and security). This will be taken into account when extrapolating these insights to the probability of nuclear terrorism.

6.2.3. Information-sharing

South Africa's PNE program was characterised by a flexible "need-to-know" policy. This coordination and communication system was less organic compared to the coordination and communications tools at Los Alamos. Yet, the flexible nature of this "need-to-know" policy did stimulate the combination of knowledge and did motivate the people involved in the PNE program. It thus benefitted the effective implementation of the project. Furthermore, however, this case study simultaneously provided support for the idea that such increased levels of information-sharing might be hard to reconcile with a group's clandestine operational environment.

South Africa's PNE program was secret. One of the established security measures was the introduction of a "need-to-know" policy.[61] Explained to all personnel when initially informed, this policy entailed that "only formally 'informed-about-the-program' personnel may receive classified information and then it shall be limited only to that required to enable the receiver to do his or her job."[62] Yet, this "need-to-know" policy was relatively lenient in practise. Everyone that "was 'informed-about-the-program' knew the overall goal and the details of his/her own work."[63] Both formally scheduled meetings and more informal and interpersonal ad hoc communication enabled coordination within the different groups and between the people in different groups in the RD Division. Showing them that they were trusted motivated the personnel.[64] Moreover, this flow of information enabled the creative combination of knowledge and experience. For instance, Buys stated:

> If you needed information for the work you were doing, you simply went to the office of the holder of the information and asked for it. You might even spend some time with him/her to discuss it. This type of communication was deemed very important and was encouraged… this communication was within and between people in the different groups and/or with other

[61] Written correspondence with André Buys, April 15, 2017; written correspondence with Johan Slabber, August 17, 2017; written correspondence with Waldo Stumpf, April 27, 2017.
[62] Written correspondence with André Buys, June 24, 2017.
[63] Ibid.
[64] Ibid.

groups/organisations. The only two criteria were that everyone involved must be "informed-about-the-programme" and there was a need for the sharing of the information.[65]

Moreover, the experts involved in the PNE program could also potentially consult outside help. Scientists needed to send a motivated request to inform an outside source about the program in case they required information from that source. A select few outside the RD Division were thus informed about the purpose of the project. These people first needed a security clearance. Buys stated in this context that "of course this entailed a burden (you had to keep track of them) and a security risk, and therefore it was carefully considered before it was approved."[66]

This touches upon the fact that this case study simultaneously provided support for the idea that information-sharing might be hard to reconcile with a group's clandestine operational environment. The PNE program established various security measures (e.g. only native-born South African citizens could acquire security clearances). Yet, there were nevertheless various security breaches throughout the implementation of this project. A higher level of information-exchange inherently raises the security risks for any clandestine project. Buys illustratively mentions an incident where top secret documents were lost in a public space and an incident of a defected AEB employee.[67] Although this employee had limited access to information because he did not work at the RD Division, he did tell the CIA about the existence of the PNE program in the 1970s.[68] Comparing this to Los Alamos, Buys said this was "our Klaus Fuchs."[69] Likewise, Dieter Gerhardt - a commodore in charge of the Simonstown naval base – sold secrets to the Soviet Union. His motivations remain unclear, but he is, e.g., often linked to the USSR's detection of the planned cold test at the Vastrap site in 1977.[70] While it is unclear how he obtained the information exactly, Von Wielligh suggest he "drew his own conclusions" after the navy was requested to provide a gun barrel.[71] Thus, increased levels of information-exchange strengthened the project team's adaptivity and creativity. Yet, it simultaneously complicated the concealment of their nuclear endeavours. Not surprisingly, the international community had substantial suspicions about South Africa's nuclear project.

[65] Written correspondence with André Buys, June 24, 2017.
[66] Ibid.
[67] The lost documents were eventually retrieved without any security breach after a team of security personnel did a house-to-house search in the area.
[68] Written correspondence with André Buys, April 15, 2017.
[69] Ibid.
[70] Von Wielligh and Von Wielligh-Steyn, *The bomb*, 143.
[71] Ibid., 143.

6.2.4. Clear and compelling goals

Clear and compelling goals strengthened the effective implementation of the project. A clear goal sharpened the focus of the project while a compelling goal inspired the individuals involved in rallying around the project. Both go hand-in-hand. Both are important tools in coping with the aforementioned security risks. Yet, the implementation of the PNE program illustrated that the formulation of clear but uncompelling goals might actually undermine the operational security of the program. This is similar to the dynamics that I have identified during the implementation of Los Alamos.

The South African PNE program enjoyed a clear operational focus. The intent of the project was to demonstrate a nuclear capability; not to develop a large arsenal of nuclear weapons. In doing so, they were going to focus on the first generation of gun-type nuclear devices. Some basic research and development studies were done, but neither the integration of an delivery system nor the development of implosion-type or fusion-type nuclear devices was a priority for the RD Division.[72] As previously explained, this operational goal was clear to the experts involved in the PNE program. Once a person was appointed, he or she was "informed about the program and that it was classified secret."[73] While they might not have known everything about the program, this clear goal enabled them to steadily progress and remain motivated. Scientists and technicians in the PNE program demonstrated perseverance and patience to the tasks at hand.

Next, the South African project PNE program was in general characterised by having established compelling goals to the people involved. Experts had to remain professionally unknown, could not travel overseas, and had a secret life for friends and family.[74] Yet, they were very motivated to build the bomb.[75] They often displayed a "laager" mentality. The more criticism and sanctions they received, the more determined they were to stand alone.[76] After opening its doors to the IAEA inspection, an U.S. State Department official stated that: "these guys were immensely proud of what they achieved under sanctions."[77] Within Afrikaner culture, there is a strong sense of a "can-do attitude." Buys explained that "it was like a game of chess, every move the international community made was answered by a counter move."[78] Although some worried, for instance, about the responsible use of these explosive devices,

[72] David Albright, "South Africa's secret nuclear weapons," Report by the Institute for Science and International Security (1994).
[73] Written correspondence with André Buys, April 15, 2017.
[74] Ibid.
[75] Written correspondence with Johan Slabber, August 17, 2017.
[76] Von Wielligh and Von Wielligh-Steyn, *The bomb*, 123.
[77] U.S. State Department official cited in Venter, *How South Africa Built Six Atomic Bombs,* 109.
[78] Written correspondence with André Buys, April 15, 2017.

they generally seemed convinced about the legitimate nature of this endeavor. As was the case during Los Alamos, it seems that achieving these type of compelling goals was actively pursued. For instance, Prime Minister P.W. Botha ended his opening speech of the Kentron Circle facility by presenting a commemorative plaque which read: "For all South Africans."[79] This type of clear and compelling goals strengthened the organisation's patience and perseverance. It was beneficial to the surmounting of unexpected obstacles and the maintaining of group cohesion.

Yet, the case of the defected AEB member or the spy activities by Dieter Gerhardt illustrate that not everyone was convinced by the operational and organisational goals of this project. These persons were not directly involved in the RD Division and their motivations remains unclear (e.g. ideologically inspired or financially driven). Yet, these examples do illustrate that any (well-) informed individual holds the potential to undermine the effectiveness and security of the plot. This underlines the idea that – even though this project was generally characterised by a high level of coherence, focus and perseverance - any clandestine organisation continuously needs to take into account the risks related to the defection of a member of the plot or the detection of (a part of) the plot by an adversary.

6.3. South Africa's PNE program: various features of an organic design

This chapter will now turn from description to exploration. Similar to the previous case study, this case study demonstrated that the organisational design shapes some of the main organisational challenges to the implementation of a nonroutine project. The following section will not yet extrapolate insights to a potential nuclear terrorism plot. Yet, it will link the four organisational dimensions – and its challenges – to the organisational design. I will elaborate on how the organisational design influenced the implementation of the PNE program.

To be precise, I will argue that the PNE program was characterised by an organisational design with various features of an organic organisational design (see table 6.1). Although the organic nature of its organisational design was not as intense as Los Alamos' organic organisational design, this type of design did also benefit the effective implementation of this nonroutine plot. Moreover, in general, this case study also illustrated that this type of organisational design did simultaneously imply increased security risks. Yet, the PNE program leads us to further refine and add nuance to this argument.

[79] Albright and Stricker, *Revisiting South Africa's Nuclear Weapons Program,* 92.

Table 6.1. Organisational design of the PNE program

	Organisational design of the PNE program
Level of interconnectedness	Sufficiently high number of intra-division and inter-division connections
Level of hierarchy	Sufficiently high level of control over operations by experts themselves + sufficient resource support to them.
Level of specialisation	High level of personal specialisation (high levels of both techne and metis)

* Note that this table is inherently arbitrarily to some extent. It is difficult to assign exact and uniform values to these design parameters.

The type of specialisation has a strong impact on the control and coordination over the different job positions. I therefore elaborate on this issue first. Similar to Los Alamos, it is clear that the effective implementation of the PNE program required individuals with a high level of personal specialisation. The South African nuclear program enjoyed the participation of the top nuclear experts in the country at that time. They were well-trained and had the necessary *techne* and *metis* to cope with the various unexpected problems that were difficult to analyse beforehand (e.g. the example of 3D numerically controlled the milling machine). The South African project was not characterised by the implementation of breakthrough technology; it was characterised by a less intense nonroutine nature of technology. Yet, access to these top nuclear experts was nevertheless of great importance to this program's effective implementation.

Second, also similar to Los Alamos, these experts were able to operate at a high functional capacity. On the one hand, there was a clear and convincing top-down decision to pursue a nuclear capability. Moreover, the leadership also provided the necessary resource support to the personnel involved in the program. On the other hand, scientists and technicians in the PNE program had sufficient operational decision-making power and control over the implementation of the project. As mentioned before, the RD Division remained "by and large that of a research laboratory."[80] There was little hierarchical top-down interference in the RD Division's execution of its work. For instance, there were no tight goals and deadlines, nor was the coordination and control over the different technical tasks and activities established via strict rules and specifications. This was beneficial to the team's flexibility, creativity and adaptability. It moreover stimulated the individual experts' intrinsic motivation and dedication to their tasks and activities.

[80] Written correspondence with André Buys, April 15, 2017.

Finally, and closely related, there were sufficient intra-division and inter-division connections. The PNE's program flexible "need-to-know" policy implied that the flow of information was less organic compared to the flow of information at Los Alamos. Yet, ultimately, the program was characterised by sufficient formal and informal moments of communication and coordination. Information-exchange between different subdivisions within the RD Division was encouraged. There was sufficient lateral communication and consultation. This organic organisational design feature enabled the creative combination of knowledge and experience. This increased the capability of the personnel to effectively cope with the nonroutine and interdependent tasks and activities that arose throughout the implementation of this program.

The South African PNE program was thus characterised by various organic design features. Although not as organic in nature as the organisational design of Los Alamos, this type of organisational design benefitted the effective implementation of this nonroutine plot. It is a problem-solving design. Moreover, in general, this case study simultaneously supports the idea that such an organisational design implies increased security risks. Yet, going beyond the Los Alamos case study, the PNE program enables us to further refine and add nuance to this argument.

Considering the Los Alamos case study, it was suggested that the increased security risks are a product of each of three organisational design features. First, it was argued that the need to recruit and employ experts in a clandestine operational environment inherently implies increased security risks. Not just everyone can complete the required tasks. Any failed recruitment effort, or the mere involvement of these particular people with specialised skills, might imply detection by counterterrorism forces. Second, a higher level of operational autonomy entails a higher level of ambiguity and fluidity. There is a lack of centralised control. This increases the likelihood of divergent behavior. This – on its turns – can imperil the group's security. Any instance of an operational error, delay or defection might give rise to the detection or interruption of the project. Finally, a higher number of interconnections inherently implies a higher risk of detection by counterterrorism forces. Any communication and coordination tool inherently implies a security risk. It provides the adversary with the opportunity to detect or infiltrate the project.

Yet, the PNE program leads us to further refine and add nuance to this argument that an organic organisational design implies increased security risks. To be precise, the increased security risks were primarily a result of the challenges related to the recruitment and employment of experts and the increased number of interconnections between these experts. These security risks are respectively illustrated by the AEB employee whom defected to the USA, the case of Dieter Gerhardt, or the loss of

top secret documents. It was remarkable, however, that we did not observe an increase in divergent behavior by the operationally autonomous scientists and technicians that were involved in the PNE program. We expected to notice an increase in divergent behavior due to the decreased control over the experts' actions. This, on its turn, could lead to increased security risks. Yet, the South African project team succeeded in forming a "close-knit group that got along very well with each other." Unlike during the implementation of Los Alamos, there was no increase in divergent behavior during the implementation of the PNE program. This observation will need to be taken into account when extrapolating relevant insights from this case to the probability of nuclear terrorism.

6.4. Extrapolations to the nuclear terrorism threat

This final section turns from description to exploration. There remain differences between the PNE program and the adopted nuclear terrorism scenario (i.e. the PNE program remains a state nuclear project; the exact tasks and activities are not identical). These differences will be taken into account while extrapolating relevant insights from this case study to the probability of nuclear terrorism. This way, we aim to verify and reflect upon the plausibility of the previously sketched effectiveness-efficiency trade-off; we generally aim to better understand the nuclear terrorism threat. In order to accumulate knowledge on this understudied dimension, this section follows the same structure as used in the previous chapter. I will highlight new insights when necessary.

6.4.1. Effectiveness…

The first hypothesis focused on the fit between the organisational design and a nonroutine nature of technology. This case study supports the plausibility of the expectation that a terrorist organisation is most likely to effectively complete a nuclear terrorism project by means of an organisational design similar to an organic organisational design (=H1). The findings of this case study are in line with what we have observed during the implementation of Los Alamos. The effective implementation of the PNE program benefitted from its access to individuals with the necessary skills, the level of operational control these experts enjoyed, and the possibility for them to exchange information. These organic organisational design features enabled the team to cope with a high task variability and low task analysability.

Various specialised and motivated experts were involved in the implementation of the PNE program. The program was not characterised by the implementation of breakthrough technology. Yet, the individuals' *techne* and *metis* was essential in coping with the various unexpected situations that arose throughout its implementation. Thus, considering that we expect that a diversity of skills and expertise would be necessary in the adopted nonroutine nuclear terrorism scenario (e.g. clandestine procurement skills, nuclear physics, advanced military skills, explosives and ballistics experts, illicit trafficking experts, financial experts, etc.), it remains plausible to attach much importance to the availability of a sufficient number of experts throughout the implementation of such a plot. The development of a 100 ton nuclear explosion would imply lower demands in terms of the required expertise than the creation of a 15kT explosion. Yet, it seems to hold true that experts with the necessary techne and metis can be expected to be of essential importance in effectively completing any nonroutine nuclear terrorism plot.

Next, the PNE program also supports the idea that these experts' functional capacity and effectiveness can be expected to rise if they can operate in an organic-like organisational design. On the one hand, this implies that the leadership should provide sufficient material resource support and formulate clear and compelling common goals. This way, political and ideological leadership can focus and support a terrorist group's implementation efforts. Moreover, on the other hand, an appropriate organisational design should also allow for sufficient levels of scientific autonomy and information-sharing. The example of Johan Slabber's expertise that foiled a criticality accident illustrated that it is best to allow for operational control to the specialised experts. That increases the likelihood that these experts can effectively complete a nonroutine project. It thus remains plausible to expect that a nuclear terrorism would also best allow for sufficient discretionary control to the experts involved. Any unnoticed security measure, technical hick-up or other contingent factor can complicate matters throughout the implementation of a nuclear terrorism plot. Experts with sufficient discretionary power are more likely to effectively cope with such unexpected situations. Moreover, sufficient intra- and inter-cell connections can be expected to benefit the effective implementation of a nonroutine project. The PNE program enjoyed sufficient connections both within and between the different functional subdivisions in the RD Division. It remains plausible to expect that a terrorist organisation will also need sufficient interconnections. For instance, terrorists that need to design and construct the nuclear device will need to be aware of the type of fissile material that has been acquired and might, on its turn, need to inform illicit traffickers about the characteristics of the required nuclear and non-nuclear components. More interconnections are thus expected to increase the likelihood that they can effectively implement a nonroutine nuclear terrorism plot.

The exact tasks and activities of the PNE program are not identical to those of the adopted nuclear terrorism scenario. Yet, in general, it is clear that the PNE program's organisational design strengthened its effective implementation. It therefore remains plausible to assume that that this type of organic organisational design would also increase the likelihood that a terrorist organisation could effectively implement a nonroutine nuclear terrorism plot. The support for this hypothesis is particularly relevant because the PNE program was more akin to the adopted nuclear terrorism scenario. The increased analogy between this case and the adopted nuclear terrorism scenario strengthens the support for this argument.

6.4.2. Versus efficiency

An organisational design similar to an organic organisational design is thus still expected to increase the likelihood that a terrorist organisation can effectively complete a nuclear terrorism project. Yet, building on this case study, it simultaneously remains plausible to expect that this institutional configuration would imply substantial security risks to the terrorist organisation (=H2). Moreover, this case does not provide any reason to theoretically refute the plausibility that a nuclear terrorism plot can be perceived to be an inefficient strategy for them (=H3).

First, considering the fit between the organisational design and a group's clandestine operational environment, the Los Alamos case study led me to suggest that each of the three organisational design features entails increased security risks. This case study generally supports the plausibility of the idea that an organic organisational design implies increased security risks to a nuclear terrorism plot (=H2). Yet, insights from the PNE program further refine and add nuance to this argument. To be precise, considering that the higher level of operational autonomy did not entail more divergent behaviour throughout the implementation of the PNE program, it appears that we need to remain cautious in expecting that a higher level of operational autonomy would imply increased security risks to a nuclear terrorism plot.

Indeed, reflecting upon the three aforementioned reasons that may explain the lack of divergent behaviour throughout the implementation of the PNE program (6.2.2. level of autonomy), it becomes clear that these reasons might also be applicable to a nuclear terrorism plot. The loss of operational control over the experts does therefore not necessarily imply an increase in divergent behavior. First, a terrorist organisation may decide to invest various resources in a nuclear terrorism plot and successfully rally its personnel around this project. A terrorist organisation's ideology might, for instance, lead to a

"can-do attitude" and increased loyalty to the organisation. Second, the technical requirements to a nuclear terrorism plot might be less demanding as those that needed to be surmounted during the implementation of Los Alamos or the PNE program. This might result in a less nonroutine nature of technology. This, on its turn, might alleviate the project's ambiguity and corresponding level of divergent behaviour. Finally, closely related to the latter remark, it might be the case that a nuclear terrorism project requires a relatively small project team. This will depend upon the exact nuclear terrorism scenario. A lower number of people involved in such a plot would inherently reduce the likelihood of divergent behaviour. We thus need to remain cautious about expecting an increase in divergent behaviour by operationally autonomous experts. It follows that we should also remain cautious about expecting an increase in security risks as a product of such diverging behaviour.

Yet, notwithstanding this observation, this case study does lend support to the suggestion that the two other organic organisational design features imply increased security risks. The security breaches during the PNE program were primarily a result of the challenges related to the recruitment and employment of experts and the information-exchange between these experts. This is illustrated by the loss of top secret documents, the defected AEB employee, and the case of Dieter Gerhardt. Not surprisingly, the international community had substantial suspicions about South Africa's nuclear program. These security breaches are of particular relevance because the number of people involved in the PNE program comes closer to the size of the adopted nuclear terrorism scenario. It therefore becomes more plausible to expect that these issues would also be applicable to a nuclear terrorism plot. As Kenney already suggested, the recruitment or training of individuals with the necessary techne and experiential know-how becomes more complex in a hostile operational environment.[81] Moreover, every connection with other members of the group provides an opportunity for counterterrorism forces to disrupt the plot. Both the issues of detection and defection are likely to be of particular concern to a terrorist organisation aiming to hide a nuclear terrorism plot. An organic organisational design would only exacerbate these concerns. It therefore remains - in general - plausible to assume that an organic organisational design would be an *inefficient* way for a terrorist organisation to guarantee the security of its nuclear terrorism plot.

Second, I will briefly make some provisional comments with respect to the match between a nuclear terrorism plot and a terrorist organisation's strategic-political goals (=H3). Yet, as previously indicated, the inherent differences between a state nuclear project and non-state nuclear project imply that the

[81] Michael Kenney, "'Dumb' Yet Deadly: Local Knowledge and Poor Tradecraft Among Islamist Militants in Britain and Spain, *Studies in Conflict & Terrorism* 33, no.10 (2010): 915.

last two case studies (of actual nonroutine terrorism plots) will be of primary importance in assessing this hypothesis.

Similar to Los Alamos, it is worthwhile to highlight in this context that the South African PNE program enjoyed a particular level of domestic and international legitimacy. Notwithstanding the exact drivers behind South Africa's nuclear proliferation (e.g. security incentives, organisational politics, or international pressure and state sensitivity to such pressure[82]), it became clear that they had access to the taxpayer's money, a well-established and motivated nuclear skills base, and a well-operating infrastructure. They enjoyed a particular level of domestic legitimacy. Mobilisation of these kind of resources would probably be a more daunting task for a terrorist organisation. Moreover, even if Pretoria was increasingly isolated, and extensive nuclear embargoes and boycotts were imposed, international pressure was often specifically predisposed to the apartheidsregime.[83] Pretoria did remain of strategic importance to the West in the context of the Cold War. Not every potential action has been taken to prevent South Africa from obtaining a nuclear capacity. There were substantial suspicions about South Africa's nuclear program. Yet, the international community never attacked, for instance, the South African nuclear facilities. This would probably not be true for a terrorist organisation. It can be expected that the smallest hint to the development of a nuclear terrorism plot would trigger a more vigorous counterterrorism response. The terrorist equivalent of Dieter Gerhardt could be disastrous for a group's nuclear terrorism plot and – potentially - its survival. A terrorist organisation might give more relative weight to these kind of considerations.

6.5. Conclusion

The South African PNE program was the second case study that I have selected to explore the plausibility of the suggested hypotheses with respect to nuclear terrorism threat. This program was theoretically relevant because it was characterised by a nonroutine nature of technology. Moreover, it is one of the few state nuclear project more akin to a nuclear terrorism project. This increases the analogy between this case and the adopted nuclear terrorism scenario. This way, this case study formed a new piece of the puzzle in better understanding the nuclear terrorism threat.

[82] For a detailed discussion on the drivers behind South Africa's nuclear armament and disarmament, please see Liberman, "The Rise and Fall of the South African Bomb."
[83] Ibid.

In general, this case first affirmed the relevance of the organisational design in adopting a nonroutine project. This is in line with the findings that followed from the Los Alamos case study. It subsequently supports the expectation that the organisational design will also impact the implementation of a nuclear terrorism plot. Next, more specifically, this case study does not provide us with any reason to theoretically refute the plausibility of the suggested effectiveness-efficiency trade-off. The PNE program supports and adds nuance to this idea. On the one hand, it remains plausible to assume that a more organic organisational design increases the likelihood that a terrorist organisation can effectively complete a nuclear terrorism plot. This type of design allows for the necessary flexibility, creativity and adaptability to effectively cope with the nonroutine nature of technology. On the other hand, it remains - in general - plausible to assume that this type of organisational design would simultaneously imply increased security risks. The PNE program supports and further refines this argument. To be precise, it remains possible that a security breach would follow from divergent behavior by the operationally autonomous experts. This will depend to a large extent on the exact nuclear terrorism scenario (and its exact nonroutine nature of technology). Yet, this case study suggests that security breaches might be more likely to stem from the challenges related to the recruitment and employment of specialised personnel and a higher level of connections and information exchange between these experts. This might also hold true for a nuclear terrorism plot and will need to be taken into account in the cross-case analysis (chapter 9).

The PNE program thus generally strengthens the plausibility of this study's theoretical propositions and hypotheses. Yet, there remain differences between this state nuclear program and the adopted nuclear terrorism scenario. This might impact, e.g., the organisation's access to resources, the loyalty of the experts involved, and the adversary's efforts to counter the project. These type of issues are difficult to study via a case study of a state nuclear program. I therefore now turn to a third case study: Aum Shinrikyo's chemical and biological armament activities. Studying a nonroutine project by an actual terrorist organisation might provide us with more insights on these type of issues. It enables us to reflect upon whether or not similar organisational dynamics and challenges were also at play during the implementation of a nonroutine project by an actual terrorist organisation.

7. Case study: Aum Shinrikyo's chemical and biological armament activities

The third case study that has been selected to explore the plausibility of the suggested hypotheses is a nonroutine project implemented by an actual terrorist organisation: Aum Shinrikyo's chemical and biological (CB) armament activities.[1] This way, we go beyond the two case studies of a state nuclear project. The analysis of an actual nonroutine terrorism plot might reveal new insights or qualifying conditions with regards to the previous theoretical extrapolations. Moreover, this case study is of particular importance to the assessment of the plausibility of the third hypothesis. Thus, in general, this case study will provide us with a next piece of the puzzle. It will enable us to better understand the nuclear terrorism threat.

Politics were separated from religion in Japan after World War II. Freedom of religion was guaranteed. This led to the emergence of many new religions.[2] Founded in the mid-1980's, Aum Shinrikyo was one of these new religious groups in Japan.[3] Characterised by a sentiment that "modern society has lost its way, and that therefore new paradigms are needed to cope with the demands of modernity,"[4] these groups often attracted a high number of young and idealistic people dissatisfied with the materialism and rigid structures of Japanese society.[5] These organisations frequently espoused catastrophic millennialist themes.[6] Aum initially proclaimed that such disaster could be avoided through spiritual action. Members had to follow the leadership of Shoko Asahara. This charismatic guru – who claimed to have achieved supreme enlightment - was Aum's focal point of authority and inspiration.[7] Yet, Aum gradually subsumed in a more radical apocalyptic doctrine. First propagating beliefs in a more dualistic battle between Good and Evil, Asahara increasingly gravitated towards prophesizing the coming Armageddon. Individual salvation was only possible through reaching Shambhala, an utopia of enlightened beings.[8] Aum members were thus encouraged to become *Shukkesha* (renunciates). They would need to give up their worldly status, leave their family, sign over their property to Aum, and

[1] Large sections of this chapter are published in: B. Volders, "Building the bomb: a further exploration of an organisational approach to nuclear terrorism" *Terrorism & Political Violence,* 2019.
[2] David Kaplan and Andrew Marshall, *The Cult at the End of the World: The Incredible Story of Aum* (United Kingdom: Arrow, 1997), 11.
[3] Ian Reader, *A Poisonous Cocktail? Aum Shinrikyo's Path to Violence* (Great Britain: NIAS Press, 1996), 12; Philippe C. Bleek, "Revisiting Aum Shinrikyo: New Insights into the Most Extensive Non-State Biological Weapons Program to Date." *Nuclear Threat Initiative* 2011. http://www.nti.org/analysis/articles/revisiting-aum-shinrikyo-new-insights-most-extensive-non-state-biological-weapons-program-date-1/ (accessed on March 22, 2017).
[4] Reader, *A Poisonous Cocktail,* 13.
[5] Reader, *A Poisonous Cocktail*; Kaplan and Marshall, *The Cult at the End of the World.*
[6] Reader, *A Poisonous Cocktail,* 13.
[7] Ibid., 12-14.
[8] Frances Flannery, *Understanding Apocalyptic Terrorism: Countering the Radical Mindset* (United Kingdom: Routledge, 2016), 217-222.

undertake "a severe path of austerity, fasting, meditating, yogic practices, and living in communal rural setting."[9]

Next, claiming that spiritual action alone was not enough, Aum decided to participate in the 1990 elections. They were, however, unsuccessful. They were not elected. This might have been the trigger for its shift from apocalypse survival to apocalypse initiation.[10] Aum increasingly perceived a need for self-protection. It even started to welcome the final Armageddon as a joyous event that would illustrate the triumph of Aum.[11] This evolution towards a more radical apocalyptic doctrine was accompanied by a growing degree of conflict between Aum Shinrikyo and outside society.[12] Asahara increasingly infused the group's thinking with conspiracy theories against Aum. Becoming more hostile towards outside society, and simultaneously feeling threatened by it, Reader notes that: "Aum was not just prophesying turmoil, destruction and Armageddon: it was making practical plans to help bring them about."[13] In doing so, Aum was driven by an extraordinary interest in futuristic technology.

Aum pursued a broad range of weaponry (e.g. Kalashnikovs, a laser gun, or nuclear weapons). Yet, the organisation is best known for its chemical and biological (CB) armament activities. Aum has officially been assigned to the launch of 17 terrorism plots that included CB weapons or agents between 1990 and 1995. This included the use of, e.g., Sarin, VX, anthrax, and botulinum toxin.[14] The motivation behind these attacks ranged from assassination to mass murder.[15] Although Aum enjoyed the protected status of a religious organisation, many of these plots were a failure.[16] Yet, some of these attacks did result in a substantial number of casualties. While its 1994 attack in Matsumoto led, e.g., to 7 deaths, its most lethal attack was its March 1995 Sarin attack. Five pairs of highly placed members boarded different subway trains with a small package containing a liquid form of Sarin. They punctured these bags with

[9] Reader, *A Poisonous Cocktail*, 25.
[10] Bleek, "Revisiting Aum Shinrikyo"; Adam Dolnik, "Aum Shinrikyo's path to Innovation," in Maria Rasmussen and Mohammed Hafez (eds.), *Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators," Defense Threat Reduction Agency Workshop report* (Defense Threat Reduction Agency, 2010), 126; John Parachini and Katsuhisa Furukawa, "Japan and Aum Shinrikyo," in Robert Art and Louise Richardson, *Democracy and Counterterrorism: Lessons from the Past* (Washington DC: United States Institute of Peace Press, 2007), 538.
[11] Dolnik, "Aum Shinrikyo's path to Innovation," 126; Parachini and Furukawa, "Japan and Aum Shinrikyo," 538; Reader, *A Poisonous Cocktail*, 70-71.
[12] Reader, *A Poisonous Cocktail*, 14-15, 23.
[13] Ibid., 70-71.
[14] Tim Ballard et al., "Chronology of Aum Shinrikyo's CBW Activities" (Monterey: James Martin Center for Nonproliferation Studies, 2005).
[15] Ibid.
[16] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006), 277. Hoffman explains, for instance, that Aum failed to make any casualties by means of botulinum toxin on at least 9 occasions. This was mostly due to insufficiently toxic agents or malfunctioning dissemination devices.

their umbrellas. The subways trains came together in the Kasumigaseki-station. Several governmental and law enforcement agencies were located nearby. This way, Aum Shinrikyo murdered 13 people and wounded several thousands of people.[17] This type of attack entails the potential to cause mass casualties. Yet, various reports mention that Aum was primarily interested in diverting attention from a pending police intervention via this attack.[18]

In what follows, this chapter will be structured according to a similar theory-generating narrative to the previous chapters. Following a similar structure facilitates the cross-case analysis in chapter nine. First, I will explain why Aum's CB armament activities are relevant to this research project. Next, I will elaborate on the four previously identified organisational dimensions: resource support, level of autonomy, level of information-exchange, and clear and compelling goals. Third, turning from description to exploration, I will reflect upon the role and impact of the organisational design throughout the implementation of Aum's CB activities. Finally, this chapter will extrapolate relevant insights to the formulated hypotheses and theoretical propositions on the nuclear terrorism threat. Considering this case study is a new piece of the puzzle, it might reveal new insights or qualifying conditions with respect to the previous theoretical extrapolations.

7.1. The relevance of Aum Shinrikyo's CB activities

Aum Shinrikyo's CB armament activities have been selected as a case study for this research project because they were characterised by a nonroutine nature of technology. This shared organisational feature is the basis for this study's extrapolations with respect to the nuclear terrorism threat. This case is theoretically relevant. Moreover, this is the first case study of an actual nonroutine *terrorism* plot. This case can probably be considered to be the case that is most analogous to the adopted nuclear terrorism scenario. This way, this case study enables us to better assess and understand the extrapolations and qualifying conditions identified in the previous case studies.

---

[17] Holly Fletcher, "Aum Shinrikyo, " *Council on Foreign Relations,* 2012. Available at: http://www.cfr.org/japan/aum-shinrikyo/p9238#p2 (accessed October 18, 2016). Note in this context that Hoffman, *Inside Terrorism,* 277 stated that nearly three-quarter of the casualties were in fact treated for shock, emotional upset, or some psychosomatic symptom. The number of people physically injured or harmed was lower than is widely believed.

[18] David Kaplan, "Aum Shinrikyo," in Jonathan B. Tuckers (ed.), *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (Cambridge: MIT Press, 2000), 303; Jean Pascal Zanders et al., "Risk Assessment of Terrorism with Chemical and Biological Weapons," in SIPRI yearbook (ed.), *Armaments, Disarmament and Security* (Sweden: SIPRI, 2000), 538.

The challenges to weaponising different forms of WMD's cannot be lumped together. It is clear that Aum's exact operational tasks and activities were not identical to those of the adopted nuclear terrorism scenario.[19] Nevertheless, weaponising CB agents in a clandestine environment did lead to a similarly high task variability and low task analysability. On the one hand, this was a result of the technical challenges that are related to retrieving, processing and disseminating chemical or biological agents. Various unexpected issues arose throughout this process. An accidental chlorine leak in Aum's chemical production facility, the use of a nonvirulent strain of a biological agent, or a malfunctioning dispersal device illustrate this case in point.[20] On the other hand, the nonroutine nature of technology was also a result of Aum's clandestine operational environment. Admittedly, Aum enjoyed the protected status of a religious organisation. Moreover, Japanese law enforcement agencies did not pursue Aum aggressively due to a lack of strong leadership and a strong dependence on confessions.[21] This might have limited the number of exceptional situations throughout the implementation of Aum's plots (see figure 4.1). Yet, Aum continuously needed to take into account the illegitimate nature of its CB armament activities. An indicative example is the dismantlement of its Sarin production facility after Sarin precursor chemicals were detected by law enforcement authorities. This fact - and the fact that a pending police raid forced Aum to act quickly - caused the Sarin strain that was used in the 1995 Tokyo attack to be a third as strong as intended.[22] Likewise, Reader notes that an incident in July 1993 led to local residents complaining "to the police of foul-smelling gases in the vicinity of an Aum facility at Kameido."[23] This type of unexpected problems that are difficult to analyse beforehand led to a nonroutine nature of technology. This was the most important criteria to select this case.

Yet, case selection was based on three other reasons as well. First, the two previous cases were state nuclear projects. This inherently implies differences with a non-state nuclear project. Aum Shinrikyo, in contrast, is one of the few cases of an actual *terrorist* organisation that implemented a WMD program. The number of people involved was relatively low. Estimates range from a few dozen people, over 30

[19] Biological weapons are based on disease-causing microbes and toxins produced by living creatures. Chemical weapons are based on man-made toxic chemicals. In order to cause a high number of casualties, biological and chemical agents would need to be weaponised. The toxic substance would need to be processed and combined with a delivery system (e.g. aerosol delivery). This can be compared to a bullet that needs a cartridge and rifle to deliver it. If not, it is just a lump of lead. The exact technical requirements to build an effective CB weapon differs from agent to agent. For a more detailed explanation, please see Tucker, *Toxic Terror,* 3-9.

[20] Dolnik, *Aum Shinrikyo's path to innovation,* 127-129; Jonathan Tucker, *War of Nerves: Chemical Warfare from World War I to Al-Qaeda* (New York: Random House inc. 2007), chapter 17; William Rosenau, "Aum Shinrikyo's Biological Weapons Program: Why Did It Fail?," *Studies in Conflict & Terrorism* 24, no. 4 (2001): 292-293.

[21] Tucker, *War of Nerves,* chapter 17.

[22] Gavin Cameron, "Multi-Track Microproliferation: Lessons from Aum Shinrikyo and Al Qaida," *Studies in Conflict & Terrorism* 22, no. 4 (1999); Parachini and Furukawa, "Japan and Aum Shinrikyo," 543; Anthony Tu, "What Were the Real Objectives of Aum Shinrikyo?" *CBRNE terrorism newsletter* 41, (2012): 6.

[23] Reader, *A Poisonous Cocktail*, 77.

to 40 people, to "five to ten leaders, while the entire program including the assistants consisted of about 50-80 persons."[24] The nature and size of this plot was therefore more analogous to the adopted nuclear terrorism scenario. Second, case selection was also based on the availability of reliable information. It is true that much information remains unavailable. Yet, it is nevertheless one of the best-documented cases of a terrorist organisation actually implementing a WMD program. This strengthens the plausibility of my empirical observations. Third, as will become clear, Aum Shinrikyo was characterised by an organisational design with various mechanistic features. This allows us to reflect upon – what the hypotheses would suggest to be – a mismatch between the organisational design and the technology that the organisation aims to adopt. Indeed, at first sight, this case seems to contradict our expectation that a terrorist organisation would need an organic organisational design to increase its effectiveness; Aum succeeded in causing substantial casualties. Yet, as will become clear throughout this chapter, "the novelty of Aum's activities has, in fact, obscured the crudeness and ultimate failure of many of them."[25]

7.2. Organisational challenges

The following sections will describe, explain and interpret the main organisational challenges throughout the implementation of Aum's CB armament activities. I will first elaborate on the four previously identified organisational dimensions and its challenges (resource support, level of autonomy, information-sharing, and clear and compelling goals). These were also relevant throughout the implementation of Aum's CB activities. Next, this chapter will elaborate in more depth on the role of the organisational design. The organisational design shapes these four organisational dimensions and its challenges. Finally, I will elaborate on the extrapolations that follow from this case study to the adopted nuclear terrorism scenario. This way, this chapter aims to verify and reflect in more depth upon the previous insights and the formulated hypotheses on the relation between the organisational design and the nuclear terrorism threat.

[24] The respective sources are (1) interview with Marc Sageman, October 24, 2016. He is a former CIA officer, and a senior Fellow in the Foreign Policy Research Institute's Center for the Study of Terrorism. (2) Interview with Sonia-Ben Ouagrham-Gormley, December 23, 2016. She is an Associate Professor in the Schar School of Policy and Government at George Mason University. (3) Interview with Jean Pascal Zanders October 27, 2016. He is an independent consultant at 'the Trench.' He specialises in questions of armament and disarmament. He covers chemical, biological, radiological and nuclear weapons.

[25] John Parachini, "Aum Shinrikyo," in Brian Jackson et al. (eds.), *Aptitude for Destruction: Volume 2: Case Studies of Organisational Learning in Five Terrorist Groups* (Santa Monica: RAND corporation, 2005), 18.

7.2.1. Resource support

This case study supports the idea that sufficient people with the necessary *techne* and *metis* are essential in coping with a plot with a high task variability and low task analysability. Aum's ideology and targeted recruitment efforts enabled them to attract some skilled individuals. These people were the driving power behind the successes that Aum did achieve. Yet, Aum ultimately lacked the necessary expertise to effectively develop a successful CB weapons program. Next, Aum acquired abundant material resources. This was beneficial to the implementation of the CB plots. Yet, this case study simultaneously illustrated that these resources were not prioritised towards optimally leveraging Aum's experts.

First, Aum enjoyed the benefits of a hands-off attitude towards religious organisations by the Japanese authorities. It could employ diverse (public) recruitment methods such as leafleting, recruitment via yoga classes, and radio-broadcasting. Moreover, Aum's ideology had some appeal to alienated members of society. Thus, even though other Japanese cults had substantially higher membership numbers,[26] Aum did succeed in recruiting 10,000 members in Japan, 30,000 members in Russia, and a few dozen members in the United States, Germany and elsewhere. Of these 10,000 members in Japan, there were approximately 1,400 renunciates.[27] Not surprisingly, Aum also succeeded in recruiting some experts with some skills relevant to setting up a CB program.[28] Yet, this number of *Shukkesha* that was actually involved in Aum's CB plots was low. Estimates range from a few dozen people, over 30 to 40 people, to "five to ten leaders, while the entire programme including the assistants consisted of about 50-80 persons."[29] This inner circle was the driving power behind the successes that Aum did achieve. Yet, this group did not master the entire spectrum of technical and practical knowledge for each phase in the weaponisation and dissemination of CB agents.[30] For instance, considering the chemical plots, Sageman noticed that Masami Tsuchiya - a leading expert in this program - was "probably the only guy that could do anything. The other guys were a joke."[31] Considering the biological plots, the head of the program - Seiichi Endo – studied molecular biology. Yet, he was not trained to isolate, manipulate,

[26] Reader, *A Poisonous Cocktail,* 42.
[27] Kaplan, "Aum Shinrikyo," 209.
[28] Zanders et al., "Risk Assessment of Terrorism with Chemical and Biological Weapon," 546.
[29] The respective sources are (1) interview with Marc Sageman, October 24, 2016. (2) Interview with Sonia-Ben Ouagrham-Gormley, December 23, 2016. (3) Interview with Jean Pascal Zanders October 27, 2016.
[30] Rosenau, "Aum Shinrikyo's Biological Weapons Program,"89-101; Sonia Ben Ouagrham-Gormley (A), *Barriers to Bioweapons: The Challenge of Expertise and Organisation for Weapons Development* (London: Cornell University Press, 2014), 142. Jean Pascal Zanders, interview October 27, 2016 illustrates that by stating that, for instance, that the production of pure Sarin in a laboratory requires a chemist. This is not the same as producing Sarin on a large scale. This requires a chemical engineer who can upgrade to pilot plant production.
[31] Interview with Sageman, October 24, 2016.

produce and aerosolize the bacterial agents they worked on.[32] It follows that there were multiple operational accidents and errors during the implementation of these CB plots (e.g. problems with isolating toxin-producing strains,[33] erratic dissemination devices, and the failure of the anthrax-related activities to result in a single kill).[34]

This lack of functional specialisation was to a large extent a result of the fact that many members of the inner circle were chosen based on loyalty rather than scientific merit.[35] Elite disciples needed to demonstrate their commitment via, e.g, intensive rituals or rigorous physical postures.[36] A majority of Aum's members were not aware of the organisation's CB armament activities. Zanders stated, e.g., that Aum often relied on loyal but relatively unskilled cult members for the operation and maintenance of the installations.[37] After 1993, there was an increase in members that attempted to leave. This included some people whom had risen high in the religious structure. Asahara subsequently became even more paranoid about potential spies and defectors.[38] Aum assassinated various of these dissident cult members. This, however, also implied particular security risks. Dolnik notes that one of the victims left a note behind stating: "If I disappear, I was abducted by the Aum Shinrikyo sect." This led the police to take action. They set a date for a raid on Aum's compounds on the 21st of March.[39] This triggered Aum's hasty 1995 Sarin attack and the following law enforcement response. These examples demonstrate the importance of the loyalty of a group's members. This issue was also identified in the previous case studies. Yet, it seems that these type of security considerations are more pressing for a terrorist organisation.

Second, Aum Shinrikyo enjoyed a relatively strong financial input. It has been said that the cult's assets were equal to approximately 1 billion dollar at the time.[40] Moreover, Aum established various front companies via which it could obtain agents, laboratory tools and industrial equipment.[41] This was

---

[32] Ouagrham-Gormley (A), *Barriers to Bioweapons,* 139-142.
[33] Ibid.*,* 139.
[34] Richard Danzig et al., "Aum Shinrikyo: Insights into how Terrorists Develop Biological and Chemical Weapons," *Center for a New American Security* (2012): 26.
[35] Interview with Zanders, October 27, 2016.
[36] Flannery, *Understanding Apocalyptic Terrorism,* 228-229.
[37] Interview with Zanders, October 27, 2016.
[38] Parachini, *Aum Shinrikyo*, 31-32.
[39] Dolnik, *Aum Shinrikyo's path to innovation,* 130.
[40] Kaplan, "Aum Shinrikyo," 210; Zanders et al., "Risk Assessment of Terrorism with Chemical and Biological Weapons," 546; Sonia Ben Ouagrham-Gormley (B), "Barriers to Bioweapons: Intangible Obstacles to Proliferation," *International Security* 36, no. 4 (2012): 99-100.
Aum's financial input was a result of, e.g., the extraction of wealth of their members (e.g. renunciates' money, Aum selling DNA from Asahara), Aum's businesses and its illegal activities.
[41] Zanders et al., "Risk Assessment of Terrorism with Chemical and Biological Weapons," 546; Ouagrham-Gormley (B), "Barriers to Bioweapons," 99-100; Kaplan, "Aum Shinrikyo," 214.

beneficial to the successes that it did enjoy. Yet, resources were not prioritised towards optimally leveraging Aum's limited number of experts.[42] On the one hand, Aum spent large parts of its resources on other organisational affairs. It invested human and material resources in, e.g. other weapons programs, land owning, support of the *Shukkesha,* and court cases.[43] Admittedly, several million dollars were spent on its CB plots. Yet, the lack resource prioritisation undoubtedly placed increasing demands on its human and material resources.[44] On the other hand, security considerations added to the creation of an sub-optimal work environment. Aum's inner circle often attempted to complete missions internally while these could have been completed via outside help.[45] This led to operational errors. Moreover, Aum's sub-optimal work environment was also a product of the "cult regime of poor diet, sleep deprivation, and the use of LSD and other drugs."[46] The (limited) number of experts could not fully dedicate themselves to their scientific vocation.

7.2.2. Level of autonomy

This case study supports the idea that experts need to have control over its operational tasks and activities. This strengthens the likelihood that they can effective implement a nonroutine project. This argument here is based on reverse reasoning. The individuals involved in the inner circle did not have a high level of operational autonomy. Asahara was the undisputed central source of control. This charismatic leader facilitated the initiation of a nonroutine plot. Yet, this focal point of authority simultaneously limited the plot's effective implementation. It limited objective decision-making by the experts and impeded flexible and creative team work.

Shoko Asahara achieved supreme enlightment and was the "religious inspiration and focus of devotion in Aum…it was he who bestowed recognition of spiritual attainment on his disciples, and he who transferred, through initiation rituals, his own powers to others."[47] There were some superficial ordering principles like the so-called ministries. Yet, it seems that the core membership of the inner circle was a type of "hub-and-spoke" network. This does not imply that Aum was a highly centralised organisation;

---

[42] Zanders et al., "Risk Assessment of Terrorism with Chemical and Biological Weapons," 548.
[43] Aum was, for instance, charged for violating the Utilization of Land Planning Act.
[44] Interview with Zanders, October 27, 2016. He mentions that 60 million dollar was spent on Aum's CW plots. Moreover, Ouagrham-Gormley (B), "Barriers to Bioweapons," 100 mentions that 10 million dollar was spent on its BW plots.
[45] Danzig et al., "Aum Shinrikyo," 18.
[46] Rosenau, "Aum Shinrikyo's Biological Weapons Program," 297.
[47] Reader, *A Poisonous Cocktail*, 30.
Reader further explains that "Aum developed the view that there was a hierarchic path to liberation via a series of stages marked out by a structured series of initiations, each of which represented a further step upwards.

there was not so much organisation to speak of. It rather means that Aum was characterised by (key) members that were very receptive to Asahara's desires.[48] Whether due to spiritual reasons or merely to gain status in the organisation, the operational experts and assistants were primarily trying to please the guru. A high-ranking member stated, e.g., that "our activities depended simply on the mood of Asahara. There is no logical reason or explanation. He would say he heard God's prophecy and gave us orders."[49]

This central point of authority advanced the initiation of Aum's CB plots. The Guru's wishes were treated as demands. Even if there was a lack of resource prioritisation to the CB plots (supra), it is true that various human and material resources could be allocated to these programs without much opposition.[50] This is in line with the argument that was formulated after the previous case studies. The political and ideological leadership should focus the group's implementation of a nonroutine project and support it with sufficient human and material resources.

Yet, it simultaneously became clear that the leadership should limit top-down interference during the implementation of the plot. Asahara's authority "boiled over to a cult of personality."[51] He often made impulsive and shortsighted decisions; he was "fickle and irrational."[52] This gave rise to various unrealistic demands and excessive production targets. Yet, notwithstanding their own expectations of failure, pleasing the guru was more important than rational scientific judgment.[53] For instance, Aum attempted to disperse botulinum toxin in 1990. Yet, inquiry into the feasibility of such weapons only started a couple weeks earlier. The attack did not result in a single casualty.[54] Likewise, the cult wanted to disseminate a Sarin liquid in June and July 1993. Yet, when they discovered that buying a high-powered sprayer from a European firm would entail a two-month delay, Asahara ordered that the members needed to build the sprayer themselves. This sprayer broke down over and over again.[55] This institutional design focused towards a charismatic authority thus did not allow room for objective operational decision-making and problem-solving. The lack of objective decision-making was only intensified by the "cult regime of poor diet, sleep deprivation, and the use of LSD and other drugs."[56]

---

[48] Interview with Daniel Smith, November 23, 2016. Daniel Smith is a Senior Faculty Specialist at START.
[49] Danzig et al., "Aum Shinrikyo," 22.
[50] Parachini and Furukawa, "Japan and Aum Shinrikyo," 534; Dolnik, *Aum Shinrikyo's path to innovation,* 132-133.
[51] Dolnik, *Aum Shinrikyo's path to innovation,* 133.
[52] Rosenau, "Aum Shinrikyo's Biological Weapons Program," 269.
[53] Ouagrham-Gormley (A), *Barriers to Bioweapons,* 140.
[54] Dolnik, *Aum Shinrikyo's path to innovation*, 126-129. Ballard et al., "Chronology of Aum Shinrikyo's CBW Activities."
[55] Danzig et al., "Aum Shinrikyo," 27
[56] Rosenau, "Aum Shinrikyo's Biological Weapons Program," 297.

Making matters even worse, the central position of Asahara contributed to internal jealousy and competition on a lateral level.[57] This led to divergent behavior by the experts involved. In order to please the Guru, people involved in the CB plots were often competing with each other. For instance, Endo Seichi had a strong rivalry with Masami Tsuchiya.[58] They held back information, sabotaged other people, and falsely reported on their achievements. This competition was only strengthened by possible (lethal) repercussions related to failure.[59] It was to some extent even cultivated by Asahara, "possibly believing that competition between his lieutenants would produce faster results."[60] Decision-making was therefore often based on personal arrangements and favoritism.

Note already that this latter remark seems to indicate a contradictory trend. On the one hand, members of the inner circle were receptive to Asahara's desires. He succeeded in imposing decisions on his subordinates. Yet, on the other hand, this did not necessarily imply that the people involved were committed to any (long term) goal of the organisation, nor that they creatively worked together towards achieving this common goal. One report mentions, for instance, an unknown Aum member to have replaced botulinum toxin by water in one plot, perhaps struck by a guilty conscience.[61] This again underlines the idea that loyalty might be a particularly important issue for a terrorist organisation and its implementation of a nonroutine plot (infra: clear and compelling goals).

7.2.3. Information-sharing

This case study supports the idea that information-sharing motivates personnel and stimulates them in creatively combining knowledge. This argument is again based on the logic of reverse reasoning. Aum's implementation of its CB plots was not characterised by high levels of information-sharing. Communication and coordination was strictly confined. This limited diffusion of knowledge benefitted the concealment of Aum's illegitimate plots. Yet, it simultaneously limited the effective implementation of these nonroutine CB armament activities.

[57] Interview with Zanders October 27, 2016.
[58] Ouagrham-Gormley (A), *Barriers to Bioweapons,* 142.
[59] Parachini and Furukawa, "Japan and Aum Shinrikyo," 535; Ouagrham-Gormley (A), *Barriers to Bioweapons,* 141. She mentions, for instance, that Endo was not able to isolate a strain of clostridium botulinum nor an effective strain of anthrax. Nevertheless, he convinced his colleagues that he succeeded in doing so. With respect to the botulinum, various group members testified that they thought that they were spraying botulinum on the Japanese Parliament, the Imperial Palace and the U.S. embassy in Tokyo. These attacks were a failure.
[60] Ouagrham-Gormley (A), *Barriers to Bioweapons,* 141.
[61] Dolnik, *Aum Shinrikyo's path to innovation,* 130.

Communication and coordination throughout the implementation of Aum's CB plots was limited both between the inner circle and the broader organisation and within the inner circle itself. On the one hand, awareness about these plots was limited to the inner circle.[62] This implied a decrease in the likelihood of leaks or the detection of the plots by law enforcement agencies. The low number of people that knew about these activities inherently implied that it was less likely that leaks or infiltration by law enforcement agencies would occur. On the other hand, communication and coordination was limited within the inner circle itself as well.[63] Ouagrham-Gormley describes Aum Shinrikyo's biological armament activities as "highly compartmentalized." She explains further by stating that "access to work areas was strictly regulated" and "communications were restricted."[64] With respect to the botulism project, for instance, she stated that it is likely that "the likelihood that the different stages of any project were coordinated or integrated is very slim."[65] Likewise, when an assistant in these plots asked his leader about the sort of things being produced, he reportedly "told him not to bother himself with such questions as they were not important for him to know."[66] This limited number of connections was beneficial to the security of Aum's CB plots. It minimised the opportunities for law enforcement agencies to detect Aum's illegal activities. It is illustrative, e.g., that Aum was initially not linked to the 1994 attack in Matsumoto. This attack led to 7 deaths and over 600 injuries. Law enforcement agencies only implicated Aum after the 1995 Sarin attack.

Yet, as also illustrated by the previous case studies, it became clear that it is is important to acquire, store and share information in order to effectively develop solutions to a nonroutine problem. The limited information-exchange throughout Aum's CB plots impeded its effective implementation in two ways. First, the fact that only the inner circle was aware of these plots inherently limited the group's access to outside-help. The inner circle did not have access to a sufficient number of people with the required knowledge and expertise to implement the project. John Parachini notes in this respect that:

> The small size of the group probably impeded the development of its capabilities, which may in part explain the crudeness of some of its efforts as well as its failures. A larger group willing to freely exchange ideas might have been able to innovate more effectively.[67]

[62] Kaplan, "Aum Shinrikyo," 209.
[63] Ouagrham-Gormley (A), *Barriers to Bioweapons,* 140-142.
[64] Ibid.*,* 140-142.
[65] Ibid.*,* 140-142.
[66] Miyadai Shinji, "Ryôshin no hanzaisha," cited in Reader, *A Poisonous Cocktail* , 49.
[67] Parachini, "Aum Shinrikyo," 19.

Parachini moreover suggests in this context that "Aum's most significant learning occurred when it obtained the Russian formula for synthesizing sarin."[68] It has not been publicly acknowledged that Aum had access to such a blueprint design to synthesize Sarin. Yet, it is remarkable that Aum managed to cause most casualties by means of Sarin. I tend to agree with Parachini' s suggestion that "getting the blueprint or formula from an external source may explain why Aum was able to produce sarin in such large quantities." This highlights the relevance of having access to (outside) technical information.[69]

Second, information-exchange was also limited within the inner circle itself. The compartmentalisation and restricted communication within the inner circle limited the adoption and implementation of innovative and creative ideas.[70] People did not sufficiently consult with each other. For instance, Endo Seichi is considered to have been the only knowledge transmission belt within the biological program. Given he lacked training in microbiology, he was however "ill-suited to this task."[71] Even worse, as mentioned earlier, there was a relatively high level of competition and jealousy on the lateral level. For instance, Endo's insecurity and rivalry with Tsuchiya pushed Endo to hide his poor results.[72] Ouagrham-Gormley notes in this context that: "because heavy compartmentalization precluded formal technical reviews, these barriers to successful outcomes could only be identified at a very late stage."[73] The limited diffusion of information and ideas thwarted Aum from optimally leveraging its limited number of experts. It impeded the effective implementation of Aum's CB plots. This seems to be particularly relevant when considering the issues of *metis*. While communication and coordination is necessary to transfer technical knowledge, it seems to be even more important in order to convey *metis.*

7.2.4. Clear and compelling goals

The previous case studies illustrated that clear and compelling goals can strengthen an organisation's coherence and perseverance. This was beneficial in surmounting unexpected obstacles and maintaining group cohesion. Yet, notwithstanding the general receptiveness of the members of the inner circle to Asahara's desires, Aum's organisational and operational goals were neither crystal clear nor fully compelling. This limited the inner circle's coherence and perseverance, thereby thus limiting the effective implementation of Aum's CB plots.

[68] Parachini, "Aum Shinrikyo," 24.
[69] Ibid., 24.
[70] Ouagrham-Gormley (A), *Barriers to Bioweapons*, 140-142.
[71] Ouagrham-Gormley (B), "Barriers to Bioweapons," 101.
[72] Ouagrham-Gormley (A), *Barriers to Bioweapons*, 142.
[73] Ibid., 142.

First, Aum did not manage to formulate one clear and common goal. Aum's broad organisational goal was to destabilise Japan and overtake all governmental functions.[74] It was characterised by a radical apocalyptic doctrine that was accompanied by a growing degree of conflict between Aum Shinrikyo and outside society. Zanders notes in this context that "chemical and biological weapons could conceivable have played a role in in destabilizing Japan, but they would have been insufficient to establish the cult's own form of governance." There was no rationale for the CB program without the other organisational goals (e.g. establishing a conventional weapons force and supporting the communes of Aum's renunciates).[75] This broad focus placed increasing demands on Aum's human and material resources. Moreover, specifically with respect to Aum's CB armament activities, these were characterised by "recurrent turnarounds and (a) scattered work agenda."[76] This is in line with Aum's delusional organisational goals. Operational orders were often impulsive and without substantial reflection. A member of Aum's inner circle stated, for instance, that "the idea of selecting sarin occurred by reading a book translated into Japanese by Tsuchiya, the story of poisons."[77] There exist some instances of persistence. Yet, the "soundest generalization is that Aum took an erratic course, rather than adopting a methodical research and development program."[78] Members of the inner circle followed the ad hoc whims of Asahara. Aum's chemical and biological armament activities were not coherent and focused.

Second, compared to the previous case studies, Aum Shinrikyo's goals did not enjoy a similar level of support; its goals were not as compelling. On the one hand, considering the organisational level, Aum's ideology had some appeal to alienated members of society. The organisation had high number of members. This is remarkable for a terrorist organisation. Yet, it is also true that several other Japanese cults could claim membership numbers running into hundreds of thousands.[79] Moreover, there was also some opposition within the broader organisation. For instance, Aum murdered up to 80 "rogue" members of the organisation.[80] Its level of support should thus not be equated to that of the previous case studies. A higher level of support might have enabled Aum to recruit more people with the required skills. On the other hand, considering the operational level, members of the inner circle were not always intrinsically motivated to work together towards achieving a common goal. They adjusted themselves to the ad how whims of their leader. There was no real cooperative relationship between the leader

[74] Tu, "What Were the Real Objectives of Aum Shinrikyo," 2.
[75] Zanders et al., "Risk Assessment of Terrorism with Chemical and Biological Weapons," 548.
[76] Ouagrham-Gormley (A), *Barriers to Bioweapons*, 141.
[77] Interview with Tomomasa Nakagawa by Antony T. Tu, *ASA Newsletter*, March 31, 2012. Available at: http://asanltr.com/wordpressV1/wp-content/uploads/2012/04/ASA-12-2Marbig-copy.pdf (accessed March 23, 2017).
[78] Danzig et al., "Aum Shinrikyo," 22.
[79] Reader, *A Poisonous Cocktail,* 42.
[80] Dolnik, *Aum Shinrikyo's path to innovation,* 126.

and the different members of the inner circle. This led to operational errors, exaggeration of scientific progress, competition and jealousy on a lateral level, or (moral) doubts by individual members about the CB plots. Considering the latter, Dolnik for instance mentions that an unknown Aum member apparently replaced botulinum toxin by water in one plot. He was perhaps struck by a guilty conscience.[81] Tucker likewise reports that one of the perpetrators of the 1995 Sarin attack doubted his actions when seeing a pretty young woman standing in front of him in the train. The perpetrator reportedly got off the train, meditated shortly to calm his thoughts, and boarded again on the next car.[82]

Aum Shinrikyo did manage to carry out several attacks; the inner circle succeeded in causing a number of casualties via CB attacks. Yet, these observations highlight the damage that uncompelled operators might inflict to the effective implementation of a nonroutine plot. The lack of clear and compelling goals limits an organisation's capacity to circumvent unexpected obstacles and maintain cohesion. It limits its capacity to effective implement a nonroutine plot.

7.3. Aum Shinrikyo's CB activities: various features of a mechanistic design

This chapter will now elaborate on how the organisational design influenced the implementation of Aum's CB plots. I have adopted a definition of the organisational design as "the sum total of the ways in which its labor is divided into distinct tasks and then its coordination is achieved among these tasks."[83] Similar to the previous case studies, I will link the four organisational dimensions - and its challenges - to the organisational design. Based on these insights, I will extrapolate relevant insights to a potential nuclear terrorism plot.

In short, Aum's implementation of its CB plots was characterised by an organisational design with various features of a mechanistic organisational design (see table 7.1). This type of organisational design was beneficial to the operational security of the group. Yet, these mechanistic features simultaneously impeded the effective implementation of Aum's chemical and biological armament activities.

[81] Dolnik, *Aum Shinrikyo's path to innovation,* 130.
[82] Tucker, "War of Nerves," chapter 17
[83] Henry Mintzberg, *Structure in Fives: Designing Effective Organisations* (New Jersey: Prentice-Hall, 1983), 2.

Table 7.1. Organisational design of Aum Shinrikyo's inner circle

	Organisational design of Aum Shinrikyo's inner circle
Level of interconnectedness	Insufficient number of intra-division and inter-division connections.
Level of hierarchy	Insufficiently high level of control over operations by experts themselves + no optimal resource prioritisation to support the experts.
Level of specialisation	Insufficiently high level of personal specialisation (insufficiently high levels of both techne and metis)

* Note that this table is inherently arbitrarily to some extent. It is difficult to assign exact and uniform values to these design parameters.

First, the effective implementation of Aum's chemical and biological armament plots required sufficient individuals with a high level of personal specialisation. Masami Tsuchiya was, for instance, one of the driving powers behind the successes Aum did achieve in its chemical armament plots. Yet, in general, the organisation did not have the necessary personnel with sufficient techne and metis to cope with the various nonroutine situations that arose throughout the implementation of its CB plots. The inner circle did not have the required expertise to implement each task related to the weaponisation of biological and chemical agents. Aum enjoyed a relatively secure operational environment. It succeeded in recruiting some well-skilled experts. Yet, its organisational design did not support the build-up of critical skills and knowledge. The organisation had, e.g. limited access to outside help and information. Likewise, Aum employed people in the inner circle based on loyalty rather than scientific merit.

Second, Aum neither succeeded in optimally leveraging this limited number of people with specialised skills. Members of the inner circle functioned in a type of "hub and spokes" network. The charismatic leader Shoko Asahara was the central point of authority. Aum was characterised by (key) members being receptive to Asahara's desires. This type of hierarchical control by the leadership is a mechanistic feature. Even if there was no optimal resource prioritisation, this type of leadership did enable the allocation of various human and material resources to these CB plots without much opposition. It was beneficial to the initiation of Aum's CB plots. Yet, this focal point of authority simultaneously limited objective operational decision-making by the specialised experts. Top down interference in the implementation of the work limited the necessary flexibility, creativity, and adaptability to cope with the diverse nonroutine tasks. Personal arrangements, favouritism, and an eagerness to please the fickle and irrational guru often dominated decision-making (e.g. the rushed attempt to disperse botulinum

toxin in 1990). Asahara did not establish a methodical research and development program which steadily progressed towards operational success.

Finally, closely related, there was an insufficient number of intra-division and inter-division connections. Aum Shinrikyo was characterised by a limited diffusion of knowledge both between the inner circle and the broader organisation and within the inner circle itself. There were few liaison devices and knowledge belts. There was a high level of compartmentalisation and no access to outside help. Making matters even worse, people in the inner circle were often competing with each other. This also limited the information-exchange. People held back information, sabotaged other people, and falsely reported on their achievements. Not surprisingly, this mechanistic organisational design feature impeded the necessary creativity and adaptivity of the inner circle. It limited this group's capacity to effectively cope with the nonroutine nature of technology.

Aum Shinrikyo's was thus characterised by various mechanistic design features. Its organisational design increased subjective control over the experts via the guru's charismatic authority rather than increasing objective control over the outcome. It did not advance the effective implementation of Aum's CB plots. It did, however, benefit the operational security of the organisation. It is not entirely clear to which extent this was an actual deliberate choice. Yet, it does demonstrate how the effectiveness-efficiency trade-off functions. I will demonstrate this by zooming on the three identified organisational design features.

First, the recruitment and employment of experts in a clandestine operational environment inherently implies increased security risks. Aum therefore attached great importance to the loyalty of the members involved in these plots. This was beneficial to its operational and organisational security. Yet, it came at the expense of its access to people with the necessary skills and expertise. Second, the inner circle was steered and guided by Asahara. Even though his demands would be unrealistic, experts would loyally execute his orders. This limited the inner circle's *operational autonomy* and its effectiveness. Yet, it simultaneously limited the operational level of ambiguity and the corresponding security risks that could result from such ambiguity. Moreover, it is likely that it reduced the likelihood of infiltration or defection. Note, however, already that this authority "boiled over to a cult of personality."[84] This also led to different forms of divergent behavior. Finally, the lower number of *interconnections* within the inner circle and between the inner circle and the broader organisation implied a decreased risk of detection by counterterrorism forces. Knowledge and information was less diffused. This limited the inner circle's

[84] Dolnik, *Aum Shinrikyo's path to innovation,* 133.

effectiveness. Yet, it follows that there were also simply less opportunities for law enforcement agencies to detect Aum's CB armament activities.

7.4. Extrapolations to the nuclear terrorism threat

The final section of this chapter will turn from description to exploration. There remain differences between Aum's CB armament activities and the adopted nuclear terrorism scenario (i.e. the exact tasks and activities; Aum's protected status as a religious organisation). I need to take into account these differences when I extrapolate relevant insights from this case study to the probability of nuclear terrorism. This way, I aim to verify and reflect upon the previous theoretical extrapolations. In order to facilitate the accumulation of knowledge on this understudied dimension, this section will follow the same structure as the structure that is used in the previous chapters. I will highlight new insights when necessary.

7.4.1. Effectiveness…

Considering the fit between the organisational design and the nonroutine nature of technology, this third case study supports the plausibility of the hypothesis that "a terrorist organisation is most likely to effectively complete a nuclear terrorism project by means of an organisational design similar to an organic design." (= H1) The support of this argument is based on reversed reasoning. Aum's organisational design was characterised by various mechanistic features. In contrast to a more organic organisational design, these mechanistic features complicated the effective implementation of Aum's nonroutine CB plots.

First, I have argued that an organic organisational design revolves around personally specialised individuals. Compelled experts with the necessary *techne* and *metis* strengthen the likelihood that the organisation can cope with a plot with a high task variability and low task analysability. Aum's access to some experts with particular skills was a driving force behind its limited successes. The inner circle did succeed in implementing some CB plots that led to multiple casualties. Yet, Aum's inner circle ultimately lacked the necessary people to effectively complete the weaponisation and dissemination of CB agents. The inner circle had, e.g. limited access to outside help and information. Moreover, Aum employed people in the inner circle based on loyalty rather than scientific merit. An organisational design that facilitated access to more well-skilled individuals could have improved the effective implementation of

Aum's CB plots. The exact requirements with respect to the experts will depend, e.g., on the exact nuclear terrorism scenario. Yet, adopting the logic of reversed reasoning, it seems to remains plausible to assume that personally specialised individuals will be of essential importance in any nonroutine nuclear terrorism plot.

Second, it became clear that Aum's organisational design was not appropriate to optimally leverage the limited number of experts. Admittedly, this case study highlighted that an organisational design that is dominated by a charismatic leader can facilitate the initiation of a nonroutine project. It suggests that it might be easier to provide the project team with sufficient resource support and clear goals when the team operates in a broader hierarchical organisation (rather than a cellular structure). This is in line with the argument that the leadership of a group that pursues a nuclear terrorism plot should support and steer the project team. Yet, this case study simultaneously highlighted that an organisational design with various mechanistic features complicated the effective implementation of the nonroutine plots. Indeed, Asahara's leadership boiled over to a cult of personality. On the one hand, this implied a lack of operational control by the experts in the inner circle. Asahara often set strict deadlines and imposed pet solutions. This led to various operational delays and errors. Moreover, it even fostered competition and rivalry on a lateral level. On the other hand, this also implied a limited level of information-exchange between members within the inner circle and between the inner circle and the broad organisation. Asahara impeded horizontal communication and coordination. This limited the inner circle's flexibility, creativity, and adaptability. This type of organisational design with various mechanistic features thus hindered the effective implementation of Aum's nonroutine CB plots. Adopting the logic of reversed reasoning, it therefore remains plausible to assume that a more organic-like organisational design would increase the likelihood that a terrorist organisation can effectively implement a nonroutine nuclear terrorism plot.

The support for this hypothesis is particularly relevant because this case is one of the few cases of an actual *terrorist* organisation that implemented a WMD program. It can probably be considered to be the one case in this research project that is most analogous to the adopted nuclear terrorism scenario. The increased analogy strengthens the support for this hypothesis.

7.4.2. Versus efficiency

An organisational design similar to an organic organisational design is thus still be expected to strengthen the likelihood that a terrorist organisation can effectively complete a nuclear terrorism

project. Yet, again adopting the logic of reversed reasoning, it simultaneously remains plausible to expect that an organic organisational design would imply substantial security risks to a terrorist organisation (=H2). This case study allows us to develop this argument in more depth by emphasizing the constraints that follow from a terrorist organisation's covert nature. Moreover, this case study does not provide any reason to theoretically refute the plausibility that a nuclear terrorism plot can be perceived to be an inefficient strategy (=H3). More specifically, it suggests that the most-likely candidate to pursue a nuclear terrorism plot would not be driven by an instrumental-rationality.

First, it remains plausible to assume that an organic organisational design would imply substantial security risks to a terrorist organisation (=H2). I will zoom in on the three identified organisational design features to support the plausibility of the suggested effectiveness-efficiency trade-off. While doing so, I will illustrate that the security constraints that follow from such a plot's covert nature deserve more attention in traditional nuclear terrorism threat assessments. Considering traditional threat assessments often focus on individual parameters or the consequences of a nuclear terrorism attack, they tend to be biased towards underestimating the pressing nature of these constraints for a terrorist organisation.

Aum Shinrikyo enjoyed some particular benefits with respect to the recruitment and employment of *experts*. It enjoyed some level of popular support and could adopt expertise-oriented recruitment efforts. Moreover, it was not vigorously targeted by law enforcement agencies due to its status as a religious organisation. Yet, the covert nature of this organisation nevertheless put heavy constraints on its recruitment efforts. Aum demanded a lot of sacrifices of its members. Loyalty was considered to be very important. The most elite disciples were bound to demonstrate their commitment via, e.g, intensive rituals or rigorous physical postures.[85] These type of requirements have also been identified by Eli Berman as an important way to control defection by a terrorist organisation.[86] It follows that the recruitment of people that are both loyal to a terrorist organisation and capable to implement a nuclear terrorism plot can be expected to be hard. Aum Shinrikyo demonstrated that success is possible. Yet, we should take into account that each recruitment efforts entails particular security risks. The mere threat of infiltration or defection might already instil caution in the terrorist organisation's considerations. Aum's inner circle was, for instance, not susceptible to the inclusion of more well-skilled individuals or outside help. These pressing organisational challenges can also be expected to be at play during a nuclear terrorism plot.

[85] Flannery, *Understanding Apocalyptic Terrorism,* 228-229.
[86] Eli Berman (Eli Berman, *Radical, Religious and Violent: The New Economics of Terrorism* (Cambridge: MIT Press, 2009)

Next, Asahara's personality cult led to a lack of *scientific autonomy* by the experts involved in the CB plots. This was detrimental to the plots' effective implementation. Yet, this level of control by Aum's charismatic leader simultaneously limited operational ambiguity and fluidity. Asahara's orders were in general loyally executed. Moreover, this level of control limited the likelihood that the inner circle would be infiltrated by law enforcement agencies or that a member of this group would defect. This way, the lack of operational autonomy by the experts involved reduced the risks of divergent behavior. Adopting the logic of reversed reasoning, this case study seems to suggest that a higher level of operational autonomy increases the likelihood of divergent behavior. Yet, this case study simultaneously made clear that too strict control by the leadership might - on its turn - also imply particular types of divergent behavior by the experts involved (e.g. competition and rivalry on a lateral level, exaggeration of scientific progress). This might imply particular security risks as well (via, e.g. an operational error that is detected by law enforcement agencies).

It is thus clear that allowing for sufficient operational autonomy while trying to limit divergent behavior is a complex balancing act. This is in line with what we have found over the two previous case studies. A sufficient level of operational autonomy is necessary to increase the likelihood that the experts can effectively implement a nonroutine plot. Yet, both too little and too strict control by the leadership might imply divergent behavior by the experts involved. This, on its turn, might imply particular security risks. It is plausible to assume that this balancing act will play a pressing role in a nuclear terrorism plot as well. This balancing act will be influenced by various factors. Both the exact nuclear terrorism scenario and the clarity and compelling nature of the organisation's goals seem of particular relevance. These might sharpen or alleviate the pressing nature of this balancing act. Yet, in general, it is clear that this is no straightforward task. The pressing nature of this balancing act deserves more attention in traditional nuclear terrorism threat assessments.

Considering the number of *interconnections*, Aum's limited information-exchange within the inner circle and between the inner circle and the broader organisation improved its operational security. It reduced the likelihood that the implementation of these plots would be detected by law enforcement efforts. Yet, it simultaneously impeded the effective implementation of its nonroutine plots. This neatly illustrates the effectiveness – efficiency trade-off. It is likely that a higher number of interconnections would have increased Aum's security risks. Michael Kenney was right in arguing that it is never easy to blend abstract techne with real-world metis, particularly "when practitioners are forced to operate in

hostile environments."[87] It is therefore plausible to expect that these type of constraints will also be at play during the implementation of a nuclear terrorism plot. Such a nonroutine plot requires sufficient communication and coordination. Yet, this inherently implies increased security risks for the terrorist organisation.

Second, this case study did not gave us any reason to theoretically refute the idea that a nuclear terrorism plot can be perceived to be an inefficient strategy (=H3). Aum enjoyed various beneficial exogenous conditions. It enjoyed some level of popular support and it had the advantage of limited law enforcement pressure. Yet, the organisation still did not succeed in effectively causing mass casualties or destabilising Japanese society. Aum's actual use of CB agents was predominantly tactical, often "prompted by a variety of secondary factors, such as attempts to expand the cult's size and influence, to fend off intervention by Japanese authorities, and to destroy its enemies."[88] A more organic design might have improved the effective implementation of Aum's CB plots. Yet, it remains questionable whether or not this would have enabled Aum to achieve its strategic objectives. Moreover, a more organic design would also have increased the security risks. Note in this context that law enforcement agencies immediately decimated the organisation after its 1995 Sarin attack. It might be expected that the response to the detection of any sign of a nuclear terrorism project will be equally swift. Adopting an instrumental-rationality approach, there is thus no reason to theoretically refute the third hypothesis.

Moreover, it is interesting to note that Aum - one of the very few cases of an extremist organisation that actually tried to push through a full WMD program - did not wield an instrumental rationality. In contrast, Aum seems to have been characterised by a value rationality. Max Weber defined this as social action that is "determined by a conscious belief in the value for its own sake of some ethical, aesthetic, religious, or other form of behavior, independently of its prospects of success."[89] Aum's unique apocalyptic ideology and obsession with futuristic technology seem to match with this type of rationality. The members of the inner circle pursued particular actions because of the value of these

[87] Michael Kenney, "'Dumb' Yet Deadly: Local Knowledge and Poor Tradecraft Among Islamist Militants in Britain and Spain, *Studies in Conflict & Terrorism* 33, no.10 (2010): 915.
[88] Kaplan, "Aum Shinrikyo," 208.
[89] Max Weber, *Economy and Society,* 24-25.
Max Weber also refers to 'traditional' types of social action. This refers to social action which is determined by ingrained habituation. Yet, as nuclear terrorism (nor something similar) has never happened, this does not seem to be relevant to our study. Moreover, Weber also refers to an affectual type of social actions. This refers to social actions that are "determined by the actor's specific affects and feeling states." This might also be an interesting perspective to look at the potential motivation for nuclear terrorism. Yet, Weber also stated that "it may, for instance, consist in an uncontrolled reaction to some exceptional stimulus." This type of rationality therefore seems more useful to reflect upon ad-hoc instance of social behavior.

actions themselves. Independent of its prospects of success, experts primarily wanted to please the guru via their actions. They were devoted to him. This is in line with Weber's distinction between devotion "oriented toward a purpose, a common cause, a rationally intended goal" and devotion to "a person as such."[90] Asahara was the charismatic authority of the group. Weber argued in this context that the 'purer' charismatic authority is, the less that the organisation can be understood in the usual sense; as an order of persons and things that function according the means-end scheme."[91] Charismatic authority seems to be intrinsically alien from neutral rational discipline.[92] Indeed, reflecting upon Aum Shinrikyo's CB plots, it is clear that an eagerness to please this fickle and irrational guru often dominated decision-making.

This case study thus suggests that the most-likely candidates to pursue a nuclear capacity would be guided by a similar charismatic authority and value-rationality. This was the driving force behind the initiation of Aum's CB program. This type of rationality could be a function of, e.g. the organisation's ideology or its organisational state of affairs. Yet, it should not necessarily be equated with the usual suspects such as Al Qaeda or the Islamic State. An in-depth case-by-case approach is necessary to assess an organisation's type of rationality. Moreover, paradoxically, these organisations might be the most-likely candidates to pursue a nuclear terrorism plot. Yet, they are simultaneously expected to be less effective in actually implementing such a nonroutine plot. Value-driven organisations might, for instance, be more likely to conflict with the need for scientific autonomy, information-exchange, or high levels of popular support. Unfortunately, these type of considerations are often underdeveloped in today's nuclear terrorism threat assessments.

7.5. Conclusion

The fact that Aum Shinrikyo's inner circle succeeded in causing various casualties is a stark reminder that this research project does not intend to make any absolute claims on the role of the organisational design. Yet, this case study was the first case study of an actual nonroutine *terrorism* plot. Moreover, it can probably be considered to be the case that is most analogous to the adopted nuclear terrorism scenario. This way, this case study helped us in further exploring the role of the organisational design in the nuclear terrorism threat. This case study was therefore a new piece of the puzzle.

[90] Max Weber, *Economy and Society: An Outline of Interpretive Sociology* (Berkeley, Los Angeles, London: University of California Press, 1978), 1150.
[91] Ibid., 1119.
[92] Ibid., 1148-1149.

Aum Shinrikyo was in many ways an outlier with particular predispositions towards a WMD program. It could adopt expertise-oriented recruitment periods and had a high number of material resources at its disposal. Moreover, Japanese law enforcement agencies did not aggressively pursue Aum's inner circle. It enjoyed a relatively secure operational environment. Nevertheless, Aum did not succeed in establishing an effective CB program. It did not succeed in effectively causing mass casualties or destabilising Japanese society. This was to some extent a consequence of its organisational design. In general, this case thus first affirmed the relevance and impact of the organisational design in implementing a project with a nonroutine nature of technology.

Next, this case did not provide any reason to theoretically refute the plausibility of the suggested effectiveness-efficiency trade-off. Similar organisational dynamics were also at play during the implementation of this nonroutine terrorism plot. This strengthens the general plausibility of the suggested effectiveness-efficiency trade-off. Moreover, this case brought forward two theoretical arguments that go beyond the general support for this idea. First, this case study demonstrated that the security constraints that follow from such a plot's covert nature deserve more attention in traditional nuclear terrorism threat assessments. The mere threat of detection by law enforcement agencies might already instil caution in a terrorist organisation's considerations with respect to such a plot. This would, however, simultaneously reduce the likelihood that it can effectively implement this nonroutine project. These type of challenges seem to be particularly pressing for a covert terrorist organisation. Second, this case study suggested that the most-likely candidates to pursue a nuclear capacity would be guided by a charismatic authority and value-rationality (rather than an instrumental rationality). Paradoxically, however, this might imply that this organisation will be less effective in actually implementing a nonroutine nuclear terrorism plot. These type of considerations are often neglected in today's nuclear terrorism threat assessments.

Aum Shinrikyo's CB armament activities thus generally strengthened the plausibility of this study's theoretical propositions and hypotheses. Yet, it was only the first case study in this research project that focused on the implementation of an actual nonroutine terrorism plot. Moreover, Aum Shinrikyo was a relatively idiosyncratic terrorist organisation. In order to strengthen the extrapolations and qualifying conditions identified in this case study, the final case study of this research project will therefore reflect upon a nonroutine terrorism plot by a more common terrorist organisation: Al Qaeda's implementation of 9/11.

8. Case study: the implementation of 9/11 by Al Qaeda

The final case study that has been selected to explore the plausibility of the suggested hypotheses is a nonroutine project implemented by a more common terrorist organisation: the implementation of 9/11 by Al Qaeda. Al Qaeda (AQ) is one of the most well-known terrorist organisations. It is often perceived as a likely perpetrator of a nuclear terrorism plot. Moreover, this case has been selected according to the logic of a least-likely case. This way, it provides us with another piece of the puzzle to better understand the nuclear terrorism threat. It enables me to assess the extrapolations and qualifying conditions that were identified in the previous case studies.

The origins of Al Qaeda are often linked to Osama Bin Laden's support for the Afghan mujahedeen in the Soviet-Afghan war (1979-1989). He was helping to run Maktab al-Khidamat (MAK) during the "holy war" against the Soviet invaders. This organisation funneled money, fighters and arms into the Afghan war. It is often considered to be the precursor of Al Qaeda. Indeed, with Soviet forces withdrawing from Afghanistan, further plans for a multinational insurgent organisation that would continue jihad were developed. This organisation would be known as Al Qaeda. This can be translated as the "base" or "foundation.[1] Al Qaeda's strength and geographical reach gradually expanded throughout the 1990's. It increasingly incited jihad and particularly denounced the Western occupation of Islamic lands. Bin Laden publicly declared jihad against the United States in 1996.[2] Not surprisingly, American interests were often targeted by the broad Al Qaeda network.[3] Yet, it was not until the morning of September 11th 2001 that Al Qaeda would strike its most devastating blow to the United States.

Khalid Sheikh Mohammed (KSM) was the "principal architect" of these 9/11 attacks.[4] He was an autonomous terrorist entrepreneur. He was "hatching and planning an extraordinary array of terrorist

[1] This section is based on, e.g., Michael Scheuer, *Through Our Enemies' Eyes: Osama Bin Laden, Radical Islam, and the Future of America*, 2nd ed. (Washington: Potomac Books Inc., 2006), 110; Ty McCormick, "Al Qaeda Core: A Short History," *Foreign Policy* (2014). Available at: https://foreignpolicy.com/2014/03/17/al-qaeda-core-a-short-history/ (accessed on April 24, 2019); Abdullah Azzam, "Al Qa'ida al-Subah" (The Solid Foundation), 1988. Available at: https://insidethejihad.com/2014/03/al-qaida-al-subah-the-solid-base/ (accessed January 12, 2018).

[2] Scheuer, *Through our Enemies' Eyes,* 145.
Considering the original version of this Fatwa, an English translation of this Fatwa is available at the website: https://is.muni.cz/el/1423/jaro2010/MVZ448/OBL___AQ__Fatwa_1996.pdf (accessed January 18, 2018).

[3] Daniel Byman, "Al Qaeda as an Adversary: Do we Understand our Adversary?", *World Politics* 56*,* no. 1 (2003): 139-163 notes that this is not to say that all activities were masterminded, ordered, or logistically supported by Bin Laden or the core Al Qaeda group. Al Qaeda had a small core group, but it was also a broader network that linked various Islamist groups and causes.

[4] National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, 1st ed. (New York: Norton, 2004), 145. This report is hereafter referenced to as the 9/11 Commission Report.

schemes."[5] Knowing that he would need personnel, money and logistical support, he proposed a grandiose plan to Bin Laden and Mohamed Atef - the military chief of Al Qaeda – in 1996. This plan included a total of 10 aircrafts to be hijacked, nine of which would crash into targets including those eventually hit on September 11, plus CIA and FBI headquarters, nuclear power plants, and the tallest buildings in California and the state of Washington. KSM would land the tenth plane and, after killing all adult male passengers, deliver a speech excoriating U.S. support for Israel, the Philippines and repressive governments in the Arab world.[6] This plan originally received a lukewarm response by Al Qaeda leaders. They considered it too complex. Yet, the basic idea of using aircrafts as weapons was accepted in early 1999. Bin Laden, KSM and Atef decided on a more realistic list of targets in a series of meetings in the spring of 1999: the White House and the Pentagon, which Bin Laden wanted, the Capitol, and the World Trade Center, which was favored by KSM.[7] Four suicide operatives were soon selected by Bin Laden and provided to KSM: Khalid al Mihdhar, Nawaf al Hazmi, Khallad, and Abu Bara al Yemeni.[8] Yet, this plot bumped into various problems. The latter two persons could not acquire an U.S. visa. KSM subsequently decided to alter the plan. Crashing hijacked aircrafts into U.S. targets remained one component of the plan. Yet, Khallad and Abu Bara al Yemeni would try to hijack U.S. flagged commercial planes flying across East Asia and destroy them in mid-air.[9] Next, the East-Asia part of this plot was cancelled. The coordination with the operation in the U.S. would be too difficult.[10] Finally, making matters worse, Mihdhar and Hazmi proved to be ill-prepared for a mission in the United States. They had no aptitude for English and could consequently not learn how to fly.[11]

Fortunately for AQ, the late 1999 arrival of four aspiring jihadists in Kandahar presented a more attractive alternative. Mohamed Atta, Ramzi Binalshibh, Marwan al Shehhi, and Ziad Jarrah left Hamburg to train for the violent jihad. The members of this so-called Hamburg Cell presented the advantage of fluency in English and familiarity with life in the West. Bin Laden and Atef understood the deficiencies of the initial operatives and the skills and knowledge of the Hamburg cell. They were consequently quick to assign these members to the 9/11 plot.[12] Binalshibh did not succeed in acquiring a U.S. visa because he was considered to be an undocumented alien seeking work in the U.S. He played

[5] The 9/11 Commission Report, 145.
[6] Ibid., 154.
[7] Staff Statement no. 16, "Outline of the 9/11 plot," the 9/11 Commission Report, 2. Available at: https://www.9-11commission.gov/staff_statements/staff_statement_16.pdf (accessed April 24, 2019).
[8] The 9/11 Commission Report, 155.
[9] Ibid., 156.
[10] Ibid., 159.
[11] Ibid., 215-223.
[12] Ibid., 160 – 169. These were not the only members of the Hamburg cell. Atkins also mentions Said Bahaji, Mohammad Belfas, Zakariya Essabor, Mounir el Motassadez, and Abdelghani Mzoudi. Some of them would play an administrative or logistical role in the plot.

a coordinating role from abroad. Yet, Atta, al Shehhi, and Jarrah arrived in the United States in the early summer of 2000. They quickly started to learn how to fly via flight schools. Moreover, AQ found a fourth pilot. Hani Hanjour was identified as a trained pilot in one of Al Qaeda's training camps.[13] The "muscle hijackers" arrived in the United States around the late spring of 2001. Mohamed Atta subsequently decided that the "planes operation" would take place on the 11th of September, 2001.[14]

In what follows, this chapter will be structured according to a similar theory-generating narrative to the previous chapters. This will facilitate the cross-case analysis in chapter nine. First, I will elaborate on the relevance of this case study. Next, I will reflect upon the four previously identified organisational dimensions and its corresponding challenges: resource support, level of autonomy, level of information-exchange, and clear and compelling goals. Third, I will elaborate on the role and impact of the organisational design. This is the common thread that permeates these organisational dimensions and challenges. Finally, I will build on these findings to extrapolate relevant insights about the formulated hypotheses with regards to the probability of nuclear terrorism.

8.1. The relevance of 9/11

The implementation of 9/11 is theoretically relevant due to its nonroutine nature of technology. The exact tasks and activities are not identical to the adopted nuclear terrorism scenario. Yet, this shared organisational feature does enable the extrapolation of relevant insights to the nuclear terrorism threat. Moreover, this case of a nonroutine terrorism project has also been selected according to the logic of a least-likely case study. Its nonroutine nature of technology was less outspoken than the adopted nuclear terrorism scenario. It follow that the previous extrapolations with respect to the formulated hypotheses would become more plausible when similar dynamics are identified throughout the implementation of 9/11.

Jenkins argued that "ingenuity rather than technical sophistication" enabled Al Qaeda to successfully carry out the "planes operation."[15] Terrorist organisations succeeded in hijacking airplanes before (e.g. the 1994 hijacking by the Groupe Islamique Armé). The exact technical tasks were often not beyond Al Qaeda's standard operations. The 9/11 hijackers used simple tools as knives and box cutters, they

[13] The 9/11 Commission Report, 223 - 226.
[14] Terry McDermott, *Perfect Soldiers: The 9/11 Hijackers: Who They Were, Why They Did It* (e-book: Harper Collins e-books, 2008), 180.
[15] Brian Jenkins, "The Organisation Men: Anatomy of a Terrorist Attack," in James Hoge and Gideon Rose (eds.), *How Did This Happen? Terrorism and the New War* (New York: Public Affairs, 2001), 3-4.

familiarised themselves with the target so as to avoid surprises,[16] and they could exploit a relatively lenient counter terrorism environment (before the Global War on Terrorism, it was, e.g., the policy to cooperate with hijackers rather than fight them).[17] I therefore follow John Mueller's argument that would-be atomic terrorists would probably be confronted with more difficulties.[18] The adopted nuclear terrorism scenario is characterised by a higher task variability and lower task analysability.

Yet, notwithstanding these differences, it remains true that this case study can be considered to be characterised by a nonroutine nature of technology. On the one hand, this was a result of the fact that it was the first time that the aircrafts itself were used as a weapon. Al Qaeda needed to successfully hijack the planes. This led them to do multiple case runs to revise and improve the operational plan. Moreover, this also required some people with specialised skills and training to successfully fly these multi-engine aircrafts into the selected targets. On the other hand, this was also a result of the fact that a diversity of tasks needed to be completed and attuned to each other in a clandestine operational environment. Al Qaeda needed, e.g., to recruit and train the pilots and muscle hijackers, move these different operatives, plan the plot, and raise and transfer the necessary money.[19] Terrorist organisations have not often succeeded in this type of coordinated attacks. It required a high level of patience and detailed planning. Not surprisingly, the implementation of 9/11 was entangled by a number of exceptional situations that were hard to work out in advance. The wobbling evolvement of the original plan illustrates this case in point. Some examples of unexpected situations are the two selected suicide operatives that proved to be ill-prepared for a mission in the United States,[20] Ramzi Binalshibh's denial of a U.S. visa,[21] or the delay of Mohammed Atta's first flight on September 11 (because of which he nearly missed his connecting flight that targeted the WTC).[22] Moghadam even sees the final plot as the end point of a trial-and-error process since 1993. KSM is likely to have learned from, for instance, his nephew's (Ramzi Youssef) 1993 bombing of the WTC and the failed 1995 Bojinka plot.[23] Moreover, it

[16] Gaetano Ilardi, "The 9/11 Attacks: A Study of Al Qaeda's Use of Intelligence and Counterintelligence," *Studies in Conflict and Terrorism* 32, no. 3 (2009): 171–87.
[17] The 9/11 Commission Report, 83.
[18] John Mueller, *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al Qaeda* (Oxford: Oxford University Press, 2010), 192.
[19] The 9/11 Commission Report, 172-173.
[20] Ibid., 215-223.
[21] Staff Statement no.1, "Entry of the 9/11 Hijackers into the United States," The 9/11 Commission Report, 5. Available at: https://govinfo.library.unt.edu/911/staff_statements/staff_statement_1.pdf (accessed April 24, 2019). This statement mentions that at least 4 individuals implicated in the 9/11 plot failed in obtaining visas.
[22] Yosri Fouda and Nick Fielding, *Masterminds of Terror: Het Ware Verhaal Achter 11 September* (Utrecht & Antwerpen: Kosmos-Z&K Uitgevers, 2003), 152.
[23] Assaf Moghadam, "How Al Qaeda Innovates," *Security Studies* 22, no. 3 (2013): 486. The Bojinka plot was an idea by Youssef to blow up a dozen US airliners in Asia. This plot failed after a fire in their apartment drew attention of law enforcement agencies. Moreover, Stephen Atkins, *The 9/11 Encyclopaedia* (Westport and London: Praeger Security International, 2008), 38 even suggests that the failure of the Group Islamique Armé (GIA) to fly a hijacked

was not always clear for AQ how to cope with such unexpected situations. The Al Qaeda leadership was, for instance, originally hoping to have 25 or 26 operatives during the plot. Yet, they ultimately ended up with 19 operatives.[24] Thus, while its nonroutine nature of technology was less outspoken, the implementation of 9/11 can still be characterised by a nonroutine nature of technology.

Going beyond the theoretical relevance of this case, it became clear that this case study simultaneously functions according to the logic of a least-likely case study. The nonroutine nature of technology was less intense compared to the nonroutine nature of technology of the adopted nuclear terrorism scenario. It follows that the extrapolations to a more nonroutine nuclear terrorism scenario would become more plausible in case such dynamics can be identified throughout the implementation of 9/11. Moreover, case selection was also based on the fact that AQ is often considered to be a traditional example of a terrorist organisation and a potential perpetrator of a nuclear terrorism plot. This case study of a less idiosyncratic terrorist group might benefit our extrapolations to the nuclear terrorism threat. Finally, there is a high number of reliable sources on the actual implementation of the 9/11 plot. Considering the unique character of this attack, its implementation received a lot of governmental and scholarly attention. This strengthens the accuracy of the empirical evidence.

8.2. Organisational challenges

The following section will elaborate on the organisational challenges at play throughout the implementation of 9/11. It is structured according to the previously identified organisational dimensions and its corresponding challenges: resource support, level of autonomy, information-sharing, and clear and compelling goals. Next, I will expand on the group's organisational design and how it influenced the implementation of this nonroutine project. Finally, I will elaborate on the extrapolations that follow from this case study to the adopted nuclear terrorism scenario. This way, this chapter aims to verify and reflect in more depth upon the previous insights and the formulated hypotheses on the relation between the organisational design and the nuclear terrorism threat.

aircraft into the Eiffel Tower in December 1994 learned AQ that they would need trained pilots to carry out their plans. This idea has also been suggested by Gaetano Ilardi, "The 9/11 Attacks," 173–175.

[24] The 9/11 Commission Report, 235; McDermott, *Perfect Soldiers,* 229.

8.2.1. Resource support

The recruitment and allocation of individuals with the necessary techne and metis was essential to the effective implementation of this nonroutine project. Al Qaeda experienced various complications throughout this process. Yet, even if this came at the expense of some operational security, AQ did succeed in recruiting and allocating a sufficient number of experts to the 9/11 plot. Moreover, sufficient material resource support contributed to the optimal exploitation of these experts. This was beneficial to the effective implementation of this nonroutine project.

Al Qaeda was simultaneously a small core group and a broader network. The members of the inner core swore fealty to Bin Laden. This group was characterised by relatively well-defined positions and tasks.[25] At the same time, Al Qaeda was also a part of a more informal network of horizontal relations and alliances. It was both a supporter and beneficiary of the facilities of the global network of Islamist movements.[26] Its relationship with the Taliban gave them a particularly strong position in Afghanistan. U.S. intelligence estimates put the "total number of fighters who underwent instruction in Bin Ladin-supported camps in Afghanistan from 1996 to 9/11 at 10,000 to 20,000."[27] Al Qaeda thus had a broad pool of potential operatives at its disposal. This was important to the success of 9/11. First, it enabled Al Qaeda to adopt "the ideas and work of enterprising and strong-willed field commanders who enjoyed considerable autonomy."[28] Indeed, it was Khalid Sheikh Mohammed who introduced the idea of the 9/11 plot to the small core group. Second, Al Qaeda's broad network gave the organisation access to a high number of potential operatives, money and logistical support. The Hamburg cell originally intended to go to Chechnya to fight against the Russians. Yet, an Al Qaeda operative convinced them to go to a training camp in Afghanistan.[29] The Hamburg cell's motivation, English skills and familiarity to the West proved to be essential to the effective implementation of 9/11. Likewise, the fourth pilot and the other muscle hijackers were also selected from Al Qaeda's training camps. Al Qaeda could select the best operatives. This benefitted the effective implementation of the plot.

Yet, Al Qaeda also experienced various complications throughout the recruitment and employment of these experts. First, Bin Laden, Atef and KSM originally wanted to assign loyal and experienced

[25] Byman, "Al-Qaeda as an Adversary," 149 states that this small inner group probably numbered in the hundreds.
[26] Byman, "Al-Qaeda as an Adversary," 149; Jenkins, "The Organisation Men," 13; The 9/11 Commission Report, 65-67;
[27] The 9/11 Commission Report, 67.
[28] Ibid., 145.
[29] Jacob Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organisation* (Princeton: Princeton University Press, 2013), 13; The 9/11 Commission Report, 160-169.

Mujahideen to this important operation. They valued loyalty over skill.[30] Yet, KSM stated that they had problems with selecting people familiar with the West.[31] Al Qaeda consequently decided to make use of the operational advantages of the Hamburg cell. Yet, this implied increased risks with regards to the potential betrayal of the organisation or the defection of one of these persons.[32] The Hamburg-cell did pledge loyalty to Bin Laden. Yet, they were not comprehensively tested in training camps or operations.[33] Second, the 9/11 plot was originally envisaged to be implemented by 25 or 26 operatives instead of 19 operatives. The muscle hijackers did not require any extraordinary skills. Selection of the muscle hijackers was based on their willingness to martyr themselves, demonstrable patience, and the likelihood that they would not raise alerts.[34] Yet, a number of muscle hijackers were not selected or dropped out. The reasons for this vary from a failed visa application, being turned away by an immigration officer on arrival, or "lacking the necessary temperament."[35] This might have had an impact on the effective implementation of the plot. For instance, although this remains in the realm of speculation, it could be the case that flight 93 would have effectively reached its intended target if there would have been 5 or 6 hijackers on board instead of 4 hijackers. These examples illustrate that various security considerations are of particular relevance to a terrorist organisation that aims to implement a nonroutine project. Al Qaeda adapted to various operational difficulties at the expense of some operational security. Yet, it is clear that the recruitment and employment of well-skilled and loyal individuals is not as straightforward as often assumed.

Next, sufficient material resource support contributed to the optimal exploitation of these experts. First, the operatives enjoyed sufficient financial support. Khalid Sheik Mohammed proposed his plan to Al Qaeda because he knew that it had the necessary resources.[36] The overall cost of the endeavor is estimated to circle around $ 400.000 – 500.000. This is generally considered to have been relatively cheap for Al Qaeda. It is estimated that this terrorist organisation spent around $30 million per year to sustain their activities prior 9/11.[37] Illustrative is the fact that the hijackers returned about $26.000

[30] The 9/11 Commission Report, 155 – 160; Michael Levi, *On Nuclear Terrorism* (Cambridge & London: Harvard University Press, 2009), 48.
[31] Fouda and Fielding, *Masterminds of Terror,* 122. He was probably referring to Mihdhar and Hazmi's poor English language skills or to Binalshibh's failed attempts to obtain a U.S. visa.
[32] Levi, *On Nuclear Terrorism,* 48.
[33] The 9/11 Commission Report, 166; 233-235. The 9/11 commission report states in this context that Bin Laden was praised by KSM for his ability to quickly recognize and select talented and devoted people.
[34] Ibid., 233-235.
[35] Ibid., 235 & 525.
[36] Ibid., 149.
[37] Terrorist Financing Staff Monograph, "The Financing of the 9/11 plot," *The 9/11 Commission Report,* 143-144. Available at: https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_App.pdf (accessed April 24, 2019).

dollar of leftover funds to Al Qaeda before 9/11.[38] These people thus had no problems to, e.g., live in the U.S., pay for their flight school, or do the preparatory case runs. This limited their frustrations, operational delays and errors. Second, AQ's broad network facilitated the logistical support to these key operatives throughout the implementation of the plot. They could consequently dedicate themselves to the tasks and activities that they had to implement. This was beneficial to the effective implementation of this nonroutine project.

8.2.2. Level of autonomy

This case study supports the idea that experts need to have control over its operational tasks and activities. This strengthens the likelihood that they can effective implement a nonroutine project. In general, the key-operatives throughout the implementation of 9/11 retained operational decision-making power while simultaneously guaranteeing the security of the plot. There was limited top-down interference in the implementation of 9/11. Simultaneously, however, this case study entails some indications with regards to the security risks related to higher levels of operational autonomy.

Bin laden set out "a flexible strategy for the group that functions at multiple levels, using both top down and bottom up approaches."[39] On the one hand, this implied that Al Qaeda was open to bottom-up ideas. Bin Laden received numerous ideas for terrorist operations. One of these ideas was the grandiose plot by KSM, whom originally did not formally join Al Qaeda.[40] The input of an operationally autonomous expert thus provided the impetus of the 9/11 plot. On the other hand, the small core group sometimes acted in a more top-down manner. This was the case for a highly visible and valuable attack such as the 9/11 plot. Bin Laden and Atef played an important role in this plot by "selecting the operatives for the attack, funding the operation, and, perhaps most critically, insisting that the operation go forward despite dissent voiced by several senior members of the group."[41] This is in line with the argument that was formulated after the previous case studies. The leadership should focus the group's implementation efforts and support it with sufficient resources. Yet, importantly, the leadership did not go as far as interfering with the plot's operational implementation. Illustrative is the following passage.

> Bin Ladin's consistent priority was to launch a major attack directly against the U.S. He wanted the planes operation to proceed as soon as possible. Mihdhar reportedly told his cousin during

[38] The 9/11 Commission Report, 252
[39] Hoffman, "Lessons of 9/11," 13.
[40] The 9/11 Commission Report, 154.
[41] Moghadam, "How Al Qaeda Innovates," 479.

> the summer of 2001 that Bin Ladin was reputed to have remarked, "I will make it happen even if I do it by myself." According to KSM, Bin Ladin had been urging him to advance the date of the attacks. In 2000, for instance, KSM remembers Bin Ladin pushing him to launch the attacks amid the controversy after then-Israeli opposition party leader Ariel Sharon's visit to the Temple Mount in Jerusalem. KSM claims Bin Ladin told him it would be enough for the hijackers simply to down planes rather than crash them into specific targets. KSM says he resisted the pressure. KSM claims to have faced similar pressure twice more in 2001…On both occasions KSM resisted, asserting that the hijacking teams were not ready.[42]

Key operatives had sufficient discretionary power to select what, when and how to do their work. This was beneficial to the effective implementation of the plot. They, e.g., did not simply down the planes. Besides the important role played by KSM, Mohammed Atta was also of significant value to the effective implementation of the plot. He was the operational leader of the Hamburg cell and coordinated the day-to-day affairs.[43] He, for instance, took care of the arrival of the hijackers in the U.S., decided on the allocation of the hijackers in the teams, played an important role in deciding upon the exact targets (e.g. arguing that the White House would be too difficult to attack) and set the exact date of the attacks. Key operatives thus enjoyed a relatively high level of decision-making power.

The effective implementation of 9/11 illustrates that such levels of operational autonomy can be combined with securing a nonroutine plot. Yet, this case study simultaneously indicated that there are some security risks related to such autonomous decision-making power. First, Al Qaeda was aware of these risks. The leadership took some precautions to avoid divergent behavior by its operatives. One potential muscle hijacker was, e.g., "not selected for the 9/11 attacks because the Al Qaeda leadership considered him too high-strung and lacking the necessary temperament."[44] The muscle hijackers were thoroughly vetted. Moreover, KSM and Binalshibh did, e.g., not bring Zacarias Moussaoui into contact with other operatives. Moussaoui has been suspected to be a back-up pilot. Yet, his incompetent behavior led his flight instructor to inform the FBI.[45] He was arrested a couple of weeks before 9/11.[46] Contact with other operatives could have endangered the implementation of the plot. Second, notwithstanding these security measures, there were some instances of divergent behavior. For instance, the Hamburg cell was less thoroughly vetted. A friction developed between Atta and Jarrah -

[42] The 9/11 Commission Report, 250.
[43] Fouda and Fielding, *Masterminds of Terror,* 83.
[44] The 9/11 Commission Report, 526.
[45] Michael Kenney, "'Dumb' Yet Deadly: Local Knowledge and Poor Tradecraft Among Islamist Militants in Britain and Spain," *Studies in Conflict & Terrorism* 33, no. 10 (2010): 917.
[46] Fouda and Fielding, *Masterminds of Terror,* 183.

two of the three pilots of the Hamburg cell. Jarrah may even have considered dropping out of the operation. This is believed to have stemmed from his frequent contact with his girlfriend and family and his sense of isolation and exclusion from decision-making.[47] This could have interrupted the effective implementation of the 9/11 plot. Likewise, Hazmi - one of the muscle hijackers - reportedly telephoned a former companion in late August that something big would soon happen.[48] Such kind of indiscretions could be detected by law enforcement agencies. These instances of divergent behavior by the operatives held the potential to lead to the interruption of the plot.

8.2.3. Information-sharing

This case study supports the idea that information-sharing benefits the effective implementation of a nonroutine plot. It enables the creative combination of knowledge. Various security mechanisms limited the information-exchange throughout the implementation of 9/11. Yet, this plot was nevertheless characterised by the establishment of sufficient coordination and communication tools. This was necessary to effectively implement the plot. Yet, it simultaneously implied increased security risks.

Al Qaeda established various security mechanisms to secure the implementation of the 9/11 plot. A manual of behavior was given to operatives who would carry out operations in the West. This manual proclaimed, e.g., that undercover members should "not resort to utilizing letters and messengers except in an emergency."[49] McDermott notes in this context that "Al Qaeda knew its electronic communications were susceptible to high-tech interception. If something important needed to be said, messages were passed by courier or in face-to-face meetings."[50] Moreover, details of the 9/11 plot were not widely shared within the Al Qaeda organisation. Only a limited number of people are suspected to have been aware of the plot (e.g. some people of the senior AQ leadership, Atef, KSM, Binalshibh and the pilots). The muscle hijackers, e.g., only learned about the full details of the plot when arriving in the U.S.[51] They were relatively easy to replace. This limited diffusion of knowledge strengthened the security of the plot. Yet, sufficient information-exchange, consultation and coordination was indispensable to the effective implementation of this nonroutine project.

[47] Staff Statement no. 16, "Outline of the 9/11 plot," 18. Note in this context that Zacarias Moussaoui might have been part of a contingency plan to replace Jarrah. Yet, as mentioned earlier, Moussaoui was arrested.
[48] The 9/11 Commission Report, 249.
[49] Atkins, *The 9/11 Encyclopaedia,* 345 -347.
[50] McDermott, *Perfect Soldiers*. 222
[51] Fouda and Fielding, *Masterminds of Terror,* 144; The 9/11 Commission Report, 236.

Indeed, this is already demonstrated by the fact that the plot originated from a bottom-up idea by a Jihadi entrepreneurs such as KSM. Al Qaeda solicited ideas from their broad network. This increased the likelihood that someone would come up with a creative approach. It stimulated thinking outside of the box.[52] Moreover, considering the actual implementation of the plot, Ramzi Binalshibh stated:

> Considering your question about the coordination of 9/11, it was all about connecting different departments, developing communication between these departments on the one hand and the headquarters in Afghanistan on the other hand, and determining priorities for each of these departments. [53]

There was a diversity of tasks that needed to be completed and attuned to each other. This required sufficient communication and coordination tools. It is illustrative that various meetings between key operatives were organised in order to coordinate the implementation of the plot (e.g. in Kuala Lumpur in 2000, in Madrid in July 2001, or in Las Vegas in the summer of 2001).[54] Moreover, various persons (e.g. Ramzi Binalshibh and Said Bahaji) took up coordinative or liaison roles between the key operatives, KSM and the Al Qaeda leadership. These persons were necessary to serve as a conduit between the different actors involved.[55] Finally, there were various face-to-face meetings between key-operatives in the months before the attack. Mohammed Atta and Nawaf el-Hazmi, for instance, regularly met to discuss and prepare the implementation of the planes operation.[56] It allowed them, e.g., to share intelligence and information which was gained via case runs by the hijackers.[57] This diversity of coordination and communication tools thus enabled the project team to effectively implement this nonroutine project.

Yet, this level of information-exchange simultaneously implied increased security risks. Al Qaeda established particular security measures and could exploit a relatively lenient counter terrorism environment. Yet, there were nevertheless a number of opportunities for counterterrorism efforts to detect and disrupt the implementation of the 9/11 plot. It is not without reason that chapter 8 in the 9/11 commission report is named "the system was blinking red." For instance, after 9/11, it was found that a high number of communications between Atta and Binalshibh had taken place in the month of

[52] Moghadam, "How Al Qaeda Innovates," 482-484.
[53] Fouda and Fielding, *Masterminds of Terror,* 127. This quote is a translated from Dutch.
[54] Ibid., 145.
[55] Atkins, *The 9/11 Encyclopaedia,* 28.
[56] The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, "Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001," 140.
[57] Ilardi, "The 9/11 Attacks," 173–175.

August.[58] Moreover, there were some late leads that held the potential to detect or disrupt the implementation of the plot. Khalid al-Midhar was a known AQ operative and identified as a participant during the Kuala Lumpur meeting. He was one of the original pilots who turned out to become a hijacker in the 9/11 plot. Yet, he could enter the U.S. and was subsequently not located while in the U.S.[59] Likewise, the so-called Phoenix memo warned for a coordinated effort by Bin Laden to send students to the U.S. to attend civil aviation schools.[60] A more stringent follow-up on this memo could have disrupted the implementation of the plot. Unfortunately, counterterrorism efforts did not pick up on these security flaws that inherently follow from such communication and coordination efforts.

8.2.4. Clear and compelling goals

This case study supports the idea that clear and compelling goals advance the effective implementation of a nonroutine plot. Clear and compelling goals are important in strengthening the coherence and perseverance of the project team. It reduces the likelihood of divergent behavior. Yet, the formulation of such clear and compelling goals is not self-evident and might imply particular security risks. To be precise, any unsuccessful attempt to compel someone about the group's operational and organisational goals might actually increase the security risks related to the defection or detection of that person.

First, considering the issue of clear goals, it is true that only a limited number of people was aware about the full details of the 9/11 plot. Yet, the operational goals of this project were clear to these key operatives relatively early in the development of the plot. For instance, Atta, Al Shehhi and Jarrah (who would become the pilots) and Binalshibh (who would take up an important coordinative function) were likely informed about this plot around late 1999.[61] This was important for them to steadily progress and remain focused. For instance, while Bin Laden at one point wanted to accelerate the mission, these key operatives and KSM decided not to expedite the implementation of the plot. The team was not yet ready to achieve the exact operational goals. This increased the effective implementation of the plot. As mentioned earlier, they flew the planes in the targets rather than just crashing them somewhere.

[58] The 9/11 Commission Report, 248.
[59] Fouda and Fielding, *Masterminds of Terror,* 137; Atkins, *The 9/11 Encyclopaedia,* 180; The 9/11 Commission Report, 266-272.
[60] The 9/11 Commission Report, 273-276. A copy of the Phoenix memo is available at: https://www.investigativeproject.org/documents/case_docs/1171.pdf (accessed April 24, 2019).
[61] The 9/11 Commission Report, 166.

Second, considering the issue of compelling goals, Al Qaeda's narrative and ideology enjoyed a particular appeal to some Muslims. This provided the organisation with a large pool of potential operatives to implement the plot (e.g. the muscle hijackers).[62] It provided Al Qaeda with the necessary resource support. Moreover, besides compelling sufficient people to Al Qaeda's organisational goals, Al Qaeda also succeeded in compelling the key operatives of the operational goals of 9/11. The Hamburg cell's operational advantages led them to be selected for this plot relatively quickly. This implied increased risks with regards to the potential betrayal of the organisation or the defection of one of these persons. Yet, Atkins mention in this respect that "Atta ranked high in all the attributes of an Al-Qaeda operative – intelligence, religious devotion, patience, and willingness to sacrifice."[63] The project team was compelled by 9/11s operational objectives. This was beneficial to the effective implementation of this plot.

Yet, the formulation of clear and compelling goals is not as straightforward as often assumed. Moreover, it might imply particular security risks to the organisation. The Al Qaeda leadership was clearly sensitive to this issue. As illustrated, e.g., they rejected a potential muscle hijackers because he was "lacking the necessary temperament."[64] Yet, notwithstanding such security measures, Al Qaeda could not completely exclude the possibility of (moral) doubts by one of its operatives.

> Jarrah clearly differed from the other hijackers in that he maintained much closer contact with his family and continued his intimate relationship with Senguen (his wife). These ties may well have caused him to harbor some doubts about going through with the plot, even as late as the summer of 2001.[65]

Ziad Jarrah was one the pilots of the 9/11 plot. He was informed about the entire plot. Yet, he was not as ruthless as the others key operatives.[66] It is probably no coincidence that Jarrah was the one who had particular arguments with Mohamed Atta. KSM and Binalshibh already thought of a replacement (Zacarias Moussaoui) in case Jarrah would drop out. Moreover, it is probably neither a coincidence that Jarrah did not live together with the others operatives of the Hamburg cell. McDermott notes about these other operatives that "a spirit of easy brotherhood often prevailed within the group. However extreme its aims, it was a kindred community. The men shared apartments, bank accounts, and cars."[67]

---

[62] Fouda and Fielding, *Masterminds of Terror,* 122.
[63] Atkins, *The 9/11 Encyclopaedia,* 23.
[64] The 9/11 Commission Report, 235 & 525.
[65] Ibid.*,* 168.
[66] Atkins, *The 9/11 Encyclopaedia,* 163.
[67] McDermott, *Perfect Soldiers*, 61.

They formed a cohesive group. Jarrah was not equally socially included in this group. Thus, although Jarrah ultimately did participate in the 9/11 plot, this example demonstrates how any uncompelled participant might undermine the effective implementation of a nonroutine plot.[68]

Finally, it should be noted that Bin Laden insisted "that the operation go forward despite dissent voiced by several senior members of the group."[69] Al Qaeda and the Taliban argued about their broader strategy for 2001. The 9/11 plot was only one element of this broader strategy. Some opposed a major operation against the United States because, e.g., it might draw the Americans into war against them.[70] Yet, Bin Laden succeeded in pushing through the implementation of this plot. This highlights the important role of the leadership in providing clear and compelling goals to the operatives.

8.3. Al Qaeda's 9/11 plot: features of an organic design

This chapter will now turn from description to exploration. I will elaborate on how the organisational design influenced the implementation of 9/11. The organisational design shaped some of the main organisational challenges throughout the implementation of this nonroutine project. The following section will link the four aforementioned organisational dimensions – and its challenges – to the organisational design.

In short, this section aims to demonstrate that – notwithstanding the fact that the nonroutine nature of technology was less outspoken - the organic design features of Al Qaeda's organisational design benefitted the effective implementation of the 9/11 plot. Yet, these organic design features simultaneously implied particular security risks to the organisation (see table 8.1).

[68] This remains in the realm of speculation. Yet, it is worth noting that Jarrah was the pilot of flight 93. This was the only flight that did not reach its target. To which extent his attitude played a role in this remains unknown.
[69] Moghadam, "How Al Qaeda Innovates," 479; The 9/11 Commission Report, 250.
[70] The 9/11 Commission Report, 251.

Table 8.1. Organisational design of the group that implemented 9/11

	Organisational design of the group that implemented 9/11
Level of interconnectedness	Sufficiently high number of intra-division and inter-division connections
Level of hierarchy	Sufficiently high level of control over operations by experts themselves + sufficient resource support to them.
Level of specialisation	Sufficiently high level of personal specialisation (sufficiently high levels of both techne and metis)

* Note that this table is inherently arbitrarily to some extent. It is difficult to assign exact and uniform values to these design parameters.

First, it is true that a large part of the relatively small project team did not require particularly high levels of personal specialisation. For instance, although the muscle hijacker did enjoy training in Al Qaeda's training camps, they did not have to have any extraordinary skills or knowledge. Nevertheless, the implementation of 9/11 did require some individuals with the necessary techne and metis. This refers to, e.g., the pilots' ability to hijack and fly a plane or the familiarity to the West by the Hamburg cell. This latter example particularly stresses the relevance of *metis.* Even if the required level of personal specialisation was relatively low, it does remain true that these key operatives were essential to the effective implementation of this plot. Al Qaeda's organisational design was beneficial to the recruitment and employment of these experts. Al Qaeda was, e.g., open to outside ideas and willing to turn to relatively new recruits with the necessary operational skills.

Second, these experts were able to operate at a sufficiently high functional capacity. One the one hand, the Al Qaeda leadership provided the key operatives with a clear and compelling operational goal. Moreover, they also provided them with sufficient resource support. This was beneficial to these experts' focus and perseverance. On the other hand, the key operatives involved were allowed sufficient operational decision-making power with respect to the implementation of this nonroutine plot. The leadership was not absent during the implementation of the plot. Yet, they neither excessively interfered top-down in its actual implementation. The key operatives, for instance, succeeded in fencing off Bin Laden's desire to expedite the execution of the plot. This organic design feature strengthened the flexibility and adaptability of the operatives involved in this plot. It is illustrative in this context that the muscle hijackers merely followed orders from these key-operatives and the Al Qaeda leadership. They did not have a similar level of personal specialisation and did not require a similar level of

operational autonomy. These muscle hijackers could thus be controlled and coordinated in a more top-down manner.

Finally, the effective implementation of 9/11 was also a function of sufficient communication and coordination tools. The number of connections might have been relatively low compared to the number of connections in the previous case studies. Yet, there were an adequate number of connections between different cells and within the group of key operatives. This is illustrated by, e.g., Al Qaeda's openness to outside information and ideas, the coordinative role by Binalshibh, or the various meetings and face-to-face interactions between different key operatives in the plot (e.g., Atta, Binalshibh and KSM). This organic design feature was essential in effectively completing the 9/11 plot. It was necessary to attune the diversity of tasks and activities that needed to be completed throughout this nonroutine project

The project team that implemented 9/11 was thus characterised by some organic design features. The nonroutine nature of technology of this plot was less outspoken. Yet, these organic design features benefitted the effective implementation of this project. It is a problem-solving design. Moreover, in general, this case study simultaneously supports the idea that such an organisational design implies increased security risks. I will illustrate this by zooming in on the three organic organisational design features.

First, the need to recruit and employ experts in a clandestine operational environment inherently implied increased security risks. For instance, the turn to relatively new recruits with the necessary operational skills implied increased security risks to the organisation. The doubts by Jarrah illustrate that this increased the risks with regards to the potential defection of one of the key operatives. Second, the operational autonomy by some of the key operatives implied an increased risk of divergent behavior by these experts. These risks did not materialize. Yet, the friction between Atta and Jarrah, or the arrest of Zacarias Moussaoui, illustrate the risks related to an increased level of operational control by autonomous operatives. Finally, an increased number of interconnections inherently implied an increased risk that law enforcement agencies could detect the plot. The 9/11 commission report noted, e.g., a "confluence of information regarding Khalid Sheikh Mohammed [was] received by the intelligence community in the summer of 2001."[71] Unfortunately, none of these security risks actually materialized. The 9/11 plot was not detected or disrupted.

[71] The 9/11 Commission Report, 276.

8.4. Extrapolations to the nuclear terrorism threat

Considering the focus of this study, the question now becomes to what extent these insights might also be applicable to a nuclear terrorism project. This case study of a nonroutine terrorism project was selected according to the logic of a least-likely case study. There were substantial differences with the adopted nuclear terrorism scenario (e.g. the less outspoken nonroutine nature of technology; the smaller size of the project). These qualifying conditions imply that the extrapolations with respect to the formulated hypotheses about the adopted nuclear terrorism scenario become more plausible in case similar dynamics were identified throughout the implementation of 9/11. In order to accumulate knowledge on this understudied dimension, this section follows the same structure as used in the previous chapters.

8.4.1. Effectiveness…

Considering the fit between the organisational design and the nonroutine nature of technology, this final case study supports the plausibility of the hypothesis that "a terrorist organisation is most likely to effectively complete a nuclear terrorism project by means of an organisational design similar to an organic design." (=H1) The nonroutine nature of technology of 9/11 was less outspoken. Correspondingly, the organic organisational design of the group that implemented 9/11 was less outspoken (compared to the organic organisational design at Los Alamos or the PNE program). Yet, it does become clear that the organic design features of this group did benefit the effective implementation of 9/11.

First, this case study supports the importance of people with the necessary skills in order to cope with a plot with a high task variability and low task analysability. The less outspoken nonroutine nature of technology of this case study alleviated the requirements with respect to the human resources. Nonetheless, this case study does demonstrate that human resources with the necessary skills are essential to the effective implementation of a nonroutine project. AQ had a pool of potential operatives at its disposal. This is in line with the argument that resourceful and popular rebel groups can adopt expertise-oriented recruitment periods.[72] It provided Al Qaeda, for instance, with access to the Hamburg cell. The recruitment and employment of this group came at the expense of some operational security. Yet, its operational techne and metis was indispensable to the effective implementation of the 9/11

[72] Steven Windisch, Michael Logan, and Gina Scott Ligon, "Headhunting Among Extremist Organisations: An Empirical Assessment of Talent Spotting," *Perspectives on Terrorism,* 12, no. 2 (2018): 19."

plot. It follows that it remains plausible to assume that such experts will also be of essential importance in a nuclear terrorism plot.

Second, this case study also supports the idea that these experts' functional capacity will rise if they can operate in an organic-like organisational design. On the one hand, the leadership succeeded in initiating the plot (notwithstanding some dissenting voices), providing adequate resource support to its implementation, and formulating clear and compelling goals. This way, the political and ideological leadership focused and supported the group's implementation efforts. On the other hand, this type of organisational design allowed for sufficient levels of operational autonomy and information-sharing. First, although there were some attempts of top-down interfering in the implementation of this plot, key operatives succeeded in fencing off these attempts and safeguarding their operational decision-making power. There were no tight intermediary goals, stringent timing requirements, or top-down meddling in the day-to-day affairs. This benefitted the effective implementation of this nonroutine plot. This is in clear contrast with what I have found during the implementation of Aum's CB armament activities. Second, there were sufficient communication and coordination tools between the different cells and within the group of key operatives (e.g. meetings, liaison persons, and face-to-face meetings). This was necessary to effectively complete the different tasks and activities. It strengthened the team's flexibility, creativity, and adaptability. Thus, even though the less outspoken nonroutine nature of technology alleviated the requirements with respect to these organic design features, this case study does support the idea that an organisational design that allows for sufficient operational autonomy and information-sharing will increase the likelihood that a terrorist organisation can effectively implement a nuclear terrorism plot.

The support for this hypothesis is of particular relevance due to the fact that the implementation of 9/11 was selected according to the logic of a least-likely case. It might be expected that the likelihood and intensity of these dynamics will increase in case of a more nonroutine nature of technology. It thus strengthens the general plausibility of this hypothesis. Yet, this case study simultaneously functions as a stark reminder that other factors (e.g. the complexity of the project and the organisation's attitude towards risk-taking) cannot be neglected. The organisational design is no omnipotent causal force.

8.4.2. Versus efficiency

An organisational design with organic design features is thus still expected to strengthen the likelihood that a terrorist organisation can effectively complete a nuclear terrorism project. Next,

notwithstanding its less outspoken nonroutine nature of technology, this case study simultaneously lends support to the hypothesis that such an organisational design would imply substantial security risks to the terrorist organisation (=H2). Moreover, adopting an instrumental-rational perspective, this case study neither provides us with any reason to theoretically refute the plausibility that a nuclear terrorism plot can be perceived to be an inefficient strategy (=H3).

First, it remains plausible to assume that an organisational design similar to an organic design implies increased security risks to a terrorist organisation (=H2). The implementation of this project with a less outspoken nonroutine nature of technology was characterised by a less outspoken organic organisational design. Nevertheless, zooming in on the three identified organisational design features supports the argument that a more organic organisational design would imply increased security risks. Finding support for this hypothesis in this case study strengthens its plausibility.

Al Qaeda enjoyed a relatively high level of popular support. Its broad pool of resources enabled the organisation to recruit and employ the necessary operatives with *specialised* skills. Yet, AQ did experience some problems in recruiting and employing these experts (e.g. the ill-preparedness of trusted operatives or the fact that there were too few muscle hijackers). Al Qaeda demonstrated some flexibility in valuing loyalty over skills. Yet, it might be assumed that this dilemma would be more pressing in the adopted nuclear terrorism scenario. The required skills for the implementation of 9/11 were not as demanding as they would be during the implementation of the adopted nuclear terrorism scenario. It is telling in this context that Al Qaeda never went as far as actively recruiting outside pilots. This might have been considered to be too risky. This underlines the importance of the loyalty of a terrorist group's operatives. Extrapolating these insights to a nuclear terrorism plot, it suggest, e.g., that the recruitment of disgruntled scientists might not be as straightforward as often assumed.

Next, this case study supports the idea that allowing for an adequate level of *operational autonomy* while trying to limit divergent behavior is a complex balancing act for any terrorist organisation. The friction between Atta and Jarrah, or the arrest of Moussaoui, illustrate the security risks that might follow from too little operational control over the experts. Such risks do not necessarily materialize. Yet, considering this issue has also been identified in this less nonroutine project, it is plausible to assume that this balancing act will also play a pressing role in a nuclear terrorism plot. It is interesting to note in this context that this case study also stresses the relevance of a clear and compelling common goal. It is illustrative that Jarrah was not living together with the other key operatives in Hamburg. The cohesion of the project team might be influenced by a variety of factors. This is likely to play an important role throughout the implementation of a nuclear terrorism plot as well.

Considering the number of *interconnections*, AQ established particular security measures that limited the information-exchange between the different cells and within the group of key operatives (e.g. details of the plot were not widely shared within the organisation, electronic communication was limited). It is probably no coincidence that the implementation of the plot took over 2.5 years. Various security measures might slow down the effective implementation of such a nonroutine plot. Nevertheless, notwithstanding these security measures, there were a number of opportunities for counterterrorism efforts to detect and disrupt the implementation of the plot. A higher number of interconnections would likely have heightened these security risks. Moreover, AQ could exploit a relatively lenient counter terrorism environment. Today's counterterrorism environment seems to be more stringent. It thus remains plausible to assume that an increased number of communication and coordination tools in a nuclear terrorism plot would inherently imply increased security risks.

Second, this case study did not gave us any reason to theoretically refute the idea that a nuclear terrorism plot can be perceived to be an inefficient strategy (=H3). In general, this case study supports this research project's starting assumption that a terrorist organisation can be expected to strategically reflect on this type of high-end plots. Al Qaeda can be characterised by a virulent and dichotomous ideology and worldview. This might be considered to be value-rational to some extent.[73] Yet, it also became clear that senior leadership did assess the instrumental value of the 9/11 plot. Al Qaeda's leadership contemplated the original grandiose plan by KSM and the potential strategic consequences of the 9/11 attack. By July 2001, a schism occurred among the senior leadership. Various weighty figures were opposing the 9/11 attack. One of the worries was, e.g., that it would draw the Americans in a war against them while the Taliban leaders were planning a military offensive against the Northern Alliance.[74] It thus remains plausible to assume that a terrorist organisation contemplating a nuclear plot will also strategically assess its options and interests.

Next, even though Al Qaeda's virulent ideology and dichotomous worldview pushed them to the 9/11 attack, it can be argued that this was not a good strategic decision. In hindsight, it seems that Al Qaeda experienced substantial negative consequences after the tactical success of 9/11. Al Qaeda did enjoy various beneficial conditions. It enjoyed a relatively high level of popular support. This is in line with the argument that stressed the importance of the legitimacy of the organisation and its goals. Moreover, Al Qaeda enjoyed a relatively lenient counter terrorism environment. For instance, the hijackers made it

[73] Note, in this context that Weber already links value-rationality to religion. He defined value-rationality as determined by a conscious belief in the value for its own sake of some ethical, aesthetic, *religious*, or other form of behavior, independently of its prospects of success. Max Weber, *Economy and Society: An Outline of Interpretive Sociology* (Berkeley, Los Angeles, London: University of California Press, 1978), 25.
[74] The 9/11 Commission Report, 251.

through U.S. airports of entry in 33 of the 34 attempts.[75] These beneficial conditions alleviated various of the security concerns related to the various organic organisational design features. Yet, notwithstanding these beneficial conditions, Al Qaeda did not effectively achieve its strategic and political goals. Abrahms argued that the 9/11 attacks "were certainly counterproductive in reducing U.S. military interference in the Persian Gulf… failed to destroy U.S. relations with pro-American Muslim leaders… failed to deter the U.S. from supporting military interventions that kill Muslims…[and] failed to end U.S. support of Israel."[76] Adopting an instrumental-rational approach, one can thus place substantial question marks to the likely strategic and political success of a potential nuclear terrorism plot.

8.5. Conclusion

Al Qaeda's implementation of 9/11 was the final case study of this research project. Besides the theoretical relevance of this nonroutine terrorism plot, Al Qaeda is also often considered to be a classic example of a terrorist organisation that is interested in a nuclear terrorism plot. Moreover, the less outspoken nonroutine nature of technology allowed for this case to function according to the logic of a least-likely case study. This way, this case study enabled this research project to better assess the extrapolations and qualifying conditions that were identified in the previous case studies.

In general, this case affirmed the relevance of the organisational design in adopting a nonroutine project. This strengthens the plausibility that the organisational design will also impact the implementation of a nuclear terrorism plot. Next, more specifically, the implementation of 9/11 did not provide us with any reason to theoretically refute the plausibility of the suggested effectiveness-efficiency trade-off. This case study was characterised by a less outspoken nonroutine nature of technology. Yet, similar organisational dynamics and challenges were at play throughout the implementation of this plot. This group's organic design features benefitted the effective implementation of 9/11. These organic design features however simultaneously implied increased security risks to the terrorist organisation. Finding support for this argument in this case generally supports the idea that it deserves attention in traditional nuclear terrorism threat assessments. Moreover, adopting an instrumental-rational approach, this case study also provided support to the idea that a nuclear terrorism plot does not seem to be an efficient strategy. Notwithstanding various beneficial variables, Al Qaeda did not effectively achieve its strategic and political goals via the

[75] Staff Statement no.1, 'Entry of the 9/11 Hijackers into the United States."
[76] Max Abrahms, *Rules for Rebels: the Science of Victory in Militant History* (Oxford: Oxford University Press, 2018), 20-24.

implementation of 9/11. It appears to be unlikely that a nuclear terrorism plot would enable a terrorist organisation to achieve more success.

Reflecting upon the four case studies in this research project, it became clear the organisational design is no omnipotent causal force. Other variables will also play a role in the nuclear terrorism threat. This case study suggested, for instance, that the exact nuclear terrorism scenario (and its corresponding nonroutine nature of technology), the organisation's attitude towards risk-taking and its level of popular support will also influence the probability that a terrorist organisation might effectively implement a nuclear terrorism plot. The final chapter of this research project will therefore provide a cross-case analysis on the role of the organisational design and explore how the organisational design might relate to other variables. Moreover, this final chapter will also reflect upon other nuclear terrorism scenarios. This way, this final chapters aims to deepen our understanding of the probability of the nuclear terrorism threat as the output of analysis.

9. Towards a deeper understanding of the nuclear terrorism threat

The goal of this research project was to enable a deeper understanding of the nuclear terrorism threat. Probability assessments on this threat should aim to be the result of an encompassing analysis. I therefore explored a critical gap in today's literature on nuclear terrorism. To be precise, it was important to reflect upon the role and impact of the organisational design of a terrorist group aiming to implement a nuclear terrorism plot. This variable is no omnipotent causal force. Yet, it is remarkable that this dimension has not been identified in-depth and systematically explored in the traditional literature on the nuclear terrorism threat. The final chapter of this research project therefore aims to aggregate, interpret and contextualise this study's most important findings. By doing so, I hope to contribute to the comprehensive nature of future nuclear terrorism threat assessments.

First, this chapter will provide a cross-case analysis on the relation between the organisational design of a terrorist organisation and the nuclear terrorism threat. Each of the four case studies was characterised by a nonroutine nature of technology. Yet, each case was simultaneously heterogeneous with respect to the exact degree of its nonroutine nature and with respect to other organisational contingencies. Thus, while each of the case studies was theoretically relevant, it remains necessary to aggregate these study's findings in order to better understand the nuclear terrorism threat. This chapter will therefore provide a cross-case analysis that brings together the findings of each of the four cases while simultaneously taking into account its qualifying conditions. This analysis will be structured according to the previously introduced effectiveness-efficiency tradeoff (and the corresponding hypotheses of this research project). Moreover, it will simultaneously reflect upon how these extrapolations are related to the three traditional nuclear terrorism variables.

Second, going beyond the adopted nuclear terrorism scenario, this chapter will also reflect upon other nuclear terrorism scenarios. The adopted nuclear terrorism scenario merely provided this research project with a framework for reasoning on the nuclear terrorism threat. It structured a more rigorous reflection upon the role and impact of the organisational design. Yet, as mentioned earlier, there is a myriad of pathways that a terrorist organisation might follow in order to implement a nuclear terrorism plot. This depends on e.g. the terrorist organisation's resources, the (state) assistance it receives, the organisation's political and strategic goals, and its operational opportunity environment. It therefore remains necessary to reflect upon other nuclear terrorism scenarios, how my findings might (or might not) apply to such scenarios, and what this would imply with respect to the nuclear terrorism threat. This way, I hope to further our comprehensive understanding of the nuclear terrorism threat.

9.1. Cross-case analysis

This section will aggregate the insights of each of the four case studies of this research project. In order to do so, I will highlight recurrent findings, take into account potentially qualifying conditions, and explore how these extrapolations relate to the three traditional nuclear terrorism variables: a terrorist organisation's motivation to use an improvised nuclear device, the availability of nuclear know-how and technology, and/or these clandestine organisations' opportunities to obtain fissile material. In order to facilitate this cross-case analysis, this chapter is structured according to the previously introduced idea of the effectiveness-efficiency trade-off. This idea corresponded with this research project's hypotheses and followed out of the fact that the organisational design simultaneously needs to cope with different organisational contingencies; namely the technology the organisation aims to adopt, the group's clandestine environment, and the organisation's strategy.

Table 9.1 and 9.2 aim to provide an overview of some of the most important findings of this study. Yet, note that this table merely aims to introduce and frame the corresponding textual explanation. It does not provide an exhaustive overview of the cross-case analysis.

Table 9.1. Overview of the cases

	Los Alamos	South African PNE program	Aum Shinrikyo	9/11
Nature of technology	Intense nonroutine nature of technology	Nonroutine nature of technology	Nonroutine nature of technology	Less outspoken nonroutine nature of technology
Organisational design	Intense organic organisational design	Various features of an organic organisational design	Various features of a mechanistic organisational design	Features of an organic organisational design
Effectiveness	Effective implementation	Effective implementation	Relatively ineffective implementation	Effective implementation
Security	Enjoyed domestic support + sufficient international legitimacy. Various security breaches, but the project was not interrupted/halted.	Enjoyed domestic support + sufficient international legitimacy Various security breaches, but the project was not interrupted/halted	Enjoyed a relatively secure operational environment and popular support (for a terrorist organisation) Few security breaches, but the plots were halted after detection	Enjoyed a relatively secure operational environment and popular support (for a terrorist organisation) Some security breaches, but the plot was not detected
Strategy	Tactical success Strategic success	Tactical success (Can be considered a) strategic success	Some tactical successes Hard to consider a strategic success	Tactical success Hard to consider a strategic success

Table 9.2. Overview findings of the cross-case analysis

H. 1	The aggregated findings support the idea that it is plausible to expect that a terrorist organisation is most likely to effectively complete a nuclear terrorism project by means of an organisational design similar to an organic design. ➢ Each of the three organic design features imply an increased likelihood that a terrorist organisation can effectively implement a nonroutine project. ➢ The exact requirements with respect to these organic design features are however a function of the exact nonroutine nature of the project.
H. 2	The aggregated findings support the idea that it is plausible to expect that an organisational design similar to an organic design implies increased security risks to a terrorist organisation and its nuclear terrorism project. ➢ Each of the three organic design features imply particular security risks: • The recruitment of people that are both loyal to a terrorist organisation and capable to implement a nuclear terrorism plot is not as straightforward as often assumed. • Allowing for an adequate level of operational autonomy while trying to limit divergent behavior would be a complex balancing act. • A higher level of intra- and inter-cell connections implies an heightened risk of detection by counterterrorism forces ➢ The exact security risks will depend on the exact nuclear terrorism scenario (and other contingent factors). Yet, in general, these security issues deserve more attention in nuclear terrorism threat assessments.
H.3	The aggregated findings support the idea that it is plausible to expect that an organisational design more similar to an organic design implies an increasingly inefficiently functioning terrorist organisation with respect to the attainment of its political and organisational goals. ➢ A value-driven terrorist organisation is expected to be most-likely to initiate such a plot. ➢ We expect an inverse relationship between a terrorist organisation's motivation to go nuclear and its capability to actually implement such a plot

9.1.1. Effectiveness…

Considering the match between the organisational design of a terrorist organisation and the implementation of a nuclear terrorism plot with a nonroutine nature of technology, this study first hypothesised that "a terrorist organisation is most likely to effectively complete a nuclear terrorism project by means of an organisational design similar to an organic design." (=H1) Each of the four case studies generally supports the plausibility of this hypothesis. I will elaborate on this argument in more depth by zooming on the three organic organisational design features. Moreover, I will simultaneously

reflect upon its implications with respect to the three traditional nuclear terrorism variables and the nuclear terrorism threat.

(1) Each of the four cases highlighted the importance of the availability of experts. They need to have the necessary *techne* and *metis* to cope with a nonroutine nature of technology. The American and South African nuclear program both enjoyed access to some of the top experts in their country at that time (and some level of outside help). Likewise, the (limited) tactical successes by Aum Shinrikyo and Al Qaeda was to a large extent function of the specialised skills of the members involved in these respective projects. More distinctively, these case studies furthermore drew special attention to the issue of *metis.* The examples of Johan Slabber's intuition that prevented a criticality accident, or the familiarity with the West by Al Qaeda's Hamburg cell, emphasize the importance of intuitive and practical knowledge. This is in line with Kenney's argument that online operational information is not necessarily accurate nor that it necessarily implies that terrorists have the experiential knowledge to effectively use the information.[1] Extrapolating these insights to the nuclear terrorism threat, this study argues that this issue deserves more thematisation when reflecting upon the availability of *nuclear know-how and technology*.[2] We should not neglect the operational value of online information. Yet, nuclear terrorism threat assessments should neither equate this blindly with a short-cut to a nuclear capacity. Research should assess and recognize when online manuals might e.g. be motivated more by psychological warfare rather than the *motivation* to actually construct such weapons.[3] Likewise, we should not always assume that correct information inherently entails the experiential knowledge to actually implement this knowledge.

Specifically considering the recruitment of such individuals with *specialised* skills, it is true that each case was characterised by different recruitment requirements. Yet, in general, each of the four case studies brought forward that a higher level of popular support and (perceived) legitimacy of the project facilitates the recruitment and allocation of experts with the necessary skills. This is theoretically in line with the argument that resourceful and popular terrorist groups can adopt expertise-oriented recruitment periods. Such terrorist groups can target and select people based on specific criteria.[4] Al

[1] Michael Kenney, "Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists," *Terrorism and Political Violence* 22, no. 2 (2010): 177-197.
[2] Specifically considering a nuclear device, Kenney, for instance, cites Anne Stenersen of the Norwegian Defense Research Establishment with respect to a manual called *The Nuclear Bomb of Jihad and the Way to Enrich Uranium.* She described this document "as a randomly organised collection of texts, illustrations and articles assembled from a hodgepodge of sources without much regard as to whether the information is correct or not."
[3] Michael Kenney, "Beyond the Internet," 192.
[4] Steven Windisch, Michael Logan, and Gina Scott Ligon, "Headhunting Among Extremist Organisations: An Empirical Assessment of Talent Spotting," *Perspectives on Terrorism,* 12, no. 2 (2018): 19; Mia Bloom, "Constructing Expertise: Terrorist Recruitment and 'Talent Spotting' in the PIRA, Al Qaeda, and ISIS," *Studies in*

Qaeda's close alliance with the Taliban, or Aum's appeal to alienated members in Japanese society, provided these groups with access to a large pool of potential operatives. Hence, we could expect a terrorist organisation with a high level of popular support and (perceived) legitimacy to be more capable to recruit people with the necessary skills. Yet, as will be outlined below, this is not as straightforward as often assumed. Both security and strategic considerations can impact a terrorist organisation's willingness and ability to recruit these individuals. Furthermore, notwithstanding this observation that other variables will also play a role in the recruitment of experts, it should also be noted that each of the four case studies simultaneously illustrated that the organisational design should support and facilitate such recruitment efforts. For instance, Aum Shinrikyo enjoyed a relatively high level of popular support (for a terrorist organisation). Yet, its inner circle valued loyalty of specialised skills. Its organisational design was not receptive towards outside help or bottom-up input. This subsequently limited the effective implementation of its CB armaments plots.

(2) Each of the four case studies pointed out that the experts involved need an adequate level of operational autonomy and decision-making power.[5] This strengthens the functional capacity of these persons and increases the likelihood that they can effectively cope with unexpected situations that cannot be analysed in advance. This does not imply that the political and ideological leadership should be absent. *Motivated* leadership can focus and support the group's implementation efforts. Each of the case studies suggested in this context that centralised control could facilitate the initiation and resource prioritisation to a nuclear terrorism plot. For instance, it is probably no coincidence that Al Qaeda's chemical and biological efforts became more crude after its decentralisation that followed after 9/11.[6] Yet, each of the case studies simultaneously demonstrated that the leadership should limit its hierarchical top-down interference in the actual implementation of a nonroutine plot. This is demonstrated by the example of Lord Cherwell who incorrectly pushed for the use of commercial dynamite, Bin Laden's impatience and his wish to expedite the 9/11 plot, or the substantial negative consequences of the top-down meddling by Shoko Asahara. The experts involved in a nuclear terrorism plot are best positioned to complete the diversity of tasks related to this plot (e.g. the acquisition of fissile material, military attacks, the illicit trafficking of nuclear and non-nuclear components, financial payments, or the actual construction of a nuclear device). Hierarchically imposing pet solutions, ad how

Conflict & Terrorism 40, no. 7 (2017): 603–23; Brian Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict & Terrorism* 24, no. 3 (2001): 183–213."

[5] My research does not allow me to further quantify the term 'adequate.' This will ultimately be a function of the exact nuclear terrorism scenario and its nonroutine nature of technology.

[6] Paul Gill et al., "Malevolent Creativity in Terrorist Organisations," *The Journal of Creative Behavior* 47, no. 2 (June 2013): 138.

whims or overly ambitious demands can be expected to increase the likelihood of operational delays, errors or human frustrations. This way, it can endanger the effective implementation of the plot. For instance, unduly demands or suggestions by terrorist leaders could lead to the disregard of essential engineering considerations in a nuclear terrorism project. Likewise, it could lead to the neglect of diverse security considerations (e.g. entering a nuclear black market to *acquire fissile material* without sufficient regard for security). These observations – and its potential consequences (infra) – are however often neglected in today's nuclear terrorism threat assessments.

(3) Each of the four cases studies supports the idea that a sufficient number of intra-cell and inter-cell connections will also strengthen the functional capacity of the experts. The four case studies differed in size, timing and exact nonroutine nature of technology. Yet, each of these case studies demonstrated that an adequate number of coordination and communication tools is necessary to creatively work together.[7] The implementation of Los Alamos, the PNE program and 9/11 was characterised by sufficient formal and informal moments of deliberation and coordination. This strengthened the experts' capability to effectively cope with unexpected situations that cannot be analysed in advance. In contrast, Aum Shinrikyo was characterised by a limited diffusion of information and knowledge. Not surprisingly, this hindered Aum Shinrikyo in optimally leveraging its human resources; it hampered the inner circle's problem-solving capacity. Building on the organisational analogy between these four cases and the adopted nuclear terrorism scenario, it thus follows that it is plausible to assume that the effective implementation of a nuclear terrorism plot would require an adequate number of intra-cell and inter-cell connections. A diversity of tasks will need to be completed and attuned to each other. The type of fissile material that might be acquired will e.g. have a strong impact on the illicit smuggling of the material and the actual construction of the device. Moreover, any unexpected situation throughout the implementation of such a plot might require the need for creativity and flexibility. Besides the need to exchange technical know-how and information, communication and coordination will be of particular relevance in conveying experiential knowledge (metis) with respect to such unexpected situations.

Concluding this section on the match between the organisational design and the nonroutine nature of technology, the general replication of these findings strengthens the plausibility of the first hypothesis. Yet, aggregating the differences between the four case studies allows us to further refine this argument. The impact of these qualifying conditions will be emphasized in the following sections. Yet, it should be noted already that a differing nonroutine nature of technology seems to impact the requirements with

[7] My research does not allow me to further quantify the term 'adequate' The exact number will ultimately be a function of the exact nuclear terrorism scenario and its nonroutine nature of technology.

respect to the group's organic design features. For instance, the nonroutine nature of technology at 9/11 was less outspoken than that at Los Alamos. Correspondingly, the organic nature of the organisational design of the group that implemented 9/11 was less outspoken than that of the group that implemented Los Alamos. There were less experts, they enjoyed a lower level of operational autonomy, and there were less interconnections. The required organic design features seem to be a function of the exact nonroutine nature of the project. Considering that this will ultimately depend on the exact nuclear terrorism scenario, it is therefore likely that the exact organic design requirements will be a function of the exact nuclear terrorism scenario. Hence, it is plausible to assume that the development of a nuclear explosion of 100 ton will require a less intense organically designed group compared to the organic design of a group that would aim to develop the terrorist equivalent of Hiroshima.

9.1.2. Versus an efficient security approach

Considering the match between an organisational design similar to an organic organisational design and a terrorist organisation's clandestine operational environment, this study hypothesised that "an organisational design similar to an organic design implies increased security risks to a terrorist organisation and its nuclear terrorism project." (=H2) A more organic organisational design would simultaneously be an *inefficient* way for a terrorist organisation to guarantee its security. The following sections will elaborate on the plausibility of this hypothesis by zooming in on the three identified organisational design features. While doing so, I will highlight findings that have recurred throughout the different case studies, take into account qualifying conditions, and explore how these extrapolations relate to the three traditional nuclear terrorism variables and the nuclear terrorism threat.

(1) Each of the four case studies made clear that the recruitment and allocation of experts with the necessary *specialised* skills is not as straightforward as often (implicitly) assumed in today's nuclear terrorism threat assessments. Both Los Alamos and the PNE program enjoyed a relatively high level of popular support and legitimacy. Nevertheless, both programs experienced some (minor) recruitment challenges. Not everyone was motivated to participate in these state programs or compelled by its goals. The secret nature of these projects furthermore continuously entailed the "problem of how much one could say." It is probably no coincidence that the nucleus of Los Alamos came from several groups working with Oppenheimer, or that the responsibility over the PNE program was given to the already existing AEB's RD Division. Approaching people from a known and trusted network might alleviate some of these security considerations. Moreover, importantly, these recruitment challenges were even more

intense throughout the implementation of both nonroutine terrorism plots. Both Aum Shinrikyo and Al Qaeda enjoyed a relatively high level of popular support and a beneficial security environment (compared to other terrorist organisations). Nevertheless, both organisations displayed a particular sensitivity to the loyalty of the members of the project team. Considering Aum, members of the inner circle were bound to demonstrate their loyalty to the organisation via e.g intensive rituals or rigorous physical postures.[8] Likewise, Al Qaeda originally envisaged the 9/11 plot to be implemented by trusted Mujahideen. Although Al Qaeda showed some flexibility in valuing loyalty over skill by selecting the members of the Hamburg cell, it is telling that it never went as far as e.g. actively recruiting outside pilots. Each member of the 9/11 plot was selected via its network of training camps.

Aggregating these findings, it seems that the recruitment of people that are both loyal to a terrorist organisation and capable to implement a nuclear terrorism plot is relatively complex. On the one hand, a nuclear terrorism plot requires people with e.g. illicit trafficking skills, nuclear expertise or military skills. The clandestine recruitment of these people needs to cope with the fact that individual claims are often difficult to verify. Few people are in a position to actually question the quality of these persons.[9] Yet, any operational error could lead to the plot's interruption or detection. On the other hand, a terrorist organisation also needs to avoid the equivalent of Klaus Fuchs or Dieter Gerhardt. A terrorist organisation needs to be cautious about opportunistic con men, infiltration by counterterrorism efforts, or uncompelled experts that might not be motivated to carry out its tasks. These considerations are conducive to the emergence of a more secure - yet simultaneously less effective - organisational design. It might lead to a limited reliance on outsider help or bottom-up input by less-trusted members of the group. Different qualifying conditions (e.g. level of popular support, the exact nonroutine nature of technology) might sharpen or alleviate this security dilemma. Yet, in general, it is plausible to assume that the recruitment of experts is not as straightforward as often (implicitly) assumed in today's nuclear terrorism threat assessments. For instance, the literature on this theme often understudies the complexity to recruiting disgruntled scientists.

(2) The extrapolations that follow out of each of the four case studies are not clear-cut with respect to the level of hierarchical control over the operational experts. Studying Los Alamos and the PNE program led to contradictory extrapolations. A higher level of operational autonomy at Los Alamos led to an increase in divergent behavior by the people involved in this project. In contrast, I did not identify an

[8] Flannery, *Understanding Apocalyptic Terrorism,* 228-229. Note in this context that authors such as Eli Berman (Eli Berman, *Radical, Religious and Violent: The New Economics of Terrorism* (Cambridge: MIT Press, 2009) already identified such commitments tests as an important way to control defection.
[9] Jacques Hymans, *Achieving nuclear ambitions: scientists, politicians, and proliferation* (United States: Cambridge University Press, 2012, 209-216.

increase in divergent behavior by the autonomous operatives in the PNE program. I have subsequently suggested to remain cautious about expecting an increase in diverging behaviour by autonomous experts in a nuclear terrorism plot.[10] Next, however, the implementation of 9/11 did provide support to the expectation that a loss of operational control over the operatives would imply an increased risk of divergent behavior. This terrorist plot enjoyed the benefits related to its less outspoken nonroutine nature of technology, a relatively lenient counterterrorism environment, and a relatively small project team. Yet, the friction between Atta and Jarrah, or the arrest of Moussaoui, illustrate the security risks to too little operational control over the experts. A terrorist organisation continuously needs to take into account these risks. Finally, making matters even more complex, Shoko Asahara demonstrated that too much hierarchical control might also imply particular security risks. His orders were in general loyally executed. This limited the operational ambiguity and fluidity. Yet, Asahara's authority boiled over to a personality cult. This increased the likelihood of operational errors via e.g. the sabotage of other people. Such operational errors might, on its turn, lead to the disruption or detection of the plot.

Aggregating these findings, I like to bring forward two intertwined issues with respect to the level of hierarchical control over the operational experts. First, it became clear that allowing for an adequate level of operational autonomy while trying to limit divergent behavior would be a complex balancing act for a terrorist organisation that pursues a nuclear terrorism plot. Both too little and too strict control by the leadership might imply divergent behavior by the operational experts. This, on its turn, might imply particular security risks to the terrorist organisation. Any instance of an operational error or defection of a member of the group might lead to the detection of the plot. Second, importantly, each of the four case studies underscored the relevance of different qualifying conditions with respect to this balancing act. Reflecting upon the case studies with an organic organisational design, it seems that the likelihood of divergent behavior would increase in case of a more intense nonroutine nature of technology, a large-sized and long-lasting nuclear terrorism plot, or a project in a more hostile operational environment. Likewise, the cohesion of the project team and the motivation of each individual member seems of particular relevance with respect to the likelihood of divergent behavior. This, on its turn, depends on a variety of factors. Each of the four case studies highlighted the relevance of a clear and compelling common goal. Yet, the motivation of operatives might also be a function of their embedding in a dense network of reciprocal relationships.[11] For instance, it was probably no coincidence that Jarrah – the 9/11

[10] I have argued that the factors that might explain this discrepancy might also be applicable to the adopted nuclear terrorism scenario. These factors were: the resource support and compelling nature of the PNE program's goals, the lower nonroutine nature of technology, and the PNE program's relatively small size.

[11] This argument has also been brought forward by, e.g., Eli Berman and David D. Laitin, "Religion, Terrorism, and Public Goods: Testing the Club Model," *Journal of Public Economics* 92, no. 10-11 (2008): 1942-1967.

operative that was least motivated - was not equally socially included in the Hamburg cell. Such factors might sharpen or alleviate the security challenges to the aforementioned balancing act.

(3) Each of the four case studies made clear that a higher level of intra- and inter-cell connections implies an heightened risk of detection by counterterrorism forces. This organic design feature clearly illustrates the effectiveness-efficiency trade-off at work. Information-exchange is necessary to effectively implement a nonroutine project. Yet, each communication or coordination tool simultaneously implies an opportunity for counterterrorism forces to detect (parts of) the ongoing operation. For instance, the increased level of communication and coordination at Los Alamos and the PNE program led to substantial suspicions about the existence of these projects. The perceived legitimacy of these state actors contributed to the fact that these projects were not interrupted. Yet, this does not alter the fact that there were various security breaches throughout their implementation. Likewise, considering the implementation of 9/11, it is illustrative that the intelligence system was blinking red in the weeks before this attack. Reports about Al Qaeda's activities and planning grew larger. Aum Shinrikyo, in contrast, was characterised by a limited level of information-exchange. This limited the effective implementation of its CB armament activities. Yet, it was beneficial to the secure implementation of its plots.

Moreover, a higher number of interconnections implies that the likely gravity of a potential security breach would increase. Compartmentalisation enables anonymity and a lack of information about other parts of the plot. In contrast, a security breach is likely to have more severe consequences in case that different persons and parts of the plot are integrated and connected to each other. This way, one piece of information might lead to the unravelling of the whole plot. The examples of Klaus Fuchs or the employee who told the CIA about the PNE program demonstrate the consequences of such a security breach. The equivalent of such a breach could imply the end of a potential nuclear terrorism plot. This underscores the issue of loyalty again. Other variables will also be relevant (e.g. the group's popular support and control over territory). Yet, a terrorist organisation will continuously need to be aware of the risks related to the communication and coordination in a nuclear terrorism plot. It makes the organisation vulnerable to any instance of defection of one the group members or detection by counterterrorism forces. This might induce the organisation to limit its information-exchange, thereby negatively impacting the likelihood that it could effectively implement a nuclear terrorism plot.

Concluding this section on the match between an organic organisational design and a terrorist group's clandestine operational environment, the aggregated findings generally support the hypothesis that "an organisational design similar to an organic design implies increased security risks to a terrorist organisation and its nuclear terrorism project." (=H2) This becomes most apparent when we consider

the need to recruit and employ individuals with the necessary skills and the need to establish an adequate number of interconnections. Both organisational design features clearly underscore the logic behind the suggested effectiveness-efficiency tradeoff. Moreover, reducing the hierarchical control over the plot's operatives might imply particular security risks as well. Allowing for an adequate level of operational autonomy while trying to limit divergent behavior would be a complex balancing act. Yet, the likelihood that these security risks would materialize seems to increase in case of e.g. a more intense nonroutine nature of technology, a large-sized and long-lasting nuclear terrorism plot, or a project in a more hostile operational environment.

Moreover, in general, it should be noted that these case studies emphasized that the security constraints that follow from such a plot's covert nature deserve more attention in traditional nuclear terrorism threat assessments. Both Los Alamos and the PNE program enjoyed a relatively high level of domestic support and international legitimacy. This was beneficial to the mobilisation of resources and the alleviation of some of the aforementioned security concerns. It allowed for a more organic organisational design to emerge. In contrast, although both Al Qaeda and Aum Shinrikyo enjoyed some level of popular support and a relatively lenient counterterrorism environment, both terrorist organisations needed to be more thoughtful about its operational and organisational security. One instance of a security breach might be enough to undermine its operational security. Such risks do not necessarily materialize. Yet, its mere threat might already instil caution in a terrorist organisation's considerations. This issue is closely related to motivation of a terrorist organisation to go nuclear. It brings us to our final hypothesis.

9.1.3. Versus an efficient strategy

Taking into account the first and second hypothesis of this research project, this study subsequently hypothesised that "an organisational design more similar to an organic design implies an increasingly inefficiently functioning terrorist organisation with respect to the attainment of their political and organisational goals." (=H3) Adopting an instrumental-rationality approach, the aggregated findings of the case studies generally support the plausibility of this hypothesis. I will elaborate on this argument in more depth and emphasize three insights that are closely related to the motivation of a terrorist organisation to go nuclear. In doing so, I will primarily build on the two case studies of a nonroutine terrorism plot.

I have outlined in chapter three that, notwithstanding the group's organisational design, one could question the strategic value of a nuclear terrorism plot. After having studied the different case studies, it remains plausible to assume that an organic organisational design would tilt the cost-benefit balance even more in favour of a negative decision. On the one hand, a nuclear terrorism plot would imply the investment of various material resources and some of the best operatives of the organisation. Although each of the four case studies differed in scale, they could all enjoy a relatively large pool of operatives and material resources. This is not self-evident for a terrorist organisation. Aum demonstrated that a terrorist organisation cannot always direct all its material and human resources to such a plot. This dilemma would become even more pressing in case that a terrorist organisation only enjoys a limited number of human and material resources. On the other hand, this type of organic organisational design would simultaneously imply increased security risks. This could lead to substantial tactical and strategic costs for the terrorist organisation. It might imply e.g. the loss of various material and human resources or a crackdown by counterterrorism efforts. The decimation of Aum Shinrikyo after its 1995 Sarin attack is illustrative of the potential negative consequences. Thus, adopting an instrumental-rationality approach, it remains plausible to assume that the likelihood that any strategic gains will be achieved would be reduced even more via an organic organisational design.

Moreover, going beyond the support for this particular hypothesis, these case studies brought forward three intertwined arguments that are closely related to this hypothesis and the motivation of a terrorist organisation. These exploratory lines of thought need further examination and validation. Yet, it is remarkable that they remain underdeveloped in today's nuclear terrorism threat assessments.

(1) These findings suggests that a lower-yield nuclear explosion (e.g. a fizzle) is more likely than the terrorist equivalent of Hiroshima. The development of a higher-yield nuclear explosion is likely to be characterised by a more nonroutine nature of technology. The effective implementation of such a plot is therefore likely to require a more organic organisational design. It would imply both a higher investment of resources and a higher risk of failure. It follows that either instrumental security considerations or accidental operational failures might reduce the effective implementation of a nuclear terrorism plot. This has been illustrated by the Sarin strain that was used in Aum's 1995 attack that was only a third as strong as Aum intended. Next, other instrumental-rational considerations might induce a terrorist organisation to actually prefer a lower-yield nuclear explosion. On the one hand, this type of nuclear terrorism plot would imply a reduced investment of resources and a lower risk of detection. On the other hand, a lower-yield nuclear explosion might simultaneously be perceived as likely to receive less blowback (by both the organisation's constituency and its adversaries). The doubts by the Al Qaeda's leadership about KSM's original grandiose plan or the desirability of the 9/11 attack are

illustrative in this context. A more limited option could be perceived as politically and organisationally beneficial to the terrorist organisation.

(2) The Aum Shinrikyo case study suggested that the most-likely candidates to pursue a nuclear capacity would probably not wield an instrumental rationality. In contrast, they would be guided by a charismatic authority and/or value-rationality. Aum adopted an unique and apocalyptic ideology and obsession with futuristic technology. This type of rationality was a driving force behind the initiation of its CB plot. Members of the inner circle implemented their particular tasks in order to please the charismatic guru. Yet, this case study made clear that this type of rationality simultaneously complicated the effective implementation of the plot. Aum's organisational design implied increased subjective control over its experts rather than increased objective control over the outcome of the plot. Next, considering the implementation of 9/11, it is clear that Al Qaeda is characterised by a virulent and dichotomous ideology and worldview. This might be considered to be value-rational to some extent. It might have pushed them to the 9/11 plot. Yet, it simultaneously became clear that the Al Qaeda's senior leadership did assess the instrumental value of the 9/11 plot. Such instrumental rational considerations might impact a nuclear terrorism plot's probability. Security considerations or resource allocation issues might, e.g., impede the effective implementation of such a plot. In contrast, a more intensely value-driven organisation might give less relative weight to these issues.

Reflecting upon this line of thought, it is plausible to expect an inverse relationship between a terrorist organisation's motivation to go nuclear and its capability to actually implement such a plot. Jenkins noted in similar lines that "psychotics are potential nuclear terrorists, but in terms of capabilities they are the least able to acquire nuclear weapons."[12] On the one hand, a value-driven terrorist organisation is expected to be most-likely to initiate such a plot. This type of organisation is most-likely to be motivated to carry out a nuclear terrorism plot. Yet, on the other hand, such an organisation might simultaneously be least likely to guarantee the need for scientific autonomy and an adequate level of information-exchange. Moreover, this type of organisation would require more commitment by its members. It can thus be assumed to enjoy less popular support and legitimacy. This would entail that it would not enjoy the security benefits related to such levels of popular support and legitimacy. Both factors would limit the terrorist organisation's capability to effectively implement a nuclear terrorism plot. This idea of an inverse relationship underscores the plausibility of the aforementioned suggestion that a lower-yield nuclear explosion is more likely than the terrorist equivalent of Hiroshima.

[12] Brian Jenkins cited in Jerrold Post, "Prospects For Nuclear Terrorism: Psychological Motivations and Constraints," *Conflict quarterly* (1987): 48.

(3) It should be repeated that it is necessary to reflect upon the relevance of the exact nuclear terrorism scenario. There is a myriad of pathways for a terrorist organisation to achieve a (crude) nuclear capacity. The exact pathway depends e.g. on the terrorist organisation's resources, the (state) assistance that it can acquire, and its exact operational environment and its opportunities. The exact nuclear terrorism scenario will impact its nonroutine nature of technology and the corresponding organisational challenges. For instance, some of the sketched organisational challenges could be alleviated in case that a terrorist organisation would have the opportunity to acquire a high quantity of weapons-grade HEU (e.g. via state assistance). A terrorist organisation might then decide to act upon such opportunities. Indeed, the exact nuclear terrorism scenario that is available to a terrorist organisation might impact its strategy and motivation with respect to that scenario.

To conclude, the aggregated findings of the case studies generally support the plausibility of the third hypothesis that the likelihood that any strategic gains would be achieved via a nuclear terrorism plot would be reduced even more via an organic organisational design. Moreover, these findings suggest that it is plausible to expect an inverse relationship between a terrorist organisation's motivation to go nuclear and its capability to actually implement such a plot. Yet, in order to come to a more comprehensive understanding of the nuclear terrorism threat, it remains necessary to reflect in more depth upon other nuclear terrorism scenarios as well.

9.2. Other nuclear terrorism scenario's

This research project adopted a particular nuclear terrorism scenario. This provided a formal way to structure thinking about the nuclear terrorism threat. It provided focus to this study. Yet, as became clear throughout the previous sections, the exact organisational challenges will also be function of the exact nuclear terrorism scenario. This section will therefore reflect upon other nuclear terrorism scenarios, how my findings might (or might not) apply to such scenarios, and what this would imply with respect to the nuclear terrorism threat. I will first briefly elaborate on the fact that the implementation of such a plot can be a dynamic process. Next, I will elaborate on scenarios that are not characterised by a nonroutine nature of technology. Both sections aim to contribute to a more comprehensive understanding of the nuclear terrorism threat.

9.2.1. A dynamic implementation process

This study hitherto implicitly assumed that a terrorist organisation would try to develop a crude nuclear device as quickly as possible. Moreover, it implicitly treated the implementation of a potential nuclear terrorism plot as a relatively linear process. Yet, these implicit expectations will not always hold true. It should be acknowledged that there are different strategies for a terrorist organisation to obtain a (crude) nuclear capacity and that a terrorist organisation might decide to shift its strategy along the way. A more comprehensive nuclear terrorism threat assessment needs to take into account the dynamic nature of this process.

The suggested effectiveness-efficiency trade-off entails a good starting point to structure our thinking on this issue. To be precise, considering the suggested trade-off, it is possible to distinguish between a "sprinting" and a "hiding" strategy.[13] A "sprinting" strategy refers to a model where a terrorist organisation would invest and allocate multiple resources to a nuclear terrorism project and adopt various of the aforementioned organic design features. This way, it would increase the likelihood that it can effectively implement such a plot as quickly as possible. Yet, as became clear throughout the previous sections, this strategy would simultaneously imply increased security risks. The pressing nature of the effectiveness-efficiency trade-off would become more intense. A terrorist organisation would thus need to be so motivated that it can reconcile itself with a high investment of resources and a high risk of failure. In contrast, a terrorist organisation might also decide to prioritise secrecy over speed via a "hiding" strategy. For instance, a terrorist organisation might decide to only act upon particular opportunities that would arise. Hiding the program becomes most important to the terrorist organisation. It could do so by, e.g., limiting the information exchange, reducing operational autonomy by the experts involved, or limiting the recruitment of outside help. The organic design features would thus be abandoned. Such a model could strengthen the organisational security of the plot. Yet, it would simultaneously reduce the likelihood that the organisation could effective implement the nuclear terrorism project. Moreover, the slow implementation of the process would entail particular security risks as well. For instance, counterterrorism efforts would have more time to detect or disrupt the plot's implementation.

[13] In order to reflect upon this issue, I was inspired by Vipin Narang work's on how states pursue the bomb. Vipin Narang, "Strategies of Nuclear Proliferation: How States Pursue the Bomb"*International Security* 41, no. 3 (2017): 110-150. He identified hedging, sprinting, hiding, and sheltered pursuit. Yet, the sprinting and hiding strategy seemed to be analytically most useful to a potential nuclear terrorism plot.

The previous chapters made clear that a variety of variables might impact a terrorist organisation's considerations in this respect. I will limit myself here to highlighting two sets of variables that should be taken into account. First, the operational security environment in which a terrorist organisation is operating will be important to consider. This includes, e.g., a terrorist organisation's control over geographic regions, its availability of safe houses, its level of popular support, and the state scrutiny in countering the group. A more conducive security environment might push a terrorist organisation towards a "sprinting" strategy. It could alleviate various of the security concerns related to an intense effectiveness-efficiency trade-off. This would thus increase the likelihood that a terrorist organisation could implement a nuclear terrorism plot. Second, internal dynamics in a terrorist organisation will also play a role in determining the terrorist organisation's strategy. A terrorist organisation is not a unified bloc. The goals, type of rationality and coherence of a terrorist organisation will be a particular relevance in this context. For instance, internal reluctance to invest so many resources might push a terrorist organisation to opt for the low-cost "hiding" strategy. This might slow down the effective implementation of a potential nuclear terrorism plot. These type of factors thus need to be taken into account in future nuclear terrorism threat assessments.

Moreover, it should be acknowledged that the implementation of a nuclear terrorism plot is not necessarily a linear process. To be precise, any nuclear terrorism plot might be detected and/or interrupted by law enforcement efforts at one point during its implementation. The detection of (a part of the) plot might lead a terrorist organisation to shift its focus towards a "sprinting" strategy. This could lead to the hastened implementation of the plot. This is exactly what happened in the 1995 Aum Sarin attack. Aum had to dismantle one of its Sarin production facility after Sarin precursor chemicals were detected by law enforcement authorities. Moreover, the organisation was pushed to act quickly due to a pending police raid. This accelerated implementation of the 1995 Sarin plot led to the Sarin strain that was used to be a third as strong as Aum intended.[14] On the one hand, such a shift in model could thus increase the likelihood that a terrorist organisation might actually implement the attack. It would induce the organisation to move forward. On the other hand, however, this would simultaneously increase the likelihood that the attack would be tactically less successful or that the plot would be completely stopped (e.g., via operational errors or counter terrorism efforts). Note that this is in line with the suggestion that a lower-yield nuclear explosion (e.g. a fizzle) is more likely than the terrorist equivalent of Hiroshima.

[14] Gavin Cameron, "Multi-Track Microproliferation: Lessons from Aum Shinrikyo and Al Qaida," *Studies in Conflict & Terrorism* 22, no. 4 (1999); Parachini and Furukawa, "Japan and Aum Shinrikyo," 543; Anthony Tu, "What Were the Real Objectives of Aum Shinrikyo?" *CBRNE terrorism newsletter* 41, (2012): 6.

Thus, a more comprehensive nuclear terrorism threat assessment will need to take into account these type of considerations. The suggested effectiveness-efficiency trade-off is a good way to structure our thinking on the dynamic nature of a nonroutine nuclear terrorism scenario. It enables us to better understand the threat. Yet, next, it remains necessary to reflect upon the possibility that the nuclear terrorism scenario would not be characterised by a nonroutine nature of technology.

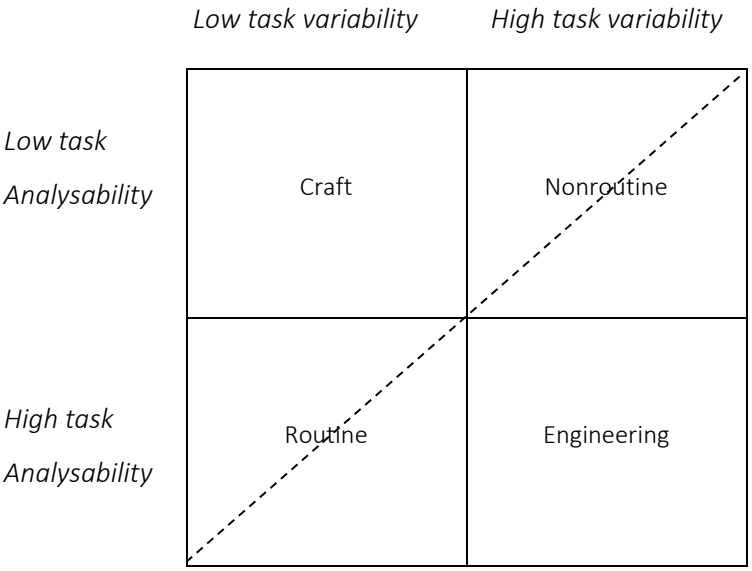
9.2.2. A different nature of technology

This research project adopted a nuclear terrorism scenario that was characterised by a nonroutine nature of technology. The extrapolations that followed from each of the nonroutine case studies were based on this organisational commonality. Yet, we should remain aware of the fact that it is not necessarily true that a nuclear terrorism scenario would be characterised by a nonroutine nature of technology. This might have a substantial impact on the probability of nuclear terrorism. The question then becomes how my findings would apply to these type of nuclear terrorism scenarios?

In order to reflect upon this issue, I will go back to Charles Perrow's model with respect to the "technology" variable. Although his two-dimensional typology led to a matrix with four quadrants, I will adopt a one-dimensional approach to this typology. As Perrow himself suggested, this matrix can be reduced to a continuum from routine to nonroutine (as indicated by the dotted line in figure 9.1 below). Burton and Obel likewise suggested that "routineness is a central concept in technology."[15] I adopt this more simplistic scheme in order to enable analysis rather than obfuscate it.[16]

[15] Richard Burton and Borge Obel, *Strategic Organizational Diagnosis and Design: The Dynamics of Fit* (New York: Springer Science, 2004), 253.
[16] Charles Perrow, *Organisational Analysis: A Sociological View* (Great Britain: Tavistock Publications, 1970), 78.

Figure 9.1. Charles Perrow's technology variable



A project with a more routine nature of technology would be characterised by the occurrence of few exceptional situations and problems that are relatively easy to resolve. Perrow noted in this context two factors that would enable the emergence of a more routine nature of technology. First, the understandability of the multiple tasks and activities. Second, the stability and variability of these tasks and activities.

> The state of the art of analysing the characteristics of the raw materials is likely to determine what kind of technology will be used… to understand the nature of the material means to be able to control it better and achieve more predictability and efficiency in transformation… The other relevant characteristic of the raw material, besides the *understandability* of its nature, is its *stability and variability*; that is, whether the material can be treated in a standardised fashion or whether continual adjustment to it is necessary. Organisations uniformly seek to standardise their raw material in order to minimize exceptional situations.[17]

These factors are closely intertwined. Both of these factors will impact the task variability and task analysability of a project. It provides us with a good way to reflect upon other nuclear terrorism scenarios. As mentioned before, the nonroutine nature of the adopted scenario follows from the diverse technical tasks that need to be completed and attuned to each other in a clandestine operational

[17] Perrow, "A Framework for the Comparative Analysis of Organisations," 196-197.

environment. Yet, as will be outlined, not every nuclear terrorism scenario will display these characteristics.

Considering the task analysability, a better understanding of the technology would imply a more straightforward analysis of the problems that might arise.[18] This might be the case for a nuclear terrorism scenario in two ways. First, a better understanding of a nuclear terrorism plot might result from access to a large number of loyal experts with the necessary techne and metis. This would strengthen the organisation's capability to control the process and achieve more predictability. It might result from e.g. systematic state assistance or the extensive training of trusted operatives.[19] Likewise, good relations with a trusted criminal organisation might enable access to people with the necessary skills. This type of nuclear terrorism scenario would still require a high level of operational discretion and information-sharing by these experts. Yet, leadership would need to worry less about different forms of divergent behavior. Second, a better understanding might also result from a reduction in the technical challenges to the nuclear terrorism plot. This would lower the demands with respect to the required expertise and skills.[20] Such a scenario could emerge, e.g., by the availability of a blueprint of the design of a nuclear device or the acquisition of a quantity and type of fissile material that can be easily used in a crude nuclear device. Both options might result from systematic state assistance or an extraordinary opportunity via e.g. access to a nuclear black market. It might imply that a smaller group would be necessary, that different tasks and activities are less intertwined, and that there is less need for operational autonomy and information-exchange. More mechanistic elements of control can thus be used to steer and guide the operatives.

Considering the task variability, an increased level of stability and variability would minimize the occurrence of unexpected problems. This might be the case for a nuclear terrorism scenario in two ways. First, the level of stability and variability is closely related to the aforementioned factors. Besides improving the task analysability, both access to the necessary experts and a reduction in the technical requirements would also reduce the likelihood that any unexpected hick-ups would occur. It follows that the control and coordination over the implementation of the plot could become more centralised and formalised. Second, a less hostile operational environment would increase the stability and variability of a nuclear terrorism project as well. Such operational environment results from e.g. systematic state assistance, a high level of popular support, or less stringent counterterrorism efforts.

[18] Perrow, "A Framework for the Comparative Analysis of Organisations," 197.
[19] Note in this context that this type of scenario this could be linked to the strategy of 'sheltered pursuit.' See Vipin Narang, "Strategies of Nuclear Proliferation."
[20] Note that the nature of technology is a matter of degree, not of kind.

This would reduce the likelihood that any exceptional situations would occur as a consequence of counterterrorism efforts. It would therefore allow the operatives involved in a nuclear terrorism plot to make mistakes and develop a positive learning curve.

Both of these factors are closely intertwined. They might reinforce each other. Access to skilled and trusted experts would, for instance, become easier in a less hostile operational environment. This would imply that the technical challenges to a nuclear terrorism plot would become more predictable and analysable. A terrorist organisation would need less flexibility, creativity and adaptability in such a scenario. These factors would therefore alleviate the need for a terrorist organisation to adopt various organic design features. This way, various of the aforementioned security concerns to such an organic design would be reduced. I will illustrate this by briefly elaborating on one potentially more routine nuclear terrorism scenario.

To be precise, it might be the case that a terrorist organisation could gain access to a nuclear facility that harbours a high quantity of weapons-grade HEU in an appropriate form. In order to implement this scenario, a relatively small group would need to have the skills to identify the target and have the capability to penetrate the facility. These latter tasks could be facilitated by a beneficial security environment (e.g. a weak security regime at that particular nuclear facility) or systematic state assistance by a rogue regime. This would imply a lower task variability and a higher task analysability. A small group might be motivated to act upon such opportunity. It would require a limited number of extraordinarily skills and there would be a limited need for communication and coordination. This would thus not go beyond the standard operations for a terrorist organisation. Next, in case this group would succeed in acquiring this type of fissile material, this same group could decide to simply drop one half of the material onto the other half. It could be motivated to carry out such a suicide mission by means of ideological or apocalyptic reasons. There would be a substantial likelihood that this would result in a nuclear explosion of a considerable size. In general, this type of nuclear terrorism scenario could be implemented in a relatively short period of time. It would still require a small group with some particular skills (e.g. illicit networking skills and military skills) and it would still imply some particular security risks (e.g. the detection of communication within the group by an adversary). Yet, it becomes clear that the intensity of the suggested effectiveness-efficiency trade-off would be substantially reduced. This would consequently increase the nuclear terrorism threat.

Thus, to conclude, the approach and findings of this study provide us with a useful tool to reflect upon other nuclear terrorism scenario's. It enables us to more comprehensively understand the nuclear terrorism threat. To be precise, reflecting upon these other nuclear terrorism scenarios, it becomes

clear that the idea of an effectiveness-efficiency trade-off should not be used to minimise the nuclear terrorism threat. If anything, it is exactly the mechanism behind the effectiveness-efficiency trade-off that warns us against lowering our security. This would substantially increase the likelihood that a potential nuclear terrorism scenario would not go beyond a terrorist organisation's standard operations. It would thus increase the likelihood that a terrorist organisation could implement such a plot.

10. Conclusion

This study worked towards a better understanding of the nuclear terrorism threat. The assessment of the probability of nuclear terrorism is a daunting task. It is necessary to understand a diverse variety of variables and their interplay. Any risk assessment should therefore aim to be the result of an encompassing analysis. I argued in this context that today's nuclear terrorism threat assessments do not systematically reflect upon the role and relevance of the organisational design of a terrorist organisation. I substantiated this claim by outlining a potential nuclear terrorism scenario, assessing today's literature on this phenomenon, and cross-referencing this field of literature with the literature on innovation and technology acquisition by a terrorist organisation. This study was the first study to systematically reflect upon this dimension. The research question was: "what is the role of a terrorist group's organisational design in implementing the construction and detonation of an improvised nuclear device?"

This research question is explorative in nature. Critics often pejoratively describe explorative research as a mere "fishing expedition."[1] Yet, exploratory research differs from confirmatory research. Exploratory research constitutes the basis for confirmatory research at a later stage. It does not adopt the same standards with respect to the issues of *validity* and *reliability.* It is more about theoretical abstractions and the generation of ideas. Yet, this does not imply that the exploration of this critical gap in the literature is not valuable, not does it imply that it should not come about in a systematic manner.

First, this study adopted a particular nuclear terrorism scenario in order to structure thinking about this phenomenon. This nuclear terrorism scenario featured a nonroutine nature of technology. Second, I studied four case studies with a similar nonroutine nature of technology: the construction of the first atomic bombs at Los Alamos, the South African PNE program, Aum Shinrikyo's CB armament activities, and Al Qaeda's implementation of 9/11. This study built on this shared organisational feature to extrapolate relevant insights from these case studies to the formulated hypotheses on the relation between the organisational design of a terrorist organisation and the nuclear terrorism threat. Finally, the last chapter aggregated these extrapolations and qualifying conditions in a cross-case analysis. Moreover, this final chapter also reflected upon nuclear terrorism scenarios other than the adopted scenario. This way, I hope that this study enabled a better understanding of the nuclear terrorism threat. I hope that it contributes to the encompassing nature of future nuclear terrorism threat assessments.

[1] Robert Stebbins, *Exploratory Research in the Social Sciences*, Qualitative Research Methods Series 48 (London: SAGE Publications, 2001), 17.

10.1. Summary of the argument

This study demonstrated that the organisational design is a relevant factor that needed to be explored in today's nuclear terrorism threat assessments. It is no omnipotent causal force; there is not one factor that can explain such a complex threat. Yet, this first exploration of the organisational design variable did enable me to formulate various insights that strengthen our comprehensive understanding of the nuclear terrorism threat. In what follows, I will summarise this study's main argument. Next, I will specifically elaborate on three issues that deserve more attention in today's nuclear terrorism threat assessments.

In general, this study introduced the plausibility of an effectiveness-efficiency trade-off. First, I argued that a terrorist organisation with an organic-like organisational design would more likely *effectively* implement a nuclear terrorism plot with a nonroutine nature of technology. The experts involved need to cope with a high task variability and low task analysability. I expect that their functional capacity benefits from an adequate level of operational decision-making power and information-exchange. Second, I simultaneously argued that such an organic-like organisational design would likely imply an *inefficient* way for a terrorist organisation to guarantee its operational and organisational security. This trade-off manifests itself most clearly via the need to recruit individuals with the necessary skills and the need to establish an adequate number of connections. Yet, the complexity for a terrorist organisation to allow for an adequate level of operational autonomy while trying to limit divergent behavior also illustrates this trade-off. Third, adopting an instrumental-rational point of view, I argued that the achievement of any strategic gains via a nuclear terrorism plot is unlikely. I expect that an organic organisational design would tilt this cost-benefit balance even more in favour of a negative decision. Indeed, this type of design likely entails an increased investment of resources and an heightened risk of failure.

The organisational design is, however, no omnipotent causal force. To be precise, the aggregated findings of this study underscore the role of the organisation's popular support and the legitimacy of its goals. These factors might sharpen or alleviate the aforementioned security concerns. Additionally, the pressing nature of the suggested effectiveness-efficiency trade-off also depends on the exact nuclear terrorism scenario. I expect that the intensity of this trade-off increases in case of a scenario with a more intense nonroutine nature of technology, a large-sized and long-lasting nuclear terrorism scenario, or a scenario in a more hostile operational environment. It is thus clear that the suggested effectiveness-efficiency trade-off is a matter of degree rather than kind. Yet, this does not undermine its contribution to our better understanding of the nuclear terrorism threat.

To be precise, this conclusion wants to stress three particular issues that came forward throughout this study. This is no exhaustive overview of this study's explorations and insights. Yet, I believe that nuclear terrorism threat assessments often overlook these three arguments. Highlighting their relevance can therefore add to the comprehensive nature of any future nuclear terrorism threat assessment.

(1) This study emphasized that various security considerations related to the implementation of a covert terrorism attack deserve more attention in nuclear terrorism threat assessments. Today's nuclear terrorism threat assessments often focus on the probability of individual input parameters or the consequences of such an attack. They consequently tend to underestimate the pressing nature of these security constraints. Yet, a terrorist organisation interested in a nuclear capacity faces various security risks throughout the entire implementation of such a plot. This study highlighted the complexity to recruiting experts that are both loyal to the group and that have the necessary techne and metis to implement a nuclear terrorism plot, the problems related to allowing for an adequate level of operational autonomy while simultaneously limiting divergent behaviour, and the inherent security risks to an increased level of information-exchange. Such security considerations might lead, e.g., to a limited reliance on less-trusted operatives or the compartmentalisation of information. It is thus conducive to the emergence of a more secure yet less effective type of organisational design. This demonstrates how traditional nuclear terrorism variables (i.e. a group's motivation and access to nuclear know-how and technology) might interact with the organisational design of a terrorist group. Yet, nuclear terrorism threat assessments often neglect these kind of considerations. We need to better integrate a terrorist organisation's perspective in future nuclear terrorism threat assessments.

(2) This study suggested an inverse relationship between a terrorist organisation's motivation to carry out a nuclear terrorism plot and its actual capability to effectively implement such a project. On the one hand, I suggested that an organisation that aims to pursue a nuclear capacity likely features a charismatic authority and/or value-rationality. I expect that such a group dares to allocate resources to such a plot while simultaneously accepting the increased security risks. It is probably no coincidence that both Aum Shinrikyo and Al Qaeda demonstrated an interest in a nuclear terrorism plot. On the other hand, however, I suggested that this type of organisation is least likely to guarantee the need for an adequate level of scientific autonomy and a sufficient level of information-exchange. Moreover, I expect that this type of organisation enjoys less popular support and legitimacy. This would thus imply increased security risk for this organisation. Both of these factors would limit the terrorist organisation's capability to effectively implement a nuclear terrorism plot. Yet, today's nuclear terrorism threat assessments hardly ever reflect upon these type of considerations.

(3) Both of the arguments above seem to imply that we should not exaggerate the nuclear terrorism threat. Yet, it should be clear that this study should not be used to minimise the nuclear terrorism threat. The (limited) tactical success of Aum Shinrikyo and Al Qaeda remind us that this research project did not try to make any absolute claims on the probability of the nuclear terrorism threat. Furthermore, importantly, it is exactly the mechanism behind the suggested effectiveness-efficiency trade-off that warns us against lowering our shields. A decreased vigilance could provide a terrorist organisation with the opportunity to, e.g., more easily reach out to well-skilled experts, communicate between each other, or acquire the right amount and quality of fissile material. Terrorist organisations might act upon these opportunities. This would increase the probability that an organisation can effectively implement a nuclear terrorism plot. Our security regime should therefore intensify the nature of the effectiveness-efficiency trade-off. Rather than minimising the threat, it is my hope that this study contributed to a more sophisticated and comprehensive understanding of the nuclear terrorism threat. This could benefit the development of a better nuclear security regime.

10.2. Further avenues for research and recommendations

This study was exploratory in nature. Although this was one of the most extensive studies of its kind, it remains true that its emphasis was on generating theory rather than verifying it. This type of research is the preferred approach when there is little or no scientific knowledge on the process that needs to be examined. Further research remains necessary in order to reflect and validate upon these findings. I want to stress three particular avenues for further research that follow out of this study.

(1) It is important that follow-up research aims to validate this study's findings. On the one hand, this implies the need to reflect in more depth upon other nuclear terrorism scenarios. This will contribute to the comprehensive nature of future nuclear terrorism assessments. On the other hand, this also implies the need to validate the findings by means of extra case studies with an analogous nonroutine nature of technology. One can think of other state nuclear projects (e.g., the Pakistani or North Korean nuclear program). Moreover, one can also think of other terrorist attacks with a nonroutine nature of technology (e.g., the IRA's development of advanced mortar bombs). I would still recommend in-depth case studies at this moment. Yet, it might also be possible to do research via small-N methodological approaches (e.g. QCA). Such research might validate my findings and strengthen our understanding of the nuclear terrorism threat.

(2) Going beyond the specific nuclear terrorism threat, it is worthwhile to further develop a line of research that reflects upon the implementation of complex terrorism attacks. Research often focuses upon the terrorist organisation as a whole and its campaign of terror. Yet, there is limited scholarly research that specifically focuses upon the implementation of individual tactical attacks. Considering that these type of attacks are often the most sensational and impactful type of attacks, this is a critical gap in the literature. The explorative findings of this study might provide a starting point for such an autonomous line of research to develop further.

(3) Finally, another line of research could focus upon advancing a psychological approach to the nuclear terrorism threat. Although I touched upon this issue, I have opted to start from a strategic approach. Reflecting upon the findings, however, it seems worthwhile to further explore such a psychological approach. This is in line with the suggestion for research to focus on whether particular texts constitute psychological warfare rather than *the motivation* to actually construct such weapons. Likewise, this type of research could focus in more depth upon the role of a charismatic leader. I am aware that this is no easy topic to study. Yet, the mere possibility of a nuclear terrorism plot and its consequences force us to rise to this challenge.

Next, despite the fact that follow-up research remains necessary, this section will also reflect upon some policy recommendations that follow from this study. Many of my arguments were in accordance with John Mueller's work on nuclear terrorism. He suggested that an atomic terrorist might be an acceptable risk.[2] In general, I would nonetheless argue that it remains important to stay vigilant. This is line with the logic of deterrence by denial. There recently seems to be a decline in the urgency and number of threat reduction programs.[3] Yet, the logic of the effectiveness-efficiency trade-off underscores the importance of a well-developed nuclear security regime. In general, this regime should intensify the pressing nature of the effectiveness-efficiency trade-off. This can be translated into a variety of measures that could lead to a better integrated defense system. Yet, I will limit myself to highlighting three particular ways that follow out of this study.

(1) The nuclear security regime should focus more on the organisation's access to the required skills and knowledge for a nuclear terrorism plot. There are already some initiatives that focus on this issue (e.g. the International Science and Technology Center). Yet, it deserves – to my knowledge - more attention

[2] John Mueller, *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al Qaeda* (Oxford: Oxford University Press, 2010), 197-198.
[3] Henry Sokolski, "The Nuclear Terrorism Threat: How Real Is It? Two Views by Brian Michael Jenkins and John Lauder," Working Paper 1602 (Nonproliferation Policy Education Center, 2016).

in today's nuclear security regime. Various security measures might complicate the participation of well-skilled and trusted operatives in a nuclear terrorism plot. For instance, one can think about the sensibilisation of experts throughout their training, the follow-up of nuclear scientists and technicians, or a focus on targeting potential recruits or members of a terrorist organisation with particular military skills, trafficking skills or networking skills. Furthermore, more broadly, counterterrorism efforts can plant false information online or invest in sting operations. These measures might not lead to a direct success. Yet, if not, they might at least lead to doubts, delays, or operational errors in a nuclear terrorism project.

(2) The nuclear security regime should also focus more upon the various security risks to a terrorist organisation. This would imply a more intense effectiveness-efficiency trade-off. On the one hand, this could limit a terrorist organisation's opportunities with respect to a nuclear terrorism plot. It is, for instance, important to improve the security of nuclear facilities with weapons-grade fissile material. Limiting the available opportunities to a terrorist organisation is simultaneously expected to negatively impact its motivation to start the implementation of such a project. On the other hand, counterterrorism forces could also exploit the security risks related to the actual implementation of a potential nuclear terrorism plot. For instance, providing exit options or dispersing ideological counternarratives might stimulate divergent behavior by the operatives involved in the plot. Likewise, counterterrorism forces should be attentive to any issue that could refer to such a plot in intercepted communication by a terrorist organisation.

(3) The nuclear security regime should also focus more upon emphasizing the lack of political utility of a nuclear terrorism plot. This will intensify the pressing nature of the suggested effectiveness-efficiency trade-off. It might limit a terrorist organisation's motivation to embark upon such an endeavour. Admittedly, this recommendation primarily follows from the adopted instrumental-rational approach. As became clear throughout this study, this is not necessary true. A more value-rational organisation might dismiss these arguments. Yet, nevertheless, such a narrative could lead to doubts about the goals of the terrorist organisation by some people in the project team. This way, it might lead to detection delays, or operational errors in a nuclear terrorism project. By intensifying the pressing nature of the effectiveness-efficiency trade-off, counterterrorism efforts can limit the probability of nuclear terrorism.

Annex

The table and the comments below provide more information on my case selection. It is based on a scan of the relevant literature. Any mistakes are mine.

First, the key criteria to select a case was its theoretical relevance. This refers to its nonroutine nature of technology. Pragmatic considerations, moreover, also forced me to take into account the availability of reliable information. I have listed these two selection criteria in bold in order to underline its importance in the table below.

Second, I have also listed other contingencies that might be relevant to the analytical comparison between the four cases and the adopted nuclear terrorism scenario. These contingencies were ultimately of secondary importance (and not investigated when the main selection criteria were not positive). Yet, extrapolations based on the selected cases will need to elaborate on the theoretical refinements and nuances that follow from (the differences in) these contingencies. The contingencies that seem most likely to have an impact on the theoretical extrapolations are: the invested human and material resources, and the timing of the project. Considering the uncertainty and secrecy related to a nuclear terrorism scenario, it is difficult to determine a reference point for this comparison. While any assessment is ultimately arbitrarily, I have thus based myself on the available literature to develop a reference point for this comparison:

- Timing: I believe the adopted nuclear terrorism scenario would take at least 6 months. This is based on a variety of literature on this theme and on conversations with different experts (e.g. conversation with Alexander Glaser; reading work by Zimmerman & Lewis, Carson et al., Willrich & Taylor, Levi, Mueller,…).[1]
- Resources: considering the invested human resources, I believe the adopted nuclear terrorism scenario would entail the participation of at least 20 persons - but probably more - with a variety of skills (physicists, military-style skills, engineers, procurement skills, trafficking skills, suicide operatives, etc.). I expect them to be divided into various cells. This is based on a review of the literature (supra. the adopted nuclear terrorism scenario). Considering the material resources, I adopt Zimmerman and Lewis' assessment that a terrorist organisation would need at least 2 million dollar to build and deliver the weapon. This includes the buying of non-nuclear components, salaries of people, etc. It does not include the buying of fissile material. The budget including this step circled around 10 million dollar.

[1] These assessments are not always clear on what they are talking about exactly (e.g. the whole project, or merely the assembly of the device). Moreover, they range from "maybe two weeks" (Conversation Glaser) to "over the course of a year in the U.S." (Zimmerman & Lewis). This assessment remains inherently arbitrary.

Table annex 1. Case study selection

Case	Nonroutine nature	Reliable information	Invested resources	Timing	Selected
State nuclear projects*					
Los Alamos	Very high task variability due to technically challenging project in a clandestine environment (+++) Very low task analysability due to the invention of the technology from scratch(- - -)	Yes. Many primary and secondary sources available on the actual implementation(+++)	Many more human resources than nuclear terrorism scenario (+++) Many more material resources than nuclear terrorism scenario (+++)	Los Alamos lasted longer than the nuclear terrorism scenario (27 months between the establishment of Los Alamos and the Trinity test) (++)	Yes
South African PNE program	Relatively high task variability due to technically challenging project in a clandestine environment (-) Relatively low task analysability: information was already available on the gun-type design (-)	Yes. Sufficient primary and secondary sources available on the actual implementation (++)	Probably more human resources than nuclear terrorism scenario (+) Probably more material resources than nuclear terrorism scenario (+)	PNE program lasted longer than the nuclear terrorism scenario (6-8 years) (+++)	Yes
Iraq	Some indications of a relatively high task variability due to technical complexity and strict clandestine environment (e.g. caution for sting operations leading to delays) (+) Some indications of relatively low task analysability (e.g. problems with high-explosive charges, and miniaturization) (- -)	Sufficient primary and secondary sources available on Iraq's nuclear program. Yet, at first sight only limited information available on the functioning of the weaponization group (the group 4 at Tuwaitha and the Atheer site). (+/-)	Uncertain, but probably more human resources than nuclear terrorism scenario (+) Uncertain, but probably more material resources than nuclear terrorism scenario (+)	Uncertain, but the program probably lasted longer than the nuclear terrorism scenario (the IAEA concluded, e.g. that the original plan set out in 1988 was to produce a small arsenal of weapons, with the first one to be ready in 1991). Iraq's nuclear efforts started, however, earlier. (++)	No

Libya	*Not assessed due to negative answer with respect to the second criteria*	Sufficient primary and secondary sources available on Iraq's nuclear program. Yet, although Libya received a nuclear weapon design by A.Q. Khan, they reportedly did not start actual weaponization phase. (- - -)	*Not assessed due to negative answer with respect to the second criteria*	*Not assessed due to negative answer with respect to the second criteria*	No
Pakistan's development of a nuclear weapon by the 'Wah Group'	Some indications of a relatively high task variability (e.g. development of own technology due to restrictions by NSG) (+) Some indications of relatively low task analysability (e.g. implosion-type design is probably more complex; development of own technology) (- -)	Sufficient primary and secondary sources available on Pakistan's nuclear program. Yet, at first sight only limited information available on the functioning of the so-called Wah Group (whom implemented the actual design and construction of the nuclear weapons) (+/-)	Uncertain, but probably more human resources than nuclear terrorism scenario (+) Uncertain, but probably more material resources than nuclear terrorism scenario (+)	Program lasted longer than the nuclear terrorism scenario (+/- 9 years) (+++)	No
North Korea's nuclear capability	*Not assessed due to negative answer with respect to the second criteria*	No. Information on the implementation process often shrouded in uncertainty and secrecy (- - -)	*Not assessed due to negative answer with respect to the second criteria*	*Not assessed due to negative answer with respect to the second criteria*	No
Iran's nuclear capability	*Not assessed due to negative answer with respect to the second criteria*	No. Information on the supposed implementation process often shrouded in uncertainty and secrecy (- - -)	*Not assessed due to negative answer with respect to the second criteria*	*Not assessed due to negative answer with respect to the second criteria*	No

Terrorism projects**					
Aum Shinrikyo's CB armament	Relatively high task variability due to technically challenging project in a clandestine environment (-) Relatively low task analysability due to technically challenging project (+/-)	Yes. Sufficient sources available on the actual implementation (primarily secondary sources) (++)	Uncertain, but probably a bit more human resources than the adopted nuclear terrorism scenario (+) Uncertain, but probably a bit more material resources than the adopted nuclear terrorism scenario (+)	The CB armament activities as a whole lasted longer. Yet, individual attacks were more similar to the timing of the adopted nuclear terrorism scenario (+)	Yes
9/11	Sufficiently high task variability due to the skills required, the complex operational plan, and AQ's clandestine environment (- -) Sufficiently low task analysability due to the skills required, the complex operational plan, and AQ's clandestine environment (+)	Yes. Sufficient sources available on the actual implementation (primarily secondary sources) (++)	Probably less human resources than nuclear terrorism scenario (-) Probably less material resources than nuclear terrorism scenario (-)	Project lasted longer than the nuclear terrorism scenario. First plan originated from 1996 (or arguable even earlier) (+++)	Yes
Islamic State's drone program	Not considered 'nonroutine' nature of technology due to the acquisition of drones via 'off the shelve' methodology.	Yes. Some secondary sources available on the actual implementation (+)	*Not assessed due to negative answer with respect to the first criteria*	*Not assessed due to negative answer with respect to the first criteria*	No
Islamic State's chemical weapons	Generally not considered 'nonroutine' nature of technology. It is more about effectively adapting resources that came in their hands. One exception – to my knowledge – was the deployment of mustard gas (reportedly produced by the group itself in any useful quantity). Yet, see criteria 2.	No. Some sources available on the use of chemical weapons by I.S. (although reliability is often difficult to assess). Yet, no information on the actual implementation of, e.g., the production of mustard gas (- - -)	*Not assessed due to negative answer with respect to the second criteria*	*Not assessed due to negative answer with respect to the second criteria*	No

Advanced mortars by the PIRA	Relatively high task variability due to technically challenging project in a clandestine environment (-) Relatively low task analysability due to technically challenging project (+)	Yes. Sufficient sources available on the actual implementation (primarily secondary sources) (+)	Probably less human resources than nuclear terrorism scenario (-) Probably less material resources than nuclear terrorism scenario (-)	Mortars were developed between the early 70s and mid90s. In two years, however, they have evolved from developing tentative weapons to reasonably reliable and safe weapons.	No
FARC's development of submersibles	Relatively high task variability due to technically challenging project in a clandestine environment (-) Relatively low task analysability due to technically challenging project (-)	Yes. Sufficient sources available on the actual implementation (primarily secondary sources) (+)	Probably more human resources than nuclear terrorism scenario (+) Probably more material resources than nuclear terrorism scenario (+)	The trial-and-error phase lasted between 1992 and 2004 (+++)	No
Tamil Tiger's chemical activities	*Not assessed due to negative answer with respect to the second criteria*	No. Only limited information available on the actual implementation of the plot. It seems, in this context, that LLTE did not produce it themselves, but acquired, e.g., chlorine externally (- -)	*Not assessed due to negative answer with respect to the second criteria*	*Not assessed due to negative answer with respect to the second criteria*	No
Hamas' (Al-Qassam Brigades) development of rockets, tunnels, or drones	*Not assessed due to negative answer with respect to the second criteria*	No. Only limited information available on the actual implementation of these plots. These plots are considered to be implemented by the Al-Qassam Brigades. Yet, I can retrieve little reliable information on their functioning (- -)	*Not assessed due to negative answer with respect to the second criteria*	*Not assessed due to negative answer with respect to the second criteria*	No

The indications (e.g. '+' or '-') are an arbitrary judgement by me on how this particular issue relates to the adopted nuclear terrorism scenario. The reference point (namely, the adopted nuclear terrorism scenario is '0'). For instance, with respect to the 'task variability', '+' indicates that the task variability was higher while '-' indicates it was lower. It refers to my judgment on this issue based on the information that I have scanned.

*This overview provides a list of (1) the two state nuclear projects that I have selected, and (2) a few examples of other state nuclear projects and the particular reasons why I did not select them. I have limited myself to two cases of state nuclear projects because of time constraints in this research project. Yet, this does not mean that other state nuclear projects cannot be studied.

1. First, I have opted to study Los Alamos as a first case study. A scan of the literature made clear that it was a nonroutine project and that there was a lot of reliable information available on the actual implementation of the project (including various interviews with people directly involved in the project) that I could understand (namely, in English). The reliability of information is probably related to the fact that various documents have been declassified over time. While the project was charactised by a more intense nonroutine nature of technology than the adopted nuclear terrorism scenario (see table and text), it was important for me to select a case where sufficient reliable information was available. This is the first case study. It is the first exploration into this topic. It needs to be substantiated by as much reliable empirical evidence as possible.
   While I only focused on the actual development and construction of the bomb (and not the entire Manhattan project, which included the enrichment of fissile material), this project was characterised by a more intense nonroutine nature of technology (this is similar in each of the nuclear proliferation programs of the P-5). Moreover, there were substantial differences in the invested number of resources and the timing of the project. This has pushed me to opt for a small state nuclear project as a second case study. Although heterogeneity in the cases is not troublesome, as explained in the text, I have nevertheless aimed to make the analogy as strong as possible.

2. Second, I have opted to study South Africa's PNE program. A provisional scan of the literature made clear that it was a nonroutine project. Next, Pretoria's first development of a nuclear capacity (=the PNE program) was more analogous (although not exactly similar) to the adopted nuclear terrorism scenario in many ways (e.g. design, size of the program, number of invested resources). It thus allows me to see if the first theoretical explorations would also hold in a state nuclear project more similar to the adopted nuclear terrorism scenario. Moreover, it is one of the few countries that successfully constructed nuclear weapons and then gave up on them. This fact – and a provisional scan of the literature – made me believe that sufficient reliable and understandable information would be available. It is therefore a good second case study. Some other case studies might also be possible (e.g. Pakistan, Iraq,…), but a scan of the literature on these programs strengthened my believe that there is not so much information publicly available.

** Besides cases of nonroutine state nuclear program, it is also necessary to include nonroutine terrorism plots. This allows us to reflect upon the applicability of the extrapolations throughout the implementation of a nonroutine plot by an actual terrorist organisation. I have first screened relevant literature on this topic to identify potential cases (e.g. a special issue of the Journal of Strategic Security on "Designing Danger: Complex Engineering by Violent Non-State Actors," an edited collection by Jonathan Tucker on "toxic terror: Assessing Terrorist Use of Chemical and Biological Weapons," a workshop report by Hafez and Rasmussen on 'Terrorist innovation,' And a book by Adam Dolnik on terrorist innovation). Moreover, I have checked the START Big, Allied, And Dangerous Database (BAAD), the START Radiological And Nuclear Non-State Adversaries Database (RANNSAD), and the CBRN attacks in the START Global Terrorism Database (GTD). By reading through a summary of these cases, I have subjectively decided whether or not they seemed to fit my definition of a nonroutine terrorist attack, and if there was enough reliable data on the implementation of these cases (for instance, 'designing danger' indicated that there was not sufficient reliable information on Hezbollah's development of guidance systems for rockets or unmanned aerial vehicles, or that the Rajneeshees' use of Salmonella or the Tamil Tiger's development of fast panga boats was a limited "complex engineering effort"). Moreover, Jonathan Tucker's edited collection explains that various plots, e.g. R.I.S.E.s bioterrorism plot or the CSA's cyanide plot, did not evolve into actually using the biological or chemical agents, let alone causing many casualties). Based on this literature review, I have listed those cases that seemed potentially relevant. For those cases that I have listed, I then re-evaluated my first assessment (e.g. was it possible for me to retrieve sufficient reliable information). While some other case studies might also be relevant (e.g. the PIRA's development of advanced mortars, FARC's development of submersibles, etc.), I subsequently decided to select:

1. Aum Shinrikyo's chemical and biological armament activities. This case is one of the very few cases where a terrorist organisation succeeded - to some extent - to endogenously develop WMDs (i.e. the production and weaponisation of chemical and biological agents). while not all WMDs can be lumped together, a scan of the literature made clear that it was a nonroutine project and that there was sufficient information available on the actual implementation of the project (including an interview with someone directly involved in the project and some secondary literature based on primary sources) that I could understand (namely, in English). This availability of data is probably related to the fact that this case already dates back from the 90s. It is harder to find reliable data on groups – and their nonroutine plots – that are still active today (e.g. information on the chemical attacks by the Islamic State are often shrouded in secrecy and uncertainty).

2. 9/11 is selected as a case study because – while it can also be considered to be nonroutine – it is probably the case where the nonroutine nature of technology is the least outspoken. The invested human and material resources are moreover considered lower than those that would be invested in the adopted nuclear terrorism scenario. This way, this case study functions according to the logic of a least-likely case. In case similar dynamics can be identified in this case, it becomes more plausible to assume that these dynamics will also be at play throughout the implementation of a more nonroutine plot. Moreover, this case study is also selected due to the availability of information on the actual implementation of the plot. The unique nature and impact of this plot attracted a lot of governmental and scholarly attention.

Bibliography

Abrahms, Max. “Why Terrorism Does Not Work?” *International Security*, 2006.

———. *Rules for Rebels: the Science of Victory in Militant History,* Oxford: Oxford University Press, 2018.

Ackerman, Gary. “Motivations for Engaging in Nuclear Terrorism.” Expert Series Fund for Peace, 2006.

———. “Designing Danger: Complex Engineering by Violent Non-State Actors: Introduction to the Special Issue.” *Journal of Strategic Security* 9, no. 1 (2016).

———. "More Bang for the Buck: Examining the Determinants of Terrorist Adoption of New Weapons Technologies," *Doctoral dissertation,* King's College 2014.

———. "Comparative Analysis of VNSA Complex Engineering Efforts," *Journal of Strategic Security* 9 (1) (2016).

Ackerman, Gary, and James Halverson. “Attacking Nuclear Facilities: Hype or Genuine Threat?” In *Nuclear Terrorism: Countering the Threat*. Global Security Studies. London & New York: Routledge, 2016.

Ackerman, Gary, and Jeremy Tamsett. *Jihadists and Weapons of Mass Destruction*. London & New York: CRC Press, 2009.

Ackerman, Gary, Charles Blair, and Jeffrey Bale. “Anatomizing Radiological and Nuclear Non-State Adversaries Task 2: Potential RN Adversary Behavioral Profiles.” START consortium, 2010.

Ackerman, Gary, Charles Blair, Jeffrey Bale, Victor Asal, and Karl Rethemeyer. “Anatomizing Radiological and Nuclear Non-State Adversaries: Task 1: Identifying the Adversary.” START consortium, 2009.

Albright, David. “South Africa’s Secret Nuclear Weapons.” Institute for Science and International Security, 1994.

———. *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies,* New York: Free Press, 2010.

Albright, David, and Andrea Stricker. *Revisiting South Africa’s Nuclear Weapons Program: Its History, Dismantlement, and Lessons for Today*. Washington: Institute for Science and International Security, 2016.

Allison, Graham. *Nuclear Terrorism: The Ultimate Preventable Catastrophe*. United States: Holt Paperbacks, 2005

———. “Did We Beat the Odds or Change Them?,” *PRISM,* no. 3 (2018).

Alvarez, Luis. *Adventures of a Physicist*. Vol. Alfred P. Sloan Foundation Series. New York: Basic books, inc., Publishers, 1987.

Amabile, Theresa, Conti Regina, Coon Heather, Lazenby Jeffrey, and Herron Michael. "Assessing the Work Environment for Creativity," *Academy of Management Journal,* 39, no. 5 (1996).

Asal, Victor, Ackerman Gary and Rethemeyer Karl. “Connections Can Be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Weapons.” *Studies in Conflict & Terrorism* 35, no. 3 (2012).

Asal, Victor, and Rethemeyer Karl. “The Nature of the Beast: Terrorist: The Organizational and Network Characteristics of Organizational Lethality.” *Journal of Politics* 70 (2) (2008).

Atkins, Stephen. *The 9/11 Encyclopaedia*. Westport and London: Praeger Security International, 2008.

Azzam, Abdullah. "Al Qa'ida al-Subah," 1988. Available at: https://insidethejihad.com/2014/03/al-qaida- al-subah-the-solid-base/

Badash, Lawrence, Joseph Hirschfelder, and Herbert Broida, eds. *Reminiscences of Los Alamos, 1943-1945*. Studies in the History of Modern Science. USA, UK, The Netherlands: Reidel Publishing Company, 1980.

Badey, T.J. “Nuclear Terrorism: Actor-Based Threat Assessment.” *Intelligence and National Security* 16, no. 2 (2001).

Ballard, Tim, Jason Pate, Gary Ackerman, Diana McCauley, and Sean Lawson. “Chronology of Aum Shinrikyo’s CBW Activities.” Monterey: James Martin Center for Nonproliferation Studies, August 26, 2005.

Barnaby, Frank. *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction*. London: Granta Books, 2003.

Berman, Eli, and Laitin David. "Religion, Terrorism, and Public Goods: Testing the Club Model," *Journal of Public Economics* 92, no.10-11 (2008).

Berman, Eli. *Radical, Religious and Violent: The New Economics of Terrorism*. Cambridge: MIT Press, 2009.

Bijker, Wiebe, and John Law. *Shaping Technology: Building Society*. Cambridge & London: MIT Press, 1992.

Blair, Charles. “Jihadists and Nuclear Weapons.” In *Jihadists and Weapons of Mass Destruction*, CRC Press, 2009.

Bleek, Philippe. "Revisiting Aum Shinrikyo: New Insights into the Most Extensive Non-State Biological Weapons Program," *Nuclear Threat Initiative,* 2011.

Bloom, Mia. “Constructing Expertise: Terrorist Recruitment and ‘Talent Spotting’ in the PIRA, Al Qaeda, and ISIS.” *Studies in Conflict & Terrorism* 40, no. 7 (2017).

Brian, Danielle, and Stockton Peter. "U.S. Nuclear Weapons Complex: Security at Risk," *POGO,* 2001.

Braut-Hegghammer, Malfrid. "*Unclear Physics: Why Iraq and Libya Failed to Build Nuclear Weapons,* Ithaca and London: Cornell University Press, 2016.

Brown, Andres, and Glaser Alexander. "On the Origins and Significance of the Limit Demarcating Low-Enriched Uranium from Highly Uranium," *Science and Global Security* 24, no. 2 (2016).

Bunn, Matthew. “Guardians at the Gates of Hell: Estimating the Risk of Nuclear Theft and Terrorism and Identifying the Highest-Priority Risks of Nuclear Theft.” Massachusetts Institute of Technology, 2007.

Bunn, Matthew, Martin Malin, Nickolas Roth, and William Tobey. “Advancing Nuclear Security: Evaluating Progress and Setting New Goals.” Project on Managing the Atom. Cambridge: Harvard Belfer Center, March 2014.

———. “Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline.” Harvard Belfer Center, March 2016.

Bunn, Matthew, and Anthony Wier. “Terrorist Nuclear Weapon Construction: How Difficult?” *The Annals of the American Academy* 607 (2006).

Burke, J. “Recollections of Processing Uranium Hydride and Plutonium at Wartime Los Alamos.” *Journal of Nuclear Materials* 100 (1981).

Burns, Tom, and Stalker G.M. *The Management of Innovation.* United States: Tavistock Publications, 1961.

Burton, Richard, and Borge Obel. *Strategic Organizational Diagnosis and Design: The Dynamics of Fit*. New York: Springer Science, 2004.

Buys, Andre. “Proliferation Risk Assessment of Former Nuclear Explosives/Weapons Program Personnel: The South African Case Study.” University of Pretoria, 2007.

———. "Written Communication," 15 April 2017.

———. "Written Communication," 24 June 2017.

Byman, Daniel L. “Al-Qaeda as an Adversary: Do We Understand Our Enemy?” *World Politics* 56, no. 1 (2003).

Cameron, Gavin. “Multi-Track Microproliferation: Lessons from Aum Shinrikyo and Al Qaida.” *Studies in Conflict & Terrorism*, 2010.

Cann, Michelle. “Nuclear Security Commitment Making: Results of the Summit Process.” In *Nuclear Terrorism: Countering the Threat*, 215–32. Global Security Studies. London & New York: Routledge, 2016.

CBS News, “Nuke Facility Raid An Inside Job?” Available at: https://www.cbsnews.com/news/nuke-facility-raid-an-inside-job-19-06-2010/.

Clarke, Lee. *Worst Cases: Terrorism and Catastrophe in the Popular Imagination*. Chicago & London: The University of Chicago Press, 2006.

Cragin, Kim, and Sara Daly. “The Dynamic Terrorist Threat: An Assessment of Group Motivation and Capabilities in a Changing World.” RAND Corporation, 2004.

Crenshaw, Martha. “The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice.” In *Origins of Terrorism: Psychologies, Ideologies, Theologies, State of Mind*, 289. John Hopkins University Press, 1998.

———. *Explaining Terrorism: Causes, Processes and Consequences*. London & New York: Routledge, 2011.

———. “Terrorism Research: The Record.” *International Interactions: Empirical and Theoretical Research in International Relations* 40 , no. 4 (2014).

Dahl, Erik J. “The Plots That Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks Against the United States.” *Studies in Conflict & Terrorism* 34, no. 8 (2011).

Danzig, Richard, Marc Sageman, Terrance Leighton, Lloyd Hough, Hidemi Yuki, Rui Kotani, and Zachary Hosford. “Aum Shinrikyo Insights Into How Terrorists Develop Biological and Chemical Weapons.” Center for a New American Security, December 2012.

Dewar, Robert, and Jerald Hage. “Size, Technology, Complexity, and Structural Differentiation: Toward a Theoretical Synthesis.” *Administrative Science Quarterly* 23, no. 1 (1978).

Dolnik, Adam. *Understanding Terrorist Innovation: Technology, Tactics, and Global Trends*. Contemporary Terrorism Series. London & New York: Routledge, 2007.

———."Aum Shinrikyo's path to Innovation," in Rasmussen Maria and Hafez Mohammed, eds., *Terrorist Innovation in Weapons of Mass Effect: Preconditions, Causes and Predictive Indicators,* Defense Threat Reduction Agency, 2010.

Donaldson, Lex. *In Defense of Organisation Theory: a Reply to the Critics.* Cambridge: Cambridge University Press, 1985.

———. *The Contingency Theory of Organizations*. London: SAGE Publications, 2001.

Downes, Robert, and Christopher Hobbs. “Nuclear Terrorism and Virtual Risk: Implications for Prediction and the Utility of Models.” *European Journal of International Security* (2017).

Enders, Walter, and Paan Jindapon. “Network Externalities and the Structure of Terror Networks.” *Journal of Conflict Resolution* 54, no. 2 (2010).

English, Richard. *Does Terrorism Work: A History*. United Kingdom: Oxford University Press, 2016.

———. “The Future Study of Terrorism.” *European Journal of International Security* (2016).

Etzioni, Amitai. “Organizational Control Structure.” In *Handbook of Organizations*, Chicago: Rand McNally & Company, 1965.

Federation of American Scientists. “Nuclear Weapons Technology.” n.d., available at: http://fas.org/irp/threat/mctl98-2/p2sec05.pdf.

Ferguson, Charles, and William Potter. *The Four Faces of Nuclear Terrorism*. United States: Center for Non Proliferation Studies, 2004.

Feynman, Richard. "Los Alamos from below," in Badash, Lawrence, Joseph Hirschfelder, and Herbert Broida, eds. *Reminiscences of Los Alamos, 1943-1945*. Studies in the History of Modern Science. USA, UK, The Netherlands: Reidel Publishing Company, 1980.

Frost, Robin. *Nuclear Terrorism after 9/11.* United States & Canada: Routledge, 2005.

Flannery, Frances. *Understanding Apocalyptic Terrorism: Countering the Radical Mindset*. United Kingdom: Routledge, 2016.

Fletcher, Holly. "Aum Shinrikyo," *Council on Foreign Relations,* 2012. Available at: https://www.cfr.org/backgrounder/aum-shinrikyo

Flyvbjerg, Bent. "Five Misunderstandings About Case-Study Research." *Qualitative Inquiry* 12, no. 2 (2006).

Fouda, Yosri, and Nick Fielding. *Masterminds of Terror: Het Ware Verhaal Achter 11 September*. Utrecht & Antwerpen: Kosmos-Z&K Uitgevers, 2003.

Freidson, Eliot. *Professionalism: The Third Logic*. Cambridge: Polity Press, 2001.

George, Alexander, and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Canbridge & London: MIT Press, 2005.

Gill, Paul, John Horgan, Samuel T. Hunter, and Lily D. Cushenbery. "Malevolent Creativity in Terrorist Organizations." *The Journal of Creative Behavior* 47, no. 2 (2013).

Glaser, Alexander. " Personal Communication," 20 September 2018.

Glaser, Barney, and Anselm Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. New Brunswick & London: AldineTransaction, 1967.

Glaser, Alexander. "On the Proliferation Potential of Uranium Fuel for Research Reactors at Various Enrichment Level," *Science and Global Security* 14 (1) (2016).

Gressang, I.D. "Audience and Message: Assessing Terrorist WMD Potential." *Terrorism and Political Violence* 13, no. 3 (2001).

Groueff, Stephane. J. Robert Oppenheimer's Interview, 1965.

Groves, Leslie. *Now It Can Be Told: The Story of the Manhattan Project*. 2nd ed. United States of America: Da Capo Press, 1983.

Gurr, Nadine, and Benjamin Cole. *The New Face of Terrorism: Threats from Weapons of Mass Destruction*. London & New York: I.B.Tauris, 2000.

Hage, Jerald. "An Axiomatic Theory of Organizations." *Administrative Science Quarterly* 10; no. 3 (1965).

Hawkins, David. "Manhattan District History: Project Y, The Los Alamos Project." Los Alamos Scientific Laboratory, December 1, 1961.

Heger, Lindsay, Danielle Jung, and Wendy Wong. "Organizing for Resistance: How Group Structure Impacts the Character of Violence." *Terrorism and Political Violence* 24, no. 5 (2012).

Hibbs, Mark. cited in Howlett Darryl, and Simpson John. "Nuclearisation and Denuclearisation in

South Africa," *Survival* 35, no. 3 (2008)

Hirschfelder, Joseph. "Scientific Technological Miracle at Los Alamos," in Badash, Lawrence, Joseph Hirschfelder, and Herbert Broida, eds. *Reminiscences of Los Alamos, 1943-1945*. Studies in the History of Modern Science. USA, UK, The Netherlands: Reidel Publishing Company, 1980.

Hoddeson, Lillian, Paul Henriksen, Roger Meade, and Catherine Westfall. *Critical Assembly: A Technical History of Los Alamos During the Oppenheimer Years, 1943-1945*. United Kingdom: Cambridge University Press, 2004.

Hoffman, Bruce. "Terrorism and WMD: Some Preliminary Hypotheses." *The Nonproliferation Review* 4 no. 3 (1997).

———. "Lessons of 9/11," Testimony submitted for the Committee Record to the United States Joint September 11, 2001 Inquiry Staff of the House and Senate Select Committees on Intelligence on October 8, 2002 (2002).

———. *Inside Terrorism*. New York: Columbia University Press, 2006.

Horton, Roy. "Out of (South) Africa: Pretoria's Nuclear Weapon Experience." INSS Occasional Paper 27. Counterproliferation Series. Colorado: USAF Institute for National Security Studies, 1999.

Howlett, Darryl, and John Simpson. "Nuclearisation and Denuclearisation in South Africa." *Survival* 35, no. 3 (1993).

Hunt, Raymond G. "Technology and Organization." *The Academy of Management Journal* 13, no. 3 (1970).

Hunter, Samuel, Shortland Neil, Crayne Matthew and Ligon Gina. "Recruitment and Selection in Violent Extremist Organisations: Exploring what Industrial and Organisational Psychology might Contribute," *American Psychologist* 72, no. 3 (2017).

Hymans, Jacques. *The Psychology of Nuclear Proliferation: Identity, Emotions, and Foreign Policy*. Cambridge: Cambridge University Press, 2006.

———. *Achieving Nuclear Ambitions: Scientists, Politicians, and Proliferation*. United States: Cambridge University Press, 2012.

———. "Review on Unclear Physics: Why Iraq and Libya failed to get the Bomb" *ISSF roundtable 9-22,* 2017. Available at: https://networks.h-net.org/node/28443/discussions/189010/issf-roundtable-9-22-unclear-physics-why-iraq-and-libya-failed-get#_Toc489128157

Ilardi, Gaetano. "The 9/11 Attacks: A Study of Al Qaeda's Use of Intelligence and Counterintelligence." *Studies in Conflict and Terrorism* 32, no. 3 (2009).

International Institute for Strategic Studies. "Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks - A Net Assessment." *Strategic Dossiers*, 2007.

International Panel on Fissile Materials. "Fissile Material Stocks," 2018. Available at: http://fissilematerials.org/.

Jackson, Brian. “Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption.” *Studies in Conflict & Terrorism* 24, no. 3 (2001).

———. “Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda.” *Studies in Conflict and Terrorism* 29, no. 3 (2006).

———. "Organisational decision-making by Terrorist Groups," in Davis, Paul K., and Kim Cragin, eds. *Social Science for Counterterrorism: Putting the Pieces Together*. Santa Monica, CA: RAND, 2009.

Jackson, Brian, John Baker, Kim Cragin, John Parachini, Horacio Trujillo, and Peter Chalk. “Aptitude for Destruction: Volume 1: Organizational Learning in Terrorist Groups and its Implication for Combatting Terrorism," RAND corporation, 2005.

———. “Aptitude for Destruction Volume 2 Case Studies of Organizational Learning in Five Terrorist Groups.” RAND corporation, 2005.

Janis, Irving. *Groupthink: Psychological Studies of Policy Decisions and Fiascos,* New York: Houghton Mifflin, 1982.

Jenkins, Brian. “The Organization Men: Anatomy of a Terrorist Attack.” In *How Did This Happen? Terrorism and the New War*. New York: Public Affairs, 2001.

———. *Will Terrorists Go Nuclear?* New York: Prometheus Books, 2008.

Jones, Gareth. *Organizational Theory, Design and Change: Text and Cases*. 4th ed. Pearson Prentice Hall, 2003.

Jones, Seth, and Martin Libicki. “How Terrorist Groups End: Lessons for Countering Al Qa’ida’.” RAND Corporation, 2008.

Kahneman, Daniel, and Amos Tversky. “Prospect Theory: An Analysis of Decision under Risk.” *Econometrica*, (1979).

Kaplan, David. “Aum Shinrikyo.” In Tucker Jonathan, ed., *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Cambridge & London: MIT Press, 2000.

Kaplan, David, and Andrew Marshall. *The Cult at the End of the World: The Incredible Story of Aum*. United Kingdom: Arrow, 1997.

Kemp, Scott. "The Non-proliferation Emperor Has No Clothes: The Gas Centrifuge, Supply-side Controls, and The Future of Nuclear Proliferation," *International Security* 38, no. 4 (2014).

Kenney, Michael. *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. Pennsylvania: The Pennsylvania University Press, 2007.

———. “‘Dumb’ Yet Deadly: Local Knowledge and Poor Tradecraft Among Islamist Militants in Britain and Spain.” *Studies in Conflict & Terrorism* 33, no. 10 (2010).

———. "Beyond the Internet: Metis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists," *Terrorism and Political Violence* 22, no.2 (2010).

Khripunov, Igor, Nikolay Ischenko, and James P. Holmes. *Nuclear Security Culture: From National Best Practices to International Standards*. IOS Press, 2007.

Kistiakowsky, George. "Reminiscences of Wartime Los Alamos," in Badash, Lawrence, Joseph Hirschfelder, and Herbert Broida, eds. *Reminiscences of Los Alamos, 1943-1945*. Studies in the History of Modern Science. USA, UK, The Netherlands: Reidel Publishing Company, 1980.

Krause, Peter. "The Political Effectiveness of Non-State Violence: A Two-Level Framework to Transform a Deceptive Debate." *Security Studies* 22, no. (2) (2013).

Kurth Cronin, Audrey. *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*. Princeton: Princeton University Press, 2009.

Kydd, Andrew, and Barbara Walter. "The Strategies of Terrorism." *International Security* 31, no. 1 (2006).

LaFree, Gary, Laura Dugan, and Erin Miller. *Putting Terrorism in Context: Lessons from the Global Terrorism Database*. Contemporary Terrorism Studies. London & New York: Routledge, 2015.

Levi, Michael. *On Nuclear Terrorism*. Cambridge & London: Harvard University Press, 2009.

Liberman, Peter. "The Rise and Fall of the South African Bomb." *International Security*, 2001.

Lieber, Keir, and Press, Daryl. "Why States won't give Nuclear Weapons to Terrorists?," *International Security* 38, no. 1 (2013).

Ligon, Gina, Pete Simi, Mackenzie Harms, and Daniel Harris. "Putting the 'O' in VEO's: What Makes an Organization?" *Dynamics of Asymmetric Conflict* 6 (2013).

Los Alamos Scientific Laboratory Public Relations. *Los Alamos: Beginning of an Era 1943-1945: Part 2,* United States: Los Alamos Scientific Laboratory, 2008.

———. *Los Alamos: Beginning of an Era 1943-1945: Part 3,* United States: Los Alamos Scientific Laboratory, 2008.

———. *Los Alamos: Beginning of an Era 1943-1945: Part 4,* United States: Los Alamos Scientific Laboratory, 2008.

Lugar, Richard. "The Lugar Survey On Proliferation Threats and Responses." Survey June 2005. Available at: https://fas.org/irp/threat/lugar_survey.pdf.

MacCalman, Molly. "A.Q. Khan Nuclear Smuggling Network." *Journal of Strategic Security* 9, no. 1 (2016).

Maerli, Morten Bremer, Annette Schaper, and Frank Barnaby. "The Characteristics of Nuclear Terrorist Weapons." *American Behavioral Scientist* 46, no. 6 (2003).

Manley, John. " A New Laboratory is Born" in Badash, Lawrence, Joseph Hirschfelder, and Herbert Broida, eds. *Reminiscences of Los Alamos, 1943-1945*. Studies in the History of Modern Science. USA, UK, The Netherlands: Reidel Publishing Company, 1980.

Mark, Carson, Theodore Taylor, Eugene Eyster, William Maraman, and Jacob Wechsler. "Can Terrorists Build Nuclear Weapons?" Washington: Nuclear Control Institute, 1987. http://www.nci.org/k-m/makeab.htm.

McAllister, Bradley, and Schmid, Alex. "Theories of Terrorism," in Schmid, Alex, *The Routledge Handbook of Terrorism Research,* New York and London: Routledge, 2011.

McCormick, Gordon. "Terrorist Decision Making." *Annual Review of Political Science* 6 (2003).

McCormick, Ty. "Al Qaeda Core: A Short History." *Foreign Policy* (blog), 2014. Available at: https://foreignpolicy.com/2014/03/17/al-qaeda-core-a-short-history/.

McDermott, Terry. *Perfect Soldiers: The 9/11 Hijackers: Who They Were, Why They Did It*. E-book: Harper Collins e-books, 2008.

McIntosh, Christopher, and Ian Storey. "Between Acquisition and Use: Assessing the Likelihood of Nuclear Terrorism." *International Studies Quarterly* (2018).

McPhee, John. *The Curve of Binding Energy*. New York: Farrar, Straus and Hiroux, 1980.

Mian, Zia. "Personal Communication," 18 September 2018.

Mintzberg, Henry. "Structure in 5's: A Synthesis of the Research on Organization Design." *Management Science*, 1980.

———. *Structure in Fives: Designing Effective Organizations*. New Jersey: Prentice-Hall, 1983.

Mobley, Blake. *Terrorism and Counterintelligence: How Terrorist Groups Elude Detection*. New York: Colombia University Press, 2012.

Morgan, Gareth. *Images of Organisation.* California: Sage Publications, 2006.

Moritz, Kutt. "Personal communication," 18 September 2018.

Moghadam, Assaf. "How Al Qaeda Innovates." *Security Studies* 22, no. 3 (2013).

Mowatt-Larssen, Rolf. "The Armageddon Test: Preventing Nuclear Terrorism." *The Bulletin of the Atomic Scientists*, 2009, 60–70.

———. "Al Qaeda Weapons of Mass Destruction Threat: Hype of Reality." Harvard Belfer Center, January 2010.

Mowatt-Larssen, Rolf, Pavel Zolotarev, Matthew Bunn, Yuri Morozov, Simon Saradzhyan, William Tobey, and Viktor Yesin. "The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism." Harvard Belfer Center, May 2011.

Mueller, John. *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al Qaeda*. Oxford: Oxford University Press, 2010.

Nakagawa, Tomomasa. "Personal Communication by Tu Anthony." 2012. Available at: http://asanltr.com/wordpressV1/wp-content/uploads/2012/04/ASA-12-2Marbig-copy.pdf

Narang, Vipin. " Strategies of Nuclear Proliferation: How States Pursue the Bomb," *International Security* 41, no. 3 (2017).

Narath, Albert. "The Technical Opportunities for a Sub-National Group to Acquire Nuclear Weapons," XIV Amaldi Conference on Problems of Global Security, 2002.

National Security History Series. *The Manhattan Project: Making the Atomic Bomb,* United States: U.S.

Department of Energy, 2010.

Nehorayoff, Andrea, Benjamin Ash, and Daniel Smith. “Aum Shinrikyo’s Nuclear and Chemical Weapons Development Efforts.” *Journal of Strategic Security* 9, no. 1 (2016).

Neumann, Peter, and Smith, M.L.R. *The Strategy of Terrorism. How it Works and Why it Fails,* London and New York, Routledge, 2008.

Nuclear Threat Initiative. *South Africa's Nuclear Chronology,* Washington: Center for Nonproliferation Studies, 2009.

———. "NTI Nuclear Materials Security Index.” 2016. Available at: http://ntiindex.org/data-results/theft-data/.

Ouagrham-Gormley, Sonia Ben. “An Unrealized Nexus? WMD-related Trafficking, Terrorism, and Organised Crime in the Former Soviet Union,” *Arms control today,* 2007.

———. “Barriers to Bioweapons: Intangible Obstacles to Proliferation.” *International Security*, 2012.

———. *Barriers to Bioweapons: The Challenge of Expertise and Organization for Weapons Development*. Cornell Studies in Security Affairs. London: Cornell University Press, 2014.

———. "Personal Communication," 23 December 2016.

Parachini, John. "Aum Shinrikyo," in Jackson Brian et al, eds. *Aptitude for Destruction: Volume 2: Case Studies of Organisational Learning in Five Terrorist Groups,* Santa Monica: Rand Corporation, 2005.

Parachini, John, and Katsuhisa Furukawa. “Japan and Aum Shinrikyo.” In *Democracy and Counterterrorism: Lessons from the the Past*, 641. Washington DC: United States Institute of Peace Press, 2007.

Perrow, Charles. “A Framework for the Comparative Analysis of Organizations.” *American Sociological Review*, 1967.

———. *Organizational Analysis: A Sociological View*. Great Britain: Tavistock Publications, 1970.

Pluta, Anna, and Zimmerman Peter. "A Disheartening dissent," *Survival,* 2006.

Post, Jerrold. "Prospects for Nuclear Terrorism: Psychological Motivations and Constraints," in Leventhal and Alexander. "Preventing Nuclear Terrorism," Massachusetts: Lexington Books, 1987.

Rasler, Don. "The Islamic State and Drones: Supply, Scale, and Future Threats," *Combating Terrorism Center,* 2018.

Ranstorp, Magnus, and Magnus Normark. *Unconventional Weapons and International Terrorism*. Political Violence. Routledge, 2009.

———. *Understanding Terrorism Innovation and Learning: Al Qaeda and Beyond*. London & New York: Routledge, 2015.

Rao, M.G., and Rao V.S.P. *Organisation Design, Change and Development,* New Delhi: Discovery Publishing House: 1999.

Rasmussen, Maria, and Mohammed Hafez. “Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators.” Defense Threat Reduction Agency Workshop report. Defense Threat Reduction Agency, 2010.

Reader, Ian. *A Poisonous Cocktail? Aum Shinrikyo’s Path to Violence*. Great Britain: NIAS Press, 1996.

Rhodes, Richard. *The Making of the Atomic Bomb*. New York: Simon & Schuster, 1986.

Rodionov, Stanislav. “Could Terrorists Produce Low-Yield Nuclear Weapons?” National Academies Press, 2002.

Rosenau, William. “Aum Shinrikyo’s Biological Weapons Program: Why Did It Fail?” *Studies in Conflict & Terrorism*, 2001.

Sagan, Scott. *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton: Princeton University Press, 1993.

Sageman, Marc. "Personal Communication," 24 October 2016.

Salama, Sammy, and Lydia Hansell. “Does Inent Equal Capability? AI-Qaeda and Weapons of Mass Destruction.” *The Nonproliferation Review* 12, no. 3 (2005).

Salik, Naeem. "Nuclear Terrorism: Assessing the Danger," *Strategic Analysis* 38, no. 2 (2014).

Schelling, Thomas. "Whatever Happened to Nuclear Terrorism?" Available at: https://d3qi0qp55mx5f5.cloudfront.net/cpost/i/docs/Schelling-Nuclear-Terrorism.pdf?mtime=1397148761

Scheuer, Michael. *Through Our Enemies’ Eyes: Osama Bin Laden, Radical Islam, and the Future of America*. 2nd ed. Washington: Potomac Books Inc., 2006.

Schmid, Alex. “Frameworks for Conceptualizing Terrorism.” *Terrorism and Political Violence*, 2004.

———. *The Routledge Handbook of Terrorism Research*. New York & London: Routledge, 2011.

Scott, Richard, and Gerald Davis. *Organizations and Organizing: Rational, Natural, and Open System Perspectives*. New Jersey: Pearson Prentice Hall, 2003.

Shapiro, Jacob. “Organizing Terror: Hierarchy and Networks in Covert Organizations,” 2005. http://www.teachingterror.net/resources/Shapiro%20organizing%20Terror.pdf.

———. “Terrorist Decision-Making: Insights from Economics and Political Science.” *Perspectives on Terrorism* 6, no. 4–5 (2012).

———. *The Terrorist’s Dilemma: Managing Violent Covert Organization*. Princeton: Princeton University Press, 2013.

Sin, Steve, and Marcus Boyd. “Searching for the Nuclear Silk Road: Geospatial Analysis of Potential Illicit Radiological and Nuclear Material Trafficking Pathways.” In *Nuclear Terrorism: Countering the Threat*, 159–81. Global Security Studies. London & New York: Routledge, 2016.

Slabber, Johan. "Written Communication," 17 August, 2017.

Smith, Daniel. "Personal Communication," 23 November 2016.

Sokolski, Henry. *Nuclear Weapons Materials Gone Missing: What Does History Teach?* United States: Strategic Studies Institute and U.S. Army War College Press, 2014.

———. "The Nuclear Terrorism Threat: How Real Is It? Two Views by Brian Michael Jenkins and John Lauder." Working Paper 1602. Nonproliferation Policy Education Center, 2016.

Sokova, Elena. "Nuclear material trafficking: historical trends and current patterns," *Presentation at Antwerp workshop on Preventing Nuclear Terrorism: the Role of Nuclear Security,* 2014.

Staff Statement No.1: Entry of the 9/11 Hijackers into the United States. National Commission on Terrorist Attacks Upon the United States, 2004.

Staff Statement No.16: Outline of the 9/11 plot. National Commission on Terrorist Attacks Upon the United States, 2004.

Stebbins, Robert. *Exploratory Research in the Social Sciences*. Qualitative Research Methods Series 48. London: SAGE Publications, 2001.

Stern, Jessica, *The Ultimate Terrorists,* Cambridge and London: Harvard University Press, 1999.

Steyn, Hannes, Richard Van der Walt, and Jan Van Loggerenberg. *Nuclear Armament and Disarmament: South Africa's Nuclear Experience*. New York: iUniverse, Inc., 2007.

Stumpf, Waldo. "Written Communication," 27 April 2017.

Sublette, Carey. "The Nuclear Weapons Archive: A Guide to Nuclear Weapons," n.d. http://www.ciar.org/ttk/hew/hew/.

Terrorist Financing Staff Monograph. Washington: National Commission on Terrorist Attacks Upon the United States, 2004.

The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, "Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001,"

The International Institute for Strategic Studies. "Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks - A Net Assessment," London: IISS, 2007.

Thorpe, Charles, and Steve Shapin. "Who Was J. Robert Oppenheimer? Charisma and Complex Organization." *Social Studies of Science* 30, no.4 (2000).

Tilly, Charles. "Terror, Terrorism, Terrorists." *Sociological Theory*, 2004.

———. "Terror as Strategy and Relational Process." *International Journal of Comparative Sociology* 46, no. 1–2 (2005).

Tishler, Nicole, "Trends in Terrorists' Weapons Adoption and the Study Thereof," *International Studies Review* (2018).

TRAC. "Maktab Al-Khidamat (MAK): Terrorist Groups," 2018. Available at: https://www.trackingterrorism.org/group/maktab-al-khidamat-mak.

Tu, Anthony. "What Were the Real Objectives of Aum Shinrikyo?" CBRNE terrorism newsletter, 2012.

Tucker, Jonathan. *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*. Cambridge & London: MIT Press, 2000.

———. *War of Nerves: Chemical Warfare from World-War 1 to Al-Qaeda,* New York: Random House Inc., 2007.

U.S. Department of Defense. "Military Critical Technologies List (MCTL) Part II: Weapons of Mass Destruction Technologies, Nuclear Systems Technology," 1998.

U.S. Atomic Energy Commission 1954, *In the Matter of J. Robert Oppenheimer,* Cambridge: MIT Press, 1971.

Van Wyk, Anna-Mart. "Personal Communication," 4 May 2017.

Venter, Al. *How South Africa Built Six Atomic Bombs*. South Africa: Ashanti Publishing, 2008.

Vogel, Kathleen. *Phantom Menace or Looming Danger? A New Framework for Assessing Bioweapons Threats*. Baltimore: The John Hopkins University Press, 2013.

Volders, Brecht, and Tom Sauer. "Introduction to the Book." In *Nuclear Terrorism: Countering the Threat*, 3–12. Global Security Studies. London & New York: Routledge, 2016.

Von Hippel, Frank. "Personal Communication," 19 September 2018.

Von Wielligh, Nic. "Written Communication," 22 April 2017.

Von Wielligh, Nic, and Lydia Von Wielligh-Steyn. *The Bomb: South Africa's Nuclear Weapons Programme*. Pretoria: Litera Publications, 2015.

Weber, Max. *Economy and Society: An Outline of Interpretive Sociology*. Berkeley,Los Angeles, London: University of California Press, 1978.

Weinstein, Jeremy. "Resources and the Information Problem in Rebel Recruitment." *Journal of Conflict Resolution*, 2005.

Wellerstein, Alex. "Critical Mass." *Restricted Data: The Nuclear Secrecy Blog* (blog). Accessed June 7, 2016. Available at: http://blog.nuclearsecrecy.com/2015/04/10/critical-mass/.

Wight, Colin. *Rethinking Terrorism: Terrorism, Violence and the State*. Rethinking World Politics. Palgrave Macmillan, 2015.

Willrich, Mason, and Taylor Theodore. *Nuclear Theft: Risks and Safeguards.* Cambridge: Ballinger Publishing Company, 1974.

Windisch, Steven, Michael K Logan, and Gina Scott Ligon. "Headhunting Among Extremist Organizations: An Empirical Assessment of Talent Spotting" 12, no. 2 (2018).

Wirz, Christoph, and Emmanuel Egger. "Use of Nuclear and Radiological Weapons by Terrorists?" *International Review of the Red Cross* 87, no. 859 (2005).

Woodward, Joan. "Technology and Organisation," in Handel, Michael. *The Sociology of Organisations: Classic, Contemporary and Critical Readings.* United States: Sage Publications, 2003.

X, “Broken Arrows: Nuclear Weapons Accidents.” *Atomic Archive* (blog), n.d. http://www.atomicarchive.com/Almanac/Brokenarrows_static.shtml.

Yin, Robert. *Case Study Research: Design and Methods*. Applied Social Research Methods Series. London: SAGE Publications, 2003.

Younger, Stephen. *Endangered Species: How We Can Avoid Mass Destruction and Build a Lasting Peace*. United States: Harper Perennial, 2008.

Zaitseva, Lyudmila, and Hand Kevin. "Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-users," *American Behavioral Scientist* 46, no.3 (2003).

Zaitseva, Lyudmila. "Nuclear Trafficking: 20 years in Review," *Contribution to WFS Meeting,* 2010.

Zanders, Jean Pascal. “Internal Dynamics of a Terrorist Entity Acquiring Biological and Chemical Weapons: Insights for the Study of Possible Nuclear Weapon Acquisition.” In *Nuclear Terrorism: Countering the Threat*, 26–54. Global Security Studies. London & New York: Routledge, 2016.

———. "Personal Communication," 27 October 2016.

Zanders, Jean Pascal, Edvard Karlsson, Lena Melin, Erik Naslund, and Lennart Thaning. “Risk Assessment of Terrorism with Chemical and Biological Weapons.” SIPRI yearbook. Sweden: SIPRI, 2000.

Zelikow, Philip, Christopher Kojm, and Daniel Marcus. “The 9/11 Commission Report.” National Commission on Terrorist Attacks Upon the United States, 2004.

Zenko, Micah. “Micah Zenko - A Nuclear Site Is Breached,” December 20, 2007. http://www.washingtonpost.com/wp dyn/content/article/2007/12/19/AR2007121901857.html.

Zentner, M.D., Coles, G.L., and Talbert, R.J. *Nuclear Proliferation Technology Trends Analysis,* PNNL-14480, Pacific Northwest National Laboratory, 2005.

Zimmerman, Peter, and Jeffrey Lewis. “The Bomb in the Backyard.” *Foreign Policy*, October 16, 2009.

Zimmerman, Peter. "The Impossibility of Probabilities," *AIP Conference Proceedings,* 2017. https://aip.scitation.org/doi/abs/10.1063/1.5009233