Refining the risk of chemical and biological terrorism

What is the nature of the gap between academic and policy perspectives on chemical and biological terrorism and how might this begin to be bridged?

Katalin Petho-Kiss

This thesis is submitted for the degree of Master of Research

Department of Security Studies and Criminology

Faculty of Arts

Macquarie University

2018

Statement of Originality

This is to certify that to the best of my knowledge; the content of this thesis is my own work. It is not substantially the same as any that I have submitted, or, is being concurrently submitted for a degree or diploma or other qualification at Macquarie University or any other university or similar institution. I further state that no substantial part of this thesis has already been submitted, or, is being concurrently submitted for any such degree, diploma or other qualification at Macquarie University or any other university of similar institution except as declared in the text.

Katalin Petho-Kiss

Acknowledgements

First and foremost, I would like to thank the Endeavour Scholarship Award which facilitated my participation in the program. I would like to acknowledge the support and contribution of my supervisor, Dr. Julian Droogan, who guided me how to transform my ideas into academic research considerations. Special thanks to Merril Howie, who highlighted the importance of writing style and practiced with me how to imply its elements into an academic paper.

And to my amazing family – my husband Roland, thank you for your endless love and support , and to our wonderful daughter, Emma. I wish to thank you for encouraging me to take this challenge, joining me in this adventure and travelling to the completely other side of the world.

Biographical sketch

I have been drawn to complete a Masters of Research in the field of CBRN terrorism because of questions that arose during my work in law enforcement in Hungary and Europe.

I have worked for the last decade in the field of countering terrorism first at the law desk of the Europol National Unit, then as the deputy-head of the Central European CBRNE Training Centre. During the course of working for the law enforcement community, I investigated criminal attempts to acquire and use CBRNE materials for deceitful purposes and was committed to identify those malicious criminal intents that meant to cause devastating harm. This work experience fueled my research interest in the topic. I intended to better understand the phenomenon of CBRN terrorism through the inclusion of a broader academic perspective. While researching and writing this thesis I have been eager to find ways to apply the considerations of academic research to the everyday work of law enforcement and intelligence agencies.

Completing the Master of Research Program and spending a significant amount of time delving into the academic spectrum of CBRNE-terrorism research, has raised my curiosity and fueled my commitment to continue research in this highly topical issue. After graduating, I intend to pursue further academic research through progressing to a PhD Program looking at the illicit trafficking of CBRN materials. In my future academic endeavors, I intend to focus on elaborating the operational environment of terrorists and criminals who intend to acquire or employ CBRN materials.

I hope that my research as well as my professional counter terrorism experience will contribute to improving the current understanding of criminal and terrorist tactics and operational practices with regard to the unlawful activities concerning weapons-usable materials and hence allow for a more accurate estimation of the risk of CBRN terrorism.

Abstract

To better understand and ultimately respond to chemical and biological terrorism, academic and law enforcement communities need to establish a closer interaction between their respective realms. This paper attempts to bridge strategist scholarly and policy considerations on chemical and biological terrorism into one unique risk-assessment. The paper has devised a novel approach and reconstructs the phases of commission – firstly, the acquisition of knowledge on chemical and biological (CB) agents, secondly, the acquisition of CB materials, thirdly, the development of the CB weapon and finally, the execution of the attack – that constitute the key units for the analysis. At each perpetration phase the discussion analyses the challenges that the offenders need to tackle. By way at case study the thesis then evaluates the effectiveness of the respective Australian and EU-level counter CB terrorism provisions to pinpoint their vulnerabilities. The analysis has attempted to identify unregulated or insufficiently regulated areas of the aforementioned counter strategies and has suggested where policy gaps can be addresses by academic considerations.

Key words: chemical and biological terrorism, EU and Australian counter CB policies

Table of Contents

Part I

Chapter One: Introduction 8

Part II

Chapter Two: Literature Review 18

Part III

Chapter Three: Introduction 35

Chapter Four: Chemical Scenario 45

Chapter Five: Biological Scenario 85

Part IV.

Chapter Six: Conclusions 100

Sources consulted 105

PART I

Chapter One

Introduction

1.1. Statement of topic

There is a conceptual gap in assessing the risk of a terrorist attack where chemical, biological, radiological or nuclear (CBRN) materials are involved. Ongoing debate in this area reflects two contrasting standpoints – that of academics and that of those who are primarily policy orientated. Despite academic skepticism concerning the estimation of terrorists' or extremists' potential for employing these weapons, widespread legislation and counterstrategy reflects the policymakers' views that the threat is compelling. While policymakers appear to be alarmists and aim to forecast future threats and challenges, academics generally adopt a more sanguine position that tends to underplay the risk of future CBRN terrorism. The academic community has put forward sober analyses of non-state actors' apparently limited motivations and capabilities in launching a successful CBRN attack. These speculations rely, however, on shortcomings. The dearth of valuable data for a robust analysis, or rather the lack of attempts to use available information, has resulted in a current 'interpretative impasse'[1] in the literature between contrasting academic and policy orientated perspectives on the risk of CBRN terrorism.

1.2. Research aim

To better understand the threat of chemical and biological (CB) terrorism, scholarly and practitioner endeavors would do well to combine and mutually strengthen their respective perspectives. As Ackerman points out, academic and law enforcement communities need to

[1] Gary Ackerman, 'WMD Terrorism Research: Whereto from Here?', *International Studies Review*, 2005, 7:1, p. 140.

find a way to 'form direct and durable links'[2] to offer more appropriate responses to CB terrorism.

This thesis aims to assist this endeavor, by mapping and clarifying the nature of the gap between academic and policy perspectives. In doing so, it reveals how these widely differing risk perceptions might begin to be bridged. With this focus in mind, the following research seeks to identify insufficiently regulated and unregulated areas in the Australian and EU-level counter CB strategies and applies academic considerations in the law enforcement machinery in order to arrive at significant benefits.

Through combining these two perspectives, this thesis devises a unique form of risk assessment in terms of CB terrorism. The novel and significant contribution of this research stems first from its bridging of distinct academic and policy risk perceptions and, second, in the assessment of the two regional counter CB policies.

1.3. Limitations to the research

It was extremely difficult to organize the policies in two remote jurisdictions — the EU-level and the Australian system of counter provisions — into one systemic framework. As each of these respective counter policies follows a different logic and therefore is structured in lieu with their idiosyncratic principles, the measures relevant for this analysis were to be collected from several sections of these counter strategies and were systematically reorganized for this concept. This difficulty was further magnified by the interdisciplinary nature of CB threats. Without becoming lost in the scientific details of the issue, this thesis aims to focus on a strategic and not too technical perspective when analyzing these respective counter CB policies.

[2] Gary Ackerman, 'Defining knowledge gaps within CBRN terrorism research', in Magnus Ranstorp and Magnus Normark (Eds.), *Unconventional Weapons and International Terrorism, Challenges and new approaches*, London and New York: Routledge, 2009, p. 16.

The preliminary intention of the research was to draw the correlation with regard to all four strands of CBRN terrorism, but the volume of this analysis would go far beyond the size of this paper. Therefore, CB events were chosen as these limited the scope at the thesis, while their use by non-state actors also arguably poses more of a threat than radiological or nuclear materials. It is widely acknowledged that chemical and biological agents are much easier to acquire and require less financing and expertise to weaponized and deploy.[3] Accordingly, a plausible chemical and biological scenario has been outlined in the second half of this thesis and used as the basis for the analysis. When choosing the two case studies it was important to consider plausible scenarios that also allow for the examination of all their perpetration phases.

Another key consideration is that a considerable part of both the EU-level and the Australian counter CBRN-terrorism provisions falls under the intelligence remit and therefore are regulated in classified documents. This applies predominantly to the Australian strategy. Finding publicly available information on the Australian national CBRN strategy has proven to be particularly challenging. However, the accessible counterterrorism-related policies and documents have been consulted as they represent the general approach that Australian counterterrorism strategy embodies. These focus rather on the human factor of counter-terrorism efforts and endeavors to better understand and thereby identify and counter radicalized individuals in the society.[4] This perspective is different from the EU-level concept, that focusses on the detection of hazardous materials.[5] Through comparting and

[3] NATIBO, "Biological Detection System Technologies Technology and Industrial Base Study: A Primer on Biological Detection Technologies," in *Book Biological Detection System Technologies Technology and Industrial Base Study: A Primer on Biological Detection Technologies*, (City: North American Technology and Industrial Base Organization, 2001); Andrea A. Nehorayoff, Benjamin Ash and Daniel S. Smith, 'Aum Shinrikyo's Nuclear and Chemical Weapons Development Efforts', *Journal of Strategic Security* 2016:1,p. 35-48, available at: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1510&context=jss.

[4] Council of Australian Governments, Australia's Counter-Terrorism Strategy, Strengthening Our Resilience, 2015, p. vi.

[5] COM (2017) 610 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, p.5-7.

contrasting such diverse approaches the results of this thesis may help illuminate a combined counter strategy that relies on a delicate balance of both approaches. It is hoped that this outcome justifies the rationale behind comparing these two jurisdictions.

1.4. Significance

This research argues the need for a closer cooperation between respective academic and practitioner domains with regard to the CB-terrorism-related threats, proposing a way to bridge the distinct risk perceptions of these two domains. This project has devised a novel approach that is tested through two plausible scenarios. The results illustrate how the respective counter policies could be improved by the inclusion of academic considerations.

This research aims to contribute to the study of CB terrorism in three ways. First, it maps the key elements of the Australian and EU-level counterstrategies in order to identify their strengths and weaknesses. Second, it pinpoints those regulative gaps in the counter policy that can be closed by academic research. And third, it aims to partially bridge the gulf between academic and policy risk perceptions.

1.5. Scope

In August 2017, Australian law enforcement and intelligence authorities disrupted a plot involving an improvised chemical dispersal device consisting of hydrogen sulphide gas.[6] In the meantime, the European Union was coping with an IS related terrorist threat of a particularly wide scope. According to the concept of 'New' terrorism, today both terrorist groups and radicalized individuals seek to inflict maximum casualties with the intention of increasing the number of victims, as well as inflicting psychological and economic hardship.[7]

[6] Andrew Zammit, 'New Developments in the Islamic State's External Operations: The 2017 Sydney Plane Plot', *CTC Sentinel*,10:9, October 2017, p. 13-18.
[7] COM (2017) 610 final, p. 2.

Both of these respective jurisdictions needed to be revised and reconceptualized to counter the current malevolent criminal trends in a novel, effective manner. Also, considering these two, geographically and politically distinct jurisdictions, strategic approaches of a wider variety can be elucidated.

It is crucial at the outset to define what we mean by 'CB terrorism'. No commonly accepted definition exists for the term.[8] Weapons of mass destruction (WMD) terrorism is generally applied for the large-scale and high-impact use of chemical, biological, radiological and nuclear substances'[9]. In this sense, violent non-state actors may resort to the criminal use of CB materials, although they may not intend to inflict the mass casualties that WMD suggests.[10]

The European Parliament and the European Council specify the 'manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, CBRN weapons'[11] as a terrorist offence.

To ensure a consistent, conceptual framework throughout the project, the following definition has to be applied for the term, '*CB terrorism*':

> *Chemical and biological terrorism encompasses all attacks in which criminals intentionally use or threaten to use CB substances for the purpose of harming humans or the environment in order to advance an ideological or political objective.*

[8] Stephen M. Maurer, 'Introduction: Worrying About WMD Terrorism', in Stephen M. Maurer, *'WMD Terrorism: Science and Policy Choices*', Cambridge, MA: MIT Press, 2009, p. 1.
[9] Jeffrey M. Bale and Gary A. Ackerman, 'Profiling the WMD Terrorist Threat', in Stephen M. Maurer, *'WMD Terrorism: Science and Policy Choices*', Cambridge, MA: MIT Press, 2009, p. 12.
[10] *Ibid.*, p. 12.
[11] Directive (EU) 2017/541 of the European Parliament and of the Council on combating terrorism, Article 3 (1)f

1.6. Research method

This thesis is structured into two sections. The first is a critical literature review investigating the risk of chemical and biological terrorism.

Given the extensive legislation on counter CB policies, this widespread counter strategy provides the baseline for the analysis in the second part of the thesis. In investigating how to make academic contributions practicable for policy efforts, the second part of the research outlines one chemical and one biological plausible incident scenario.

A CBRN incident requires a broad spectrum of counteractions both during the prevention and preparedness phase. These actions cover technical, medical, scientific, law enforcement, human, societal and political aspects. Thinking through different scenarios offers the potential to examine and analyze the system of counterstrategy in a methodologically rigorous manner. Elaborating specific scenarios allows the comparative analysis of the critical steps of counteractions and helps to identify and understand crucial factors and aspects of such comprehensive incidents.[12] This research method facilitates the testing and validation of counterstrategies and thereby pinpoints particular needs and gaps[13].

Criminal conduct that aims to engage in CBRN terrorism has essentially four phases. These are: first, the acquisition of knowledge on CBRN materials; second, the acquisition of CBRN materials; third, the development of CBRN weapon and finally, the execution of the attack. These phases of commission provide the key units for the analysis. In each scenario, the research takes a retrospective approach from the occurrence of the CBRN attack and attempts

[12] Daniel M. Gerstein, *Bioterror in the 21st Century: Emerging Threats in a New Global Environment*, Annapolis, MD: Naval Institute Press, 2009, p. 142.

[13] H. S. Heireng, M. Endregard, H. Breivik, H. Erikkson, P. A. Fonteyne, D. Kelly and T. Sandrup, 'The development and use of CBRN scenarios for emergency preparedness analyses', Conference paper, 11th International Symposium on Protection Against Chemical and Biological Warfare Agents, 3-5 June, 2013, Stockholm.

to reconstruct all four phases of non-state actors' conduct. The discussion follows all these perpetration phases to understand the barriers and challenges criminals needs to surmount for a successful CBRN attack. Simultaneously, the analysis also aims to test the effectiveness of current Australian and EU-level counter CBRN terrorism strategies. This structure provides suggestions concerning how to address identified gaps.

To orient the discussion in the thesis, the following set of frames have been deployed when selecting the appropriate scenarios. First, when referring to perpetrators, the scope of the thesis covers only non-state actors (terrorist or extremist groups). While state sponsorship might be a factor for terrorist or extremist groups to engage in CBRN terrorism, the encompassing of WMD motives of rogue states would require a far broader perspective for the analysis, thereby exceeding the scope of this thesis. Second, this research aims to elaborate the risk of CBRN materials getting into the hands of criminals, and therefore addresses the prevention and preparedness phase of counter strategies. Counter CBRN terrorism strategies incorporate essentially three pillars, namely, prevention of, preparedness for and the response to CBRN terrorist attacks. The scope of this thesis covers the counter provisions for the prevention, but not the response to CBRN attacks. Two arguments substantiate the importance of addressing the prevention phase. First, the catastrophic consequences of a CBRN attack highlight that a strong emphasis should be placed on preventing such incidents occurring. Therefore, one of the main pillars of counter policies is prevention. Both the EU-level and the Australian counter strategies devote a considerable part of their regulation to the prevention of CBRN-related terrorist attacks.[14] Another aspect is the fact that to acquire the essential information and the agent, the perpetrators need to attend in person and contact others, thus exposing themselves to the risk of detected by law enforcement agencies. Therefore, the possibility of exposure is highest during the acquisition phase. The further the

[14] As Howard argues 'the only effective way to influence the bin Ladens of the world is to preempt them before they can act'. In: Russell D. Howard, 'Preemptive Military Doctrine: No Other Choice' in James J. Forest and Russell D. Howard (Eds.), *Weapons of Mass Destruction and Terrorism Second Edition*, New York: McGraw-Hill, 2012, p. 473.

terrorist proceeds in the phases of commission, the less chance there is of detecting the malicious intent. This initial phase is the best time to identify suspicious behavior or interactions that aim to engage in CBRN warfare.

Additionally, CBRN incidents resulting from an accident or the unintentional criminal use of hazardous materials are outside the scope of this discussion. Both scenarios have been selected as being highly plausible, moreover in terms of both the phases of the perpetration can be easily identified and analyzed and the relevant, applicable can be logically represented accordingly.[15]

1.7. Outline of the chapters

This thesis will proceed in six chapters. The literature review in Chapter Two is divided into sections and the discussion is organized into the following thematic subjects. The review begins with an introduction to the conceptual gap between the academic and the policy strategist risk perceptions. The next section discusses the literature on the potential for the criminal use of chemical and biological agents. To further understand the academic skepticism towards the validity of the threat, the current state-of-the-art and the shortcomings of the academic research on CB terrorism are explored. Chapter Three provides an introduction for the upcoming analysis. Chapter Four elaborates the chemical, while Chapter Five the biological scenario. The final conclusions of this research are discussed in the concluding chapter.

The research's three main recommendations are:

- To improve the anticipation of CB-terrorism related threats, intelligence and law enforcement agencies need to better understand the actor(s) behind these endeavours and consider the capabilities, motives and other influencing factors of criminal

[15] Monica Endregard, Hanne Breivik, Hege Schultz Heireng, Elin Enger, Therese Sandrup and Dominic Kelly, *D2.1 Scenario template, existing CBRN scenarios and historical incidents*, PRACTICE WP2 Deliverable, 2011.

entities. This would also facilitate a more effective legislative approach in terms of the concerns of dual-use technologies.

- By providing insightful analyses of past incidents where insiders compromised the safety of hazardous CB agents, academic discussions would shed light on those loopholes that undermine the necessary elevated level of security around these materials.
- Having acknowledged that the general public plays a remarkably important role in detecting the indicators of these malicious endeavours, public awareness raising campaigns should be extended to the potential early warning signs during the development phase of a CB-terrorist incident, and not only concern the crisis management of the attacks.

PART II

Chapter Two

2.1. Literature Review

This chapter encompasses a concise outline of the prevalent academic standpoints and debates on the risk of chemical and biological terrorism. The purpose of this review is two-fold. First, it introduces the CB threat-related scholarship by mapping and exploring the academic contributions and the current state-of-the-art in the field. And second, it aims to identify the applicability of these academic assertions and position them in the system of the respective counter policies – a point that is followed up in the third part of the thesis.

2.2. Is the threat of terrorists' or extremists' chemical and biological potential real?

There has been an ongoing debate on the threat of mass casualty attacks where chemical and biological (CB) weapons are involved, reflecting two contrasting standpoints. While policymakers seem to be 'alarmists'[1] and speculate on future predictions and risk, academics apparently take the position of 'minimalists'[2] and investigate past incidents[3], their findings tend to underestimate the risk of future CB terrorism. However, the actual use of CB weapons has been particularly rare, the recently interdicted WMD plots[4] push the academic community to 'separate fact from fiction by examining, synthesizing, and critically evaluating the existing scholarly and policy-related literature'[5].

[1] Chris Dishman, 'Understanding Perspectives on WMD and Why They Are Important', in *Studies in Conflict and Terrorism*, 2001:24, p. 303-304.
[2] *Ibid.*
[3] John V. Parachini, 'Comparing Motives and Outcomes of Mass Casualty Terrorism Involving Conventional and Unconventional Weapons', in Bruce Hoffman and Anders Strindberg (Eds.), *Terrorism and Beyond: A 21st Century Perspective*, Routledge Library Editions, Terrorism and Insurgency, Routledge, London and New York, 2015, p. 76-93.
[4] e.g. Andrew Zammit, 'New Developments in the Islamic State's External Operations: The 2017 Sydney Plane Plot', *CTC Sentinel*,10:9, October 2017, p. 13-18.
[5] Stephen M. Maurer, *WMD Terrorism: Science and Policy Choices*, Cambridge, MA: MIT Press, 2009, p. 11.

Three 'major schools of thought'[6] can be identified in the debate around the risk of CB terrorism, namely the optimist, the pessimist and the pragmatist. Optimists assess the potential for the criminal use of weapons-usable materials in terms of a 'very low probability, very low consequence'[7] threat based upon the assumption that terrorist groups neither have the motivation nor the capability to engage in such attacks. Pessimists regard the threat as a 'low, but growing probability, high consequence'[8] one. The technological advancements and developments in the capabilities and intentions of terrorists, together with the increasing influence of religious-driven ideologies all account for this pessimistic estimation. Pragmatists state that the risk of CB terrorism is a 'low probability, high consequence'[9] threat. They focus on understanding the factors that play a crucial role in the decision-making of terrorist groups. Although acknowledging the easier ways offered by modern technology, they aim to examine the challenges of the acquisition and development of unconventional weapons.[10]

In this debate the academic community agrees only on some aspects of the CB terrorism-related risk. There is consensus with regard to certain assertions, such as incentives that make unconventional weapons attractive to terrorists, or the fact that many terrorist organizations have considered the use of CB weapons, moreover stating that modern technological advancements facilitate an easier acquisition of CB capabilities.[11]

To represent the diversity in understanding the potential for the criminal use of weapon-usable materials, some competing standpoints on this topic are cited below. Embracing the tenets of new terrorism, Campbell asserts that the inherently evolving nature of terrorism

[6] G. D. Kobentz, 'Predicting Peril or the Peril of Prediction? Assessing the Risk of CBRN Terrorism', *Terrorism and Political Violence*, 2011, 23:4, p. 501.
[7] *Ibid.*, p. 503.
[8] *Ibid.*, p. 503.
[9] *Ibid.*, p. 503.
[10] *Ibid.*, p. 503.
[11] Victor H. Asal, Gary A. Ackerman, R. Karl Rethemeyer, 'Connections Can be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Weapons', *Studies in Conflict and Terrorism*, 2012, 35:3, p. 231.

constantly generates more lethal motives, that if combined with technological advancements will result in an increased potential for terrorists and other criminals to use weapons of mass destruction.[12] Meanwhile, Sprinzak argues that modern terrorists are generally not politically motivated, such that they do not avoid inflicting mass casualties in order to facilitate the witnessing by others of their terrorist acts[13]. Previously terrorists were motivated by having a seat at the negotiation table, but now they 'want to destroy the table and everyone sitting at it'[14]. At the same time, Sprinzak reasons that these politically motivated terrorist groups are not invisible, thus their attempts to acquire or use CB weapons will likely be noticed by the authorities.[15] Hoffman moves beyond this consideration, highlighting how religious ideologies influence modern terrorists' motives which tends to push them toward inflicting mass casualties. He cites different reasons, however, as to why they are still reluctant to employ CB materials in their attacks. Hoffman asserts that terrorists prefer to use conventional tactics and devices with which they are already familiar such as guns and bombs.[16]

In terms of terrorists' and other non-state actors' capabilities for acquiring and constructing such weapons, two important points should be noted. There exists at least one sub-set of terrorists who are capable of overcoming the 'technical, organizational and logistical obstacles'[17] linked to weapons of mass destruction. In the same vein, terrorists have already proved their consistent ability to keep up with modern technological advancements and be innovative in achieving either their strategic or operational objectives. On the other hand, the commercialization of biotechnology, for example, facilitates even non-state actors ability to

[12] In *Hype or Reality: The "New Terrorism" and Mass Casualty Attacks*, Alexandria, VA: Free Hand Press, Chemical and Biological Arms Control Institute, 2000.
[13] Brian Jenkins, 'Terrorism and Beyond: A 21st Century Perspective', *Studies in Conflict and Terrorism*, 2001.
[14] Quote attributed to James Woolsey, 1994.
[15] Ehud Sprinzak, 'The great superterrorism scare', *Foreign Policy*, 1998:112, p. 110-124.
[16] Bruce Hoffman, 'The Debate Over the Future Use of Chemical, Biological, and Radiological, and Nuclear Weapons', *Hype or Reality: The "New Terrorism" and Mass Casualty Attacks*, Alexandria, VA: Free Hand Press, 2000.
[17] Steven Simon and Daniel Benjamin, 'America and the New terrorism', *Survival*, 2000, 42:1, p. 8.

acquire access to this equipment and techniques that used to be the privilege of the state's apparatus.

Having the capability to engage in CBRN warfare, however, does not necessarily mean that the terrorist entity will resort to unconventional means. While the capabilities of potential terrorist groups have been given an utmost scholarly attention, only a small fraction of the WMD-terrorism-related literature considers the motivations of these violent non-state actors.[18] In this vein, jihadist groups ideological motivations and operational objectives require a careful assessment.[19] More specifically, there are numerous 'formidable inhibitors'[20] that keep criminals away from employing unconventional weapons. First, there is a general reluctance to experiment with these less or unfamiliar type of weapons in case the user of the device gets hurt. Similarly, there is concern, as to whether these weapons would work at all. Second, the application of these weapons has only been sometimes successful. Third, it may result in alienating supporters because of the moral issues inherent in such attacks.[21]

On the other side, there are various facilitators that may push criminals toward developing and using non-conventional weapons. One of the most crucial incentives for employing weapons of mass destruction is the significance of the psychological consequences these attacks aim to induce. Civilian research institutes situated in conflict zones and the increasing number and easy access to precursors enable more assessable solutions. Moreover, the information revolution offers quick and credible sources regarding information on how to develop and use these types of weapons, and the widespread network of transnational organized crime helps the acquiring of appropriate components. Likewise, because of the

[18] Jeffrey M. Bale, *The Darkest Sides of Politics, Volume II, State Terrorism, "Weapons of Mass Destruction", Religious Extremism and Organized Crime*, New York: Routledge, 2018, p. 154-155.
[19] *Ibid.*
[20] Alex P. Schmid, 'Terrorism and the use of weapons of mass destruction: From where the risk?', *Terrorism and Political Violence*, 1993, 11:4, p. 120.
[21] *Ibid.*

relatively small size of these materials, their transportation is easy, while their detection is particularly challenging for the authorities.[22]

Asal et al., attempt to move beyond these motivational incentives to quantify how these factors interact with each other and thus influence the terrorists' decision-making. Their finding shows that first, economic embeddings and alliances are both associated with a greater likelihood of employing CBRN weapons. Second, the larger organizations are more prone to use weapons of mass destruction, and last, inexperienced organizations are less likely to launch CBRN attacks.[23]

It is important to distinguish between incidents where CBRN materials are used to cause mass casualties and attacks where these unconventional weapons would be used only at a smaller scale. Preparing for and successfully completing an incident which involves large-scale weapons of mass destruction depends on numerous factors. The more sophisticated and difficult the execution is, the less likely it is to occur.[24] Cole arrives at the same conclusion, arguing that the 'nature and extent of the current threat from CBRN terrorism remains unclear'[25]. To more accurately predict the future threat, he suggests examining factors such as the technical challenges of employing WMD, and the motivations and disincentives that may reflect the dynamics of their decision-making.[26]

When assessing the threat of bioterrorism, Ackerman and Moran lists a comprehensive range of factors that essentially determine whether terrorists or other non-state actors will or can engage in causing mass-casualties by employing unconventional weapons. Their capability to deploy these weapons varies in accordance with the following aspects. First, Ackerman

[22] *Ibid.*, p. 121.
[23] Victor H. Asal, Gary. A. Ackerman, R. Karl Rethemeyer, 'Connections Can be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Weapons', *Studies in Conflict and Terrorism*, 2012, 35:3, p. 243.
[24] Gary Ackerman, 2009, p. 13.
[25] B. Cole, *The Changing Face of Terrorism: How Real is the Threat from Biological, Chemical and Nuclear Weapons?*, New York: I. B. Tauris, 2011, p. 28.
[26] *Ibid.*

and Moran suggest that a kind of central leadership is necessary to coordinate the acquisition, development and deployment of these weapons.[27] It goes without saying that funding these efforts is of paramount importance, as well as the financial capacity of the actor[28] who intends to use these unconventional technologies. Another key condition for a successful attack is the ability to transport and communicate[29] within the organization in an efficient manner. Having the equipment and technology to develop such weapons presumes the expertise to use these technical advancements in a sophisticated way. The challenge in terms of this scientific expertise is that it needs to cover not only the 'explicit knowledge'[30] that can be gained from textbooks, but even the so-called 'tacit knowledge'[31] that is the outcome of practical experience. The capability of a non-state actor is not enough to deploy apocalyptic weapons. They also need to be motivated to engage in such activities. Ideological, strategical and tactical incentives[32] such as emphasizing their power by carrying out large-scale and highly sophisticated attacks or idiosyncratic needs may push criminal groups towards employing unconventional weapons. However, there are also constraints that may distract them, such as the perceived challenges of using these technologies, the unpredictability of their outcome or simply the easier alternatives offered by conventional weapons.

It is worthwhile considering that recent scholarly publications have asserted a shift in terms of the role WMD play in jihadist achievements. While jihadists previously threatened to employ CBRN weapons only as an instrument of deterrence, now it has turned into a 'legitimate first strike weapon'[33]. When discussing the threat of CBRN terrorism, Ackerman et al. point out that despite jihadist attempts to acquire WMD, no jihadist group could pursue

[27] Gary A. Ackerman and Kevin S. Moran, 'Bioterrorism and Threat Assessment, Prepared for the Weapons of Mass Destruction Commission', 2006, p. 11.
[28] Gary A. Ackerman and Kevin S. Moran, 2006, p. 11.
[29] *Ibid.*
[30] *Ibid.* p. 11-12.
[31] *Ibid.* and Donald Mackenzie and Graham Spinardi, 'Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons', *American Journal of Sociology*, 101:1, 1995, pp. 44-99.
[32] *Ibid.*, p. 14-16.
[33] Gary Ackerman and Jeremy Tamsett (Eds.), *Jihadists and Weapons of Mass Destruction*, CRC Press, 2009, p. xv.

a successful CBRN attack.[34] The authors conclude that while the intent to launch a successful WMD attack is medium to high on the risk scale − taking into account the challenges of acquiring, developing or using such apocalyptic weapons − the 'requisite capability is relatively low'[35]. Based on these estimations, the overall threat of WMD use is a low to medium one, far below the threat posed by conventional or low-tech terrorist attacks. Ackerman et al. take a dynamic approach and address the question of future developments, noting both terrorism and technology are 'inherently dynamic phenomena'[36]. Proceeding on the assumption that none of these phenomena are static, the threat of a plausible CBRN attack can never be completely dismissed.[37] In the long term, careful consideration should be given to the fact that jihadist groups often maintain strong alliances to other terrorist groups that may positively influence their probability for pursuing CBRN warfare.[38] Of concern however is the fact that the series of conventional or small-scale CBRN attacks may weaken the psychological effect they aim to induce, motivating these criminal groups to get engaged in even more sophisticated strikes.[39]

As Hummel concludes his risk assessment with respect to the Islamic States' WMD potential, 'reality constraints'[40] their progress. Although there are main obstacles that hinder their intent, it is still particularly challenging to get easy access to an appropriate target.[41] The Islamic States' willingness to employ biological weapons has been communicated in numerous cases. At the same time, the successful Western medical countermeasures - even with regard to the 2001 anthrax attacks and the Ebola crisis in 2014 – presumes only a limited impact of any biological incident.[42] Last but certainly not least, the Islamic State is presumed

[34] *Ibid.*, p. 405.
[35] Gary Ackerman and Jeremy Tamsett, 2009, p. 406.
[36] *Ibid.*, p. xxiv.
[37] *Ibid.*, p. 406.
[38] Victor H. Asal and R. Karl Rethemeyer, 'Islamist Use and Pursuit of CBRN Terrorism', in Gary Ackerman and Jeremy Tamsett (Eds.), *Jihadists and Weapons of Mass Destruction*, CRC Press, 2009, p. 348.
[39] Gary Ackerman and Jeremy Tamsett, 2009, pp. 414.
[40] Stephen Hummel, 'The Islamic State and WMD: Assessing the Future Threat', CTC Sentinel, 2016, available at: https://ctc.usma.edu/posts/the-islamic-state-and-wmd-assessing-the-future-threat
[41] *Ibid.*
[42] *Ibid.*

to continue employing the easiest and most accessible form of WMD, and a terrorist attack involving a chemical weapon remain of great concern.[43]

Another important perspective here is the WMD potential of lone actors and autonomous cells. While operating outside a formal terrorist organization might make their detention far more challenging for the law enforcement authorities, they can only depend upon limited capabilities in terms of organized trainings.[44] Modern global technical achievements offer them a cheaper, user-friendly pathway for development and empowerment in acquiring, constructing and using CBRN weapons.[45] In this vein, lone actors or autonomous cells are more likely to employ apocalyptic weapons compared to formal terrorist organizations, which need to take into account the morale of their sponsors and maintain clear operation-related traditions. These 'super-empowered individuals'[46] are fueled to cause shocking casualties – relying only on their own resources – to justify their unique power. Thus, since having a higher risk tolerance limit, CBRN weapons could be advantageous for them to achieve their aims. The inherent challenges around the acquisition, construction and use of such unconventional weapons make this mode of operation even more attractive for them.[47] Weapons of mass destruction can cause far more psychological harm than traditional guns or bombs, by satisfying the essential element of terrorism.[48] As Ellis argues, lone wolves or autonomous cells may not be engaged in sophisticated CBRN attacks, but can cause disruption even with the use of small-scale unconventional weapons such as industrial chemicals or radioactive material.[49] To further substantiate this claim, Fredholm argues that

---

[43] *Ibid.*

[44] Gary A. Ackerman and Lauren E. Pinson, 'An Army of One: Assessing CBRN Pursuit and Use by Lone Wolves and Autonomous Cells', *Terrorism and Political Violence*, 2014, 26:1, p. 226.

[45] *Ibid.*, p. 227.

[46] Thomas L. Friedman, *Longitudes and Attitudes: Exploring the World After September 11*, New York: Farrar, Straus and Giroux, 2002.

[47] Gary A. Ackerman and Lauren E. Pinson, 2014, p. 228.

[48] *Ibid.*, p. 228.

[49] P. D. Ellis, 'Lone Wolfe Terrorism and Weapons of Mass Destruction: An Examination of Capabilities and Countermeasures', *Terrorism and Political Violence*, 2014, 26:1, p. 220.

the likelihood of a successful lone actor CBRN attack remains slim, except for small-scale attacks, such as poison incidents'[50].

In terms of the bioterror threat, Koblentz stresses that although the biological weapon capabilities of terrorists are 'limited'[51], 'the advances in technology and the emergence of more violent groups pose long-term risks'[52]. While admitting that only a few terrorist groups have attempted to develop biological weapons, he concludes that the threat posed by terrorists using biological weapons should be kept 'in context'[53]. He forecasts that the next bioterror attacks will possibly entail 'second generation capabilities'[54] for acquiring and developing 'small quantities of low-quality biological agents and crude means of dissemination'[55]. These incidents may induce mass panic, and may result in mass casualties if there is no appropriate public health response to the attack. When assessing the terrorist potential to resort to biological weapons, he analyses two variables. First, the impact of modern developments in biotechnology and biodefense programs. And second, the matter of interest for applying biological capabilities to obtain objectives.[56]

In a related vein, Gerstein further stresses the direct relationship between globalization, terrorism and biotechnology and points out that these interactions will result in an increased terrorist capacity to develop and use biological weapons.[57] He notes that while the development in biotechnology is beneficial for humankind, at the same time there are also grave concerns that these innovations may facilitate the proliferation and malicious exploitation of these technologies. Gerstein draws attention to the significance of

[50] M. Fredholm (Ed.), *Understanding Lone Actor Terrorism: Past Experience, Future Outlook, and Response Strategies*, New York, NY: Routledge, 2016, p. 230.
[51] Gregory D. Koblentz, *Living Weapons: Biological Warfare and International Security*, Ithaca, NY: Cornell University Press, 2009, p. 3.
[52] *Ibid.*
[53] *Ibid.*, p. 226.
[54] *Ibid.*, p. 226.
[55] *Ibid.*, p. 226.
[56] *Ibid.*, p. 229.
[57] Daniel M. Gerstein, *Bioterror in the 21st Century: Emerging Threats in a New Global Environment*, Annapolis, MD: Naval Institute Press, 2009, p. 150.

advancements in biotechnology that made the development of biological weapons considerably easier. Likewise, the proliferation of these technological innovations will make it simpler for terrorist organizations to obtain biological weapon-usable material and alter it in accordance with their purposes.[58] Therefore, in the long run, as technological capabilities to develop a biological weapon become more accessible, the motivations of non-state actors will be the prevalent factor in deciding whether to resort to biological warfare.[59] Consequently, while assuming that only a minor subset of terrorist organizations will be capable of successfully acquiring and developing biological weapons whilst at the same time being motivated to resort to biological weapons, we need to prepare for the threat of bioterrorism a 'relatively low-probability yet high-consequence event'[60].

Assessing the threat of CBRN terrorism inherently calls upon 'adopting a multi- and interdisciplinary approach'[61]. Instead of elaborating these phenomena 'sui generis'[62], bridging various perspectives available 'on this multi-faceted problem'[63] would enable a more precise threat-assessment and a more suitable policy-analysis in the field. Volders suggests to contextualize the most common three independent variables in the literature – namely, i) the motivation of the terrorist organization to engage in CBRN warfare, ii) the availability of knowledge on these weapons-usable materials and iii) the availability of the materials.[64] Accordingly, he sets an interplay between the two necessary levels of the assessment, first, with regard to the question of the group's willingness versus opportunity trade-off and second, 'the implementation of the technical and organizational challenges'[65].

2.3. How to appropriately assess terrorists' or extremists' CBRN potential?

[58] Daniel M. Gerstein, 2009, p. 169.
[59] *Ibid.*, p. 171.
[60] *Ibid.*, p. 176.
[61] Brecht Volders and Tom Sauer, *Introduction*, in Brecht Volders and Tom Sauer (Eds,): *Nuclear Terrorism: Countering the Threat.* Abingdon-on-Thames: Routledge, 2016, p. 7.
[62] *Ibid.*
[63] *Ibid.*
[64] *Ibid.*, p. 13-14.
[65] *Ibid.*, p. 15.

Assessing the threat of CBRN terrorism is a particularly challenging task – especially without up-to-date access to classified intelligence. Academia has been extensively investigating how to assess the risk of CBRN terrorism and predict plausible future CBRN attacks for decades. Jenkins noted in 1975 that 'This type of forecasting is hazardous. The resultant predictions must be viewed as highly conjectural, tentative, and quite possibly dead wrong.'[66] Further, Rapoport states that 'no way exists to demonstrate terrorists will never use apocalyptic weapons'[67]. An independent scientific advisory group's risk assessment concluded that it was 'simply not possible to validate predictive models of rare events that have not occurred, and unvalidated models cannot be relied upon'[68]. Steinbruner regards as difficult the task to 'judge the actual probability'[69] of a deliberate mass destruction attack, however, adds that 'the danger is serious enough to justify the overriding priority […] of managerial control over the two technologies of greatest destructive potential – nuclear explosives and virulent biological pathogens'[70]. Notably, there have been numerous academic attempts to assess the risk of CBRN terrorism, however differing standpoints have emerged in relation to the evaluating the components of the risk as well as what weight should be given to these elements.[71]

When forecasting future attacks, historic incidents are inevitably considered. On one hand, as Jenkins[72] and Ackerman argue 'recorded history is an imperfect guide'[73] as not having

[66] Brian Michael Jenkins, *Will Terrorists Go Nuclear?*, Santa Monica, CA: RAND, 1975, p. 3.
[67] David C. Rapoport, 'Terrorism and Weapons of the Apocalypse', in *National Security Studies Quarterly* 5:3, 1999, p. 50.
[68] JASON The Mitre Corporation, *Rare Events*, McLean, VA: MITRE Corporation, 2007, p. 7.
[69] John Steinbruner, 'Terrorism: Practical Distinctions and Research Priorities', in The Forum: Nonstate Actors, Terrorism, and Weapons of Mass Destruction', *International Studies Review*, 2005:7, p. 139.
[70] *Ibid.*
[71] G. D. Kobentz, 'Predicting Peril or the Peril of Prediction? Assessing the Risk of CBRN Terrorism', *Terrorism and Political Violence*, 2011, 23:4, p. 502.
[72] Brian Jenkins, *The WMD Terrorist Threat: Is There a Consensus View?*, in Brad Roberts (Ed), *Hype or Reality? The „New Terrorism" and Mass Casualty Attacks*, Alexandria, VA: Chemical and Biological Arms Control Institute, 2000, p. 242, 245.
[73] Gary Ackerman, 2009. p. 16.

documented all relevant factors and aspects of these previous incidents, may lead to the generation of misguiding trends. It is important to emphasize, however, that there are valuable trends that can be measured and consistently observed which offer tangible contribution to future risk anticipations.[74]

Forest and Sinai offer an alternative analytical framework for examining the potential threat of the highly complex CBRN terrorism. To develop a more accurate analysis, they move beyond the previous analytical concepts that relied upon the combination of group intentions and capabilities, or were focused only on certain terrorist group, and rather monitor 'trends in seven areas of particular concern'[75]. According to their approach, the convergence of the following factors may elevate the threat of CBRN terrorism i) the proliferation of CBRN weapons, materials, and knowledge; ii) terrorist ideologies, strategies, and organizational structure; iii) organized crime; iv) cybersecurity; v) rogue and irresponsible states; vi) weak and failed states; and vii) the exploitation of democratic processes.

As a future trajectory for the research on CBRN terrorism, Ackerman points out that literature on the impact of technological change in patterns of criminal behavior could indicate the level of terrorist engagement in WMD weapons.[76] In terms of the future methodological challenges, Koblentz elaborates those heuristics and biases that account for both the under and over-estimation of the risk. He explores the influence of these systemic errors that lead to the misunderstandings in the risk assessment process, arguing that educating on these biases helps individuals avoid them.[77] He urges authorities to place a 'concerted'[78] emphasis on better understanding the risk assessments of CBRN terrorism.

---

[74] Gary Ackerman, 2009. p. 16.
[75] Joshua Sinai and James J. F. Forest, *Threat Convergence, A Framework for Analyzing the Potential for WMD Terrorism*, in James J. Forest and Russell D. Howard (Eds.), *Weapons of Mass Destruction and Terrorism Second Edition*, New York: McGraw-Hill, 2012, p. 725.
[76] Gary Ackerman, *WMD Terrorism Research* in J. Horgan and K. Braddock (Eds.), *Terrorism Studies: A Reader*, New York: Routledge, 2011, p. 391.
[77] G. D. Kobentz, 'Predicting Peril or the Peril of Prediction? Assessing the Risk of CBRN Terrorism', *Terrorism and Political Violence*, 2011, 23:4, p. 515.
[78] *Ibid.*, p. 516.

Up to this point the discussion has engaged in citing the corpus of scholarly standpoints and recommendations around the risk of CBRN terrorism. The following section looks beyond the academic perspective and sheds light on the existing shortcomings of the research. This may explain the academic skepticism towards the validity of the CBRN terrorism related threat.

2.4. The current state-of-the-art in terms of research on CBRN terrorism

The literature on terrorism has been increasing exponentially, enabling new perspectives to emerge in the study of this phenomenon.[79] However, this vast volume of terrorism-related writing – comprising predominantly literature reviews[80]– has relied on fairly limited empirical research[81]. The current state-of-the-art in terms of the research on terrorism has various shortcomings and these observations apply even to the literature on CBRN terrorism. The literature dealing with CBRN terrorism mainly focuses on terrorists' motivations for using CBRN weapons. However, these identified 'drivers and barriers are poorly defined and unclear'[82], lacking quantitative bases. Only a minor part of this scholarship engages in elaborating the potential of terrorists' using unconventional weapons or the consequence-management of such devastating attacks.[83]

Despite the abundance of available, open-source information, there is only some work that draws on empirical data. Since there is an absence of empirical data, the literature's assertions

[79] Adam Dolnik, 'Conducting Field Research on Terrorism: a Brief Primer', *Perspectives on Terrorism*, 2011, Volume 5, Issue 2, p. 3-35.
[80] Andrew Silke, 'Research on Terrorism', *Terrorism Informatics*, 2008, Volume 18, p. 27-50.
[81] Alex P. Schmid and Albert Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Oxford: North Holland 1988), p.179.
[82] Gary Ackerman et al (START National Consortium for the Study of Terrorism and Responses to Terrorism), *Profiling the CB Adversary: Motivation, Psychology and Decision-Research Brief*, 2017, p. 1.
[83] Victor H. Asal, Gary. A. Ackerman, R. Karl Rethemeyer, 'Connections Can be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Weapons', *Studies in Conflict and Terrorism*, 2012, 35:3, p. 231.

are overwhelmingly generalized and speculative predictions.[84] Additionally, we still do not know much about the operative capabilities or practices of terrorist groups. [85] Furthermore, there is a lack of knowledge around the technical and tactical aspects of terrorism.[86] Likewise, statistical data has not been used as a major research source, and the data that has been accessed has been used mainly in terms of descriptive analysis[87]. Further concerns exist with regard to the methodologies for gathering data and the data analysis process itself[88]. Even in the aftermath of 9/11 the available data for the analysis of terrorism is unsystematic and unreliable.[89] The research on the phenomenon still lacks 'precise, factual knowledge'.[90] As Ackerman states, the current research literature on CBRN terrorism has reached an 'interpretative impresse'[91], where no new insights are provided, only the same materials are constantly recycled and reevaluated.

Academic research could certainly enhance our understanding of CBRN terrorism. There are well-substantiated arguments to bridge the distinct policy and academic perspectives.[92] But achieving this goal has numerous prerequisites. First, scientific and social science research should collaborate and combine their endeavors in a multidisciplinary way to strengthen one another and thereby improve our formal understanding of CBRN terrorism.[93] Second, there is a strong need for operationalizing the basic research approaches. There is an impressive volume of literature discussing the factors that substantially influence the decision-making of terrorists that can help determine whether they will resort to CBRN warfare. As Ackerman

[84] Merari, in Alex P. Schmid (Ed.), *The Routledge Handbook of Terrorism Research*, p. 468.
[85] M. J. Gohel, in Alex P. Schmid (Ed.), *The Routledge Handbook of Terrorism Research*, p. 468.
[86] Davies, in Alex P. Schmid (Ed.), *The Routledge Handbook of Terrorism Research*, p. 468.
[87] Alex P. Schmid, 'Statistics on Terrorism, The Challenge of Measuring Trends in Global Terrorism', *UNODA Forum on Crime and Society*, 2004, Volume 4, Issue 1, 2, p. 50.
[88] Alex P. Schmid and Albert Jongman, p.179.
[89] Robert O Slater and Michael Stohl, 'Introduction: Towards a Better Understanding of International Terrorism', *Current Perspectives on International Terrorism*, MacMillan, London, 1988, p. 3.
[90] Alex Schmid and Albert Jongman, p.177.
[91] Gary Ackerman, 'WMD Terrorism Research: Whereto from here?', *International Studies Review*, 2005:7, p. 140.
[92] Bruce Hoffman, *Change and Continuity in Terrorism*, in Bruce Hoffman and Anders Strindberg (Eds.), *Terrorism and Beyond: A 21st Century Perspective*, Routledge Library Editions, Terrorism and Insurgency, Routledge, London and New York, 2015, p. 113.
[93] Gary Ackerman, 2009. p. 19.

highlights, more work needs to be done to identify which factors can be valuable as early warning indicators for a future attack. While emphasizing that there is no way to predict the timing, nature, or location of future WMD attacks within any scientific certainty'[94], Ackerman points out that researchers should make efforts to transform their academic achievements into operational outcomes that can be used by professional staff who might not be engaged in the 'cumulative knowledge base on CBRN terrorism'[95].

One useful academic contribution would be to empirically validate the existing literature on the criminal motivations and capabilities for resorting to CBRN warfare (e.g. the works of Gurr[96], Stohl and Stohl[97], Post et al[98], Sinai[99], Ranstorp[100], Hayden[101]) and provide 'usable and useful analytical tools'[102] for the field. All the already available knowledge on the phenomenon should be reconceptualized to be useful for intelligence and law enforcement analysists[103] and thus become highly valuable for threat assessments[104]. Regardless of the fact that this information derives only from open-source materials, it could render a comprehensive qualitative analysis of certain groups' relevant characteristics. In doing so, qualitative, quantitative and empirical methodologies should strengthen and complement each other to facilitate the development of comprehensive perpetrator profiles. Furthermore,

---

[94] Gary Ackerman, *WMD Terrorism Research* in J. Horgan and K. Braddock (Eds.), *Terrorism Studies: A Reader*, New York: Routledge, 2011, p. 391.
[95] Gary Ackerman, 2009. p. 17.
[96] Ted Robert Gurr, *Which Minorities Might Use Weapons of Mass Destruction?* in T*he Forum: Nonstate Actors, Terrorism, and Weapons of Mass Destruction*, in *International Studies Review*, 2005:7, p. 143-146.
[97] Cynthia Stohl and Michael Stohl, *Approaching Global Organizing*, London: SAGE Publications, 2005.
[98] Jerrold Post, Ehud Sprinzak and Laurita Denny, 'Terrorists in Their Own Words: Interviews with Thirty-Five Incarcerated Middle Eastern Terrorists', *Terrorism and Political Violence*, 2003:15, p. 171-184.
[99] Joshua Sinai, 'Forecasting Terrorists' Likelihood to Embark on „Conventional" to CBRN Warfare', in The Forum: Nonstate Actors, Terrorism, and Weapons of Mass Destruction', in *International Studies Review*, 2005:7, p. 151-153.
[100] Magnus Ranstorp, 'Terrorism in the Name of Religion', *Journal of International Affairs*, 1996:1, p. 41-62.
[101] Nancy K. Hayden, *Terrifying landscapes Understanding motivations of non-state actors to acquire and/or use weapons of mass destruction*, in Magnus Ranstorp and Magnus Normark (Eds.), *Unconventional Weapons and International Terrorism, Challenges and new approaches*, UK and USA, Routledge, 2009. p. 163-194.
[102] Gary Ackerman, 'WMD Terrorism Research: Whereto from Here?' in The Forum: Nonstate Actors, Terrorism, and Weapons of Mass Destruction', *International Studies Review*, 2005:7, p. 140.
[103] Gary Ackerman, *WMD Terrorism Research* in J. Horgan and K. Braddock (Eds.), *Terrorism Studies: A Reader*, New York: Routledge, 2011, p. 390.
[104] Gary Ackerman, 2005, p. 142.

to be able to produce usable analytical knowledge for the law enforcement community, academics need to take into account the operating principles of the law enforcement realm.[105] Beyond this, Ackerman and Bale suggest taking a broader context for analyzing the terrorist potential for launching CBRN attacks and raise awareness of the operational cooperation between various terrorist groups and organizations. These combined endeavors may strengthen such terrorist capabilities that previously were unable to pursue attacks where unconventional weapons were involved.[106]

[105] Gary Ackerman, 2009. p. 16-17.
[106] Gary Ackerman, 2011, p. 392.

PART III

Chapter Three

3.1. Introduction to the Scenario Section

The third part of the thesis proceeds in three chapters. The first chapter introduces the phases of commission in terms of a CB attack. These phases provide the key units for the analysis. The rest of this introductory chapter outlines the principles first of the EU-level and second, the Australian counter-CB terrorism policies. Chapters Two and Three elaborate a chemical and a biological scenario respectively. Each of these scenarios takes a retrospective approach concerning the emergence of the attack and guides the reader along each perpetration phase that eventually lead to the incident. The goal of these analyses is to examine the crucial steps and challenges that criminals need to tackle when mounting a CBRN attack. At the same time, these discussions aim to test and validate the counter policies in order to pinpoint their gaps. The ultimate goal is to identify those vulnerabilities that can be eliminated or improved by academic research.

3.2. The phases of perpetration in a case of a CB attack

This research builds upon the concept that when compared to traditional criminal groups, terrorists are much less spontaneous and devote considerable efforts for planning. Accordingly, they commit 'ancillary and preparatory crimes'[1] prior to the planned terrorist attack. With this presumption in mind, one can distinguish four essential phases of criminal conduct that aims to use CBRN materials for malevolent purposes. First, violent non-state actors must know more about these weapons-usable materials; they need to learn about how to construct such apocalyptic weapons; and how to transport or disperse the developed devices in order to have the knowledge to engage in unconventional weapons. Accordingly, the first phase of perpetration is the *acquisition of knowledge on CB materials*. This knowledge

[1] Brent L. Smith, Kelly R. Damphousse and Paxton Roberts, *Pre-Incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct*, May 2006. pp. 2., available at: https://www.hsdl.org/?abstract&did=464263

acquisition can happen in various forms, for instance by reading relevant literature on the topic, approaching experts in the field or looking for employment opportunities at specialized facilities.

It is important to note, however, that the mere acquisition of highly valuable information might not be wholly sufficient for constructing viable CB devices. Having access to scientific information on weapons-usable materials does not necessarily mean that perpetrators are in possession of other dependent assets (such as certain background knowledge that is necessary to exploit scientific data, sociotechnical factors[2], etc.) that are essential to efficiently use this scientific data. Gaining access to explicit knowledge[3] also requires the so-called 'tacit knowledge'[4].

Once the individuals have obtained the necessary knowledge on CB material(s), they need to *acquire the material* for mounting an attack. If criminals already have the necessary knowledge together with the required materials and equipment, the next step is to construct the CB weapon. This is the *development phase*. After successfully developing the CB weapon, the last phase of the perpetration – *the execution* – starts when the successfully deployed CB device is deployed and ready to go off.

3.3. The counter-CB strategy of the European Union

The Islamic State used chemical weapons in Syria and Iraq, other incidents show their interest in developing biological or radiological weapons[5]. Similarly, terrorist propaganda

[2] Sonia Ben Ouagrham-Gormley, 'Barriers to Bioweapons: Intangible Obstacles to Proliferation', *International Security*, 2012, 36:4, p. 80-114.
[3] 'which is knowledge captured in writing', in: Horacio R. Trujillo and Brian A. Jackson, 'Identifying and Exploiting Group Learning Patterns for Counterterrorism', *Terrorism Informatics, Knowledge Management and Data Mining for Homeland Security*, 2008, p. 179.
[4] that refers to 'developing the expertise that is necessary to be able to use the explicit knowledge', in: Horacio R. Trujillo and Brian A. Jackson, 'Identifying and Exploiting Group Learning Patterns for Counterterrorism', *Terrorism Informatics, Knowledge Management and Data Mining for Homeland Security*, 2008, p. 179.
[5] Europol, Terrorism Situation and Trend report (TE-SAT), 2017, p. 14.

deals with the potential of CB attacks, and possible tactics and targets are circulated on these platforms.[6] While up to now no terrorists have used CB weapons on European soil, there are credible indicators that suggest there are violent non-state actors who may have the intention to resort to CB warfare having made efforts to develop the knowledge that is essential for engaging in unconventional weapons.[7] On the whole, the risk of CB terrorism is still a low – but 'evolving[8]' – threat with high possible impact. Accordingly, a widespread European Union policy aims to address the CB terrorism-related threat.

The EU CBRN counterstrategy is underpinned by a 'horizontal'[9] concept stating that the preparedness for a CBRN attack requires the collaboration between diverse areas and actors. The recent anti-CBRN measures aim to (i) reduce the accessibility of CBRN materials, (ii) ensure a more robust preparedness for and response to CBRN security incidents, (iii) build stronger internal-external links in CBRN security with key regional and international EU partners and (iv) enhance our knowledge of CBRN risks.[10] The European-level norms addressing the CBRN risk calls upon a closer cooperation between the Member States to 'learn from each other and pool expertise and assets'[11] in order to have a better preparedness for a future CBRN attack.

It needs to be emphasized, however, that Member States' national authorities are primarily responsible for protecting their citizens from possible CBRN terrorist attacks. National law enforcement, disaster management agencies and medical services tackle the challenges of prevention, preparedness and response to such devastating incidents. EU-level regulations are intended to provide cross-border crisis management mechanisms and tools to help the

[6] Europol, Terrorism Situation and Trend report (TE-SAT), 2017, p. 16.
[7] *Ibid.*
[8] COM (2017) 610 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, p. 2.
[9] *Ibid.*, p. 4.
[10] *Ibid.*, p. 3.
[11] *Ibid.*, p. 3.

Member States' counteractions. Community programmes and instruments provide funding opportunities for the implementation of the respective European Union policy. The need for an EU-level approach is justified, when considering the criminal trend that precursor materials are purchased in one Member State and then are transferred to another Member State where they are used in an attack.[12]

The *EU CBRN Action Plan* of 2009[13] suggests deploying a risk and cost-benefit based approach to CBRN security in the European Union. It aims to improve the information exchange between Member States and set the counter policy's three main pillars: prevention, detection and preparedness/response to a CBRN terrorist incident. Enhancing international cooperation with respect to the exchange of information and good practices[14] is one of the most prominent principles of the document. Consequently, the European Commission intends to establish a web portal for good-practices on CBRN security together with a database of applicable information for national authorities on the nature of high-risk CBRN materials and their handling.[15] The *Action Plan* sets the demand for improving the training of first responders.[16] Its overall objective – in line with the *EU Counter Terrorism Strategy* and the *Internal Security Strategy* – is to 'reduce the threat of, and damage from CBRN incidents of accidental, natural and intentional origin, including terrorist acts'[17]. The EU approach prefers a scenario-based, modelling plan of action.[18] This approach requires a sophisticated understanding of the existing criminal trends in the field. The European Union's ultimate

[12] COM (2014) 247 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a new EU approach to the detection and mitigation of CBRN-E risks, p. 4.
[13] COM (2009) 273 final, Communication from the Commission to the European Parliament and the Council – an EU CBRN Action Plan
[14] 15505/1/09 REV 1 – Council conclusions on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union – an EU CBRN Action Plan, 2009, p. 67.
[15] *Ibid.*, p. 70.
[16] *Ibid.*, p. 72.
[17] Progress Report on the Implementation of the EU CBRN Action Plan, May 2012 (public version), p.1.
[18] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 67.

goal in this regard is to 'develop practical and effective tools for practitioners'[19]. It is important to point out here, however, that the *Action Plan* is not a legal instrument. Consequently, it does not have either immediate legal or budgetary consequences.

As European Commission President Juncker recently stressed in terms of the European security: 'fragmentation is what makes us vulnerable'[20]. He sets the demand for a 'genuine Security Union[21]'. The recent European counterterrorism strategy lies upon four strategic pillars. First, stricter rules make it more difficult to legally acquire high capacity weapons and also restrict access to certain chemical substances. Similarly, by cutting off the sources of terrorist financing the European efforts aim to deny terrorists the means for their deceitful purposes.[22] Second, the European Commission places a strong focus on the significance of information sharing by raising awareness and providing practical solutions via the available interoperable European information channels.[23] The third pillar targets the online platforms of terrorist propaganda. These endeavors aim to ensure that 'illegal content is taken down as quickly as possible'[24]. The fourth pillar addresses the demand for better protecting the external EU borders.[25] This involves the systematic check of all travelers against European databases, the establishment of the new European Border and Coast Guard and the proposal for a new, modernized external border management system intended to be in operation by 2020.[26]

The *CBRN Action plan*[27], endorsed in October 2017, is an essential part of the EU anti-terrorism package aiming to improve the understanding of CBRN risks. With this goal in mind, resources and expertise are pooled together to: (i) regularly review and analyze CBRN risks

[19] COM (2014) 247 final, p. 4.
[20] European Commission President Jean-Claude Juncker, European Parliament, 12 April 2016
[21] *Ibid.*
[22] European Commission, Security Union, A Europe That Protects, October 2017, p. 2.
[23] *Ibid.*, p. 2-3.
[24] *Ibid.*, p. 3.
[25] *Ibid.*, p. 4.
[26] *Ibid.*, p. 4.
[27] COM (2017) 610 final

and threats; (ii) identify the existing policy gaps and elaborate how to cover these gaps; and (iii) to develop cooperation amongst all these entities.[28]

This terrorist-centred EU regulation is further complemented by the *European Union Strategy against the Proliferation of Weapons of Mass Destruction (WMD Strategy)*[29]. The EU strategy against the criminal use of weapons of mass destruction takes into account both state and non-state actors. It takes a 'societal security-based approach'[30] in terms of the regulation on CBRN threats and tries to mitigate the associated risk as well as prevent WMD proliferation. The main scope of the EU WMD Strategy is on chemical, biological and nuclear weapons as well as missile delivery systems[31]. However, this document acknowledges that if terrorists can acquire the appropriate materials, 'their means of delivery adds a new critical dimension to this threat'[32]. Consequently, 'non-proliferation, disarmament and arms control provide valuable contributions to the combat against terrorism, by mitigating the risk of non-state actors gaining access to weapons of mass destruction'[33]. The EU WMD Strategy stresses the necessity of taking an 'effective multilateralist approach[34]' in addressing the WMD threat. This principle is reflected in the emphasizing of the significance of the 'multilateral treaty system[35]', which sets the normative basis for the non-proliferation policies. As this strategy suggests, the international legal environment that ensures the efforts against the non-proliferation of WMD needs to be further enhanced by regional security regulations.[36]

The *EU CBRN Action Plan* of 2017 is also conceptualized upon a so-called horizontal approach, stressing that different areas and actors need to firmly collaborate to effectively

[28] COM (2017) 610 final, p. 13-14.
[29] 15708/03, The European Council, Fight against the proliferation of weapons of mass destruction, 2003.
[30] Ian Anthony and Lina Grip, *Strengthening the European Union's Future Approach to WMD Non-proliferation*, SIPRI Policy Paper No. 37, 2013, p. V.
[31] *Ibid.*, p. 27.
[32] 15708/03, The European Council, Fight against the proliferation of weapons of mass destruction, 2003, p. 2.
[33] *Ibid.*, p. 3.
[34] *Ibid.*, p. 5-8.
[35] *Ibid.*, p. 6.
[36] *Ibid.*, p. 7.

combat the threat of CBRN terrorism.[37] Duplications in information sharing practices, the differences in the national jurisdictions of the Member States, and different approaches to the control or monitoring the transport of hazardous CBRN substances are all EU-specific problems.[38] One of the problematic fields that needs further improvement is the need for 'cross-border and cross-sectoral trainings and exercises'[39], based upon a 'pre-agreed curricula'[40].

Another important program in the field is the CBRN Centre of Excellence (CoE) initiative established by the EU in 2010. To mitigate CBRN risks of criminal, this innovative approach aims to offer comprehensive regulatory, enforcement and technical cooperation in countries outside the European Union.[41]

3.4. The Australian counter-CBRN strategy

Recently disrupted terrorist plots in Australia – Melbourne (2016)[42] and Sydney (2017)[43] – remind Australians to 'be prepared for terrorist attacks across the spectrum of tactics and capabilities'[44]. The current threat environment shows the potential of lone actor attacks using everyday items as weapons. A mass-casualty chemical, biological, radiological or nuclear

[37] COM (2017) 610 final, p. 4.
[38] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 10-13.
[39] COM (2017) 610 final, p. 4.
[40] *Ibid.*
[41] See: http://www.cbrn-coe.eu/
[42] 'Melbourne terrorist plot: Four charged, one in custody over alleged Christmas Day attack plan', *ABC News*, 24, December 2016, available at: http://www.abc.net.au/news/2016-12-23/police-foil-alleged-christmas-day-terrorist-plot-in-melbourne/8143762
[43] Riley Stuart and Louis Hall, 'Sydney terror plotters 'tried to blow up Etihad plane, unleash poison gas attack', *ABC News*, 4 August 2017, available at: http://www.abc.net.au/news/2017-08-04/sydney-terror-raids-police-say-plane-bomb-plot-disrupted/877375
[44] ASIO Annual Report, p. 20.

attack is thought to 'remain beyond the reach of most groups'[45]. The *Australian CBRN National Strategy* is a classified document. However, other, counterterrorism-related national documents facilitate to depict the main pillars of the respective Australian counter strategy.

The *Australian Counter-terrorism Strategy*[46] sets the framework for the system of the Australian counter provisions. The *National Counter-terrorism Plan* supplements this legal document by outlining 'governance and jurisdictional arrangements and operational responsibilities for preventing, preparing, responding to and recovering from domestic terrorist attacks'[47]. The prevailing principle that pervades the Australian counter-terrorism response is the importance of the Australian community's resilience[48], ensured by social cohesion and effective public communication[49]. At the same time, the Strategy depends upon widespread partnerships throughout the stakeholders in government, society and private sector.[50] This concept is based upon five core elements, namely: (i) challenging violent extremist ideologies; (ii) preventing people from becoming terrorists; (iii) taking considerable efforts to shape the global environment; (iv) disrupting terrorist activity within Australia; and (v) having robust arrangements in place to respond to acts of terrorism.[51] The essential focus of the strategy lies on prevention.[52]

The Australian counter terrorism strategy relies on tight 'cooperative, coordinated and consultative relationships between Australian governments and agencies'[53]. These intergovernmental national counter-terrorism arrangements aim to enable 'nationally

[45] Australian Government Department of the Prime Minister and the Cabinet, Review of Australia's Counter-Terrorism Machinery, January 2015, p. 11.
[46] Council of Australian Governments, Australia's Counter-Terrorism Strategy, Strengthening Our Resilience, 2015.
[47] *Ibid.*
[48] *Ibid.*, p. VI.
[49] *Ibid.*, p. 5.
[50] *Ibid.*, p. VI.
[51] *Ibid.*, p. VI-VII.
[52] *Ibid.*, p. 9
[53] National Counter-terrorism Plan, 3rd Edition, 2012, p. 3.

consistent approaches to countering terrorism, with an emphasis on interoperability'[54]. International partnerships improve this close collaboration between Australia's national security partner agencies.[55] The Australian strategic approach to terrorism is essentially risk-based[56], having a strong intelligence-led[57] and multi-agency[58] framework, incorporating the so-called PPRR concept that implies the preparedness, prevention, response and recovery from a terrorist act[59]. The Australian counter-terrorism machinery not only addresses the disruption of terrorist activities but aims to impede the 'development of terrorist capability – particularly their tactical and operational security training both directly and online'[60]. However, one of the main criticisms of the Australian counter terrorism efforts is that it has mainly been 'reactive – agencies have responded to threats as they have emerged'[61], instead of the proactive approach necessary in order to successfully address the current dynamic threats.

The *National Counterterrorism Strategy* approaches prevention from two distinct perspectives. On one hand, it aims to prevent or divert people from becoming terrorists but – more importantly for the purpose of this research – it sets the goal for preventing terrorist attacks through intelligence-led disruption, specifically 'investigating the planning of, support for and facilitation of terrorist activity'[62]. The Australian counter-terrorism approach is predominantly based on intelligence-related activities. Intelligence is collected to facilitate risk and threat-assessments conducted by the National Threat Assessment Centre of ASIO

[54] Intergovernmental Agreement on Australia's National Counter-Terrorism Arrangements, 5 October 2017, 2.3. (b)
[55] ASIO Annual Report, 2016-2017, p. 6.
[56] New South Wales Counter Terrorism Plan, December 2016, p. 10.
[57] National Counter-terrorism Plan, 3rd Edition, 2012, p. 8.
[58] New South Wales Counter Terrorism Plan, December 2016, p. 7.
[59] National Counter-terrorism Plan, 3rd Edition, 2012, p. 3.
[60] Review of Australia's Counter-Terrorism Machinery, January 2015, p. 2.
[61] *Ibid.*, p. 18.
[62] Australia New-Zealand Counter-Terrorism Committee, National Counter Terrorism Plan, 4th Edition, 2017, p. 14.

on the 'likelihood and probable nature of terrorism'[63], providing the baseline for operational and policy countermeasures.[64] To 'enhance the full spectrum of national security capabilities'[65] and 'allow the national security community to make smarter use of information'[66] the Australian Government sets the objective for national security sciences and innovation 'to develop better approaches to inform decision making'[67]. These innovations in forecasting, modelling, risk assessment techniques and tools 'help understand the likelihood and consequences of the threat we face'[68] as well as 'risk-informed approaches, effective resource allocations and planned responses'[69] .

[63] Australia New-Zealand Counter-Terrorism Committee, National Counter Terrorism Plan, 4th Edition, 2017, p. 14.
[64] *Ibid.*, p. 14.
[65] Australian Government, The National Security Science and Innovation Strategy, 2009, p. 10.
[66] *Ibid.*
[67] *Ibid.*, p. 11.
[68] *Ibid.*
[69] *Ibid.*

Chapter Four

Chemical Scenario

An individual arrives at the entrance of the underground station carrying the malevolent device in a large suitcase. When entering the underground, chlorine is disseminated on the travelling public.

4.1. Acquisition of knowledge on chlorine, its availability and potential use

European-level counter measures

As Gerstein forcefully argues 'Information will kill us in the techno-terrorist age.'[1] The Council of the European Union further asserts that 'in the field of CBRN threat we have to start our preparation before terrorists acquire know-how or capacities to target our infrastructures'[2]. This knowledge acquisition phase occurs in various forms. Accordingly, the following discussion aims to first, map the potential ways a non-state actor can acquire this crucial information, and second, intends to elucidate the respective measures or provisions that seek to counter intentions.

Non-state actors often access, share or receive relevant content online. As the countering efforts mainly fall under the national intelligence realm, publicly available EU-level strategic policy provisions only partly address such situations. One of the few strategic goals that explicitly concern such interactions is the European Commission's recommendation to encourage the Member States to adopt 'effective, proportionate and dissuasive domestic penalties[3]' for the unlawful and intentional criminal purposes engaging in activities of

[1] Gerstein, *Bioterror in the 21st Century: Emerging Threats in a New Global Environment*, Annapolis, MD: Naval Institute Press, 2009, p. 205.
[2] 15894/1/10, 29 November 2010, Council of the European Union, 'EU Counterterrorism Strategy – Discussion Paper', p. 6.
[3] COM (2017) 606 final, ANNEX 1 to the Proposal for a Council Decision on the conclusion, on behalf of the European Union, of the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), Article 11 (1)

'training for terrorism'[4]. As the definition states, these activities encompass all acts that aim to intentionally provide instructions on 'noxious or hazardous substances or other weapons'[5] for the purpose of 'contributing to the commission of a terrorist offence'[6]. At the same time, not only those individuals that offer this kind of training, but also those who receive such training, should be subject to penalties.[7]

Another notable provision in the Article 21 of the *EU Terrorism Directive*[8], that calls on the Member States to take the necessary measures and ensure the prompt removal of online content which incites terrorist acts.[9] However, when referring to this online terrorist material, the respective EU policy[10] interprets it as terrorist propaganda, and covers only 'incitement to terrorism, xenophobic and racist speech'[11] and not explicitly infers to the content that aims to assist in constructing a malicious chemical device.

The *EU Internal Referral Unit's (EU IRU)* – together with some national *IRU*s[12] – offers a considerable contribution in this regard. Operating at Europol, its mission is to scan the web for online terrorist material. It has the expertise to determine whether an online content 'constitutes terrorist or extremist online content'[13]. *EU IRU* can flag a content of concern and request its removal. Besides this primary objective, it endeavors to 'better understand the tactics and modi operandi of online propagandists and thus ultimately improve the

[4] COM (2017) 606 final, Article 7
[5] *Ibid.*, Article 7 (1)
[6] *Ibid.*
[7] COM (2017) 607 final, ANNEX 1 to the Proposal for a Council Decision on the conclusion, on behalf of the European Union, of the Additional Protocol supplementing the Council of Europe Convention on the Prevention of Terrorism (CETS No. 217), Article 3.
[8] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017
[9] COM (2017) 555 final, Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Tackling Illegal Content Online, Towards an enhanced responsibility on online platforms, p. 3.
[10] Note: Tackling Illegal Content Online in COM (2017) 555 final
[11] COM (2017) 555 final, p. 2.
[12] *Ibid.*, p. 8.
[13] *Ibid.*

disruption mechanisms'[14]. By the same token, *'Check the web' (CTW)* portal operated by Europol may provide key information on terrorist trends. As the policy recommendations in terms of the future phases of the *CTW program* suggest[15], expert support could certainly enhance law enforcement capacities and thus improve the law enforcement expertise to counter the use of Internet for terrorist purposes.

Interactions when the non-state actor intends to obtain this essential information from a book or a magazine and therefore attends in person in a bookstore, subscribes to a topic-specific scientific journal or − to overcome the technical difficulties of developing the malevolent chemical device − approaches individuals, who have widespread expertise and/or experience in working with chemicals. Or, as the 2017 Sydney Plane Plot presented, the bomb-making kit may arrive by mail to the untrained plotters.[16] In this respect, the *EU CBRN Action Plan* of 2009 sets out to improve the identification and reporting of alarming transactions and behavior[17]. When referring to suspicious transactions, however, the document does not define whether these behaviors are related to the acquisition of knowledge on CBRN materials, or rather, are about reporting the loss or other suspicious transactions with regard to the material. In the same vein, Action H.10. of this plan[18] establishes that the European Commission, together with the Member States, should set guidelines for the industry, the medical sector and the research community in order to establish how to identify the forms of suspicious behavior – but again only with regard to transactions.

Australian counter provisions

[14] EU Internal Referral Unit Year One Report, 2017
[15] 12653/10 ADD 1 – Commission Staff Working Paper – Taking Stock of EU Counter-Terrorism Measures, Accompanying document to the Communication from the Commission to the European Parliament and the Council, The EU Counter-Terrorism Policy: main achievements and future challenges, 2010, p. 5-6.
[16] Andrew Zammit, 'New Developments in the Islamic State's External Operations: The 2017 Sydney Plane Plot', *CTC Sentinel*,10:9, October 2017, p. 13.
[17] 15505/1/09 REV 1 – Council conclusions on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union – an EU CBRN Action Plan, 2009, p. 30.
[18] *Ibid.*

The Australian provisions on preventing a terrorist attack rely upon a risk-based approach, encapsulating capabilities such as: 'detection and disruption of terrorism planning and preparations through intelligence and law enforcement at the earliest possible stage'[19]; and 'cooperative partnerships with Australian and international government intelligence and law enforcement networks'[20]. Such investigative capabilities aim to generate intelligence relevant to the prevention of terrorism and to collect evidence that may support prosecutions for terrorism and related criminal offences[21]. National law enforcement and intelligence agencies form their counteractions upon a certain threat and risk assessment model that assesses the intent and capability of potential terrorist actors.[22]

The efforts aiming to detect and undermine terrorist activities by 'impeding the development of terrorist capability (particularly their tactical and operational security training both directly and online)'[23] further justifies the significance of addressing the planning phase of a terrorist attack. This strategy implies first, that changes in the threat environment need to be identified, and second, that shifts in terrorist methodologies need to be detected by the authorities.[24] The power of social media, in the Australian context, is regarded as a priority issue. Consequently, it is argued that it is necessary to limit 'the spread and influence of violent extremist ideas'[25] to constrain propaganda and expose the false claims that contradict the society's values and foster the valued ideas. The targeted part of exploiting these platforms, however, is related to terrorist propaganda and messages, building community resilience to violent extremism[26] and only partly concerns the transfer of information on CBRN know-how. Although having the ability 'to engage with previously difficult-to-access

[19] New South Wales Counter Terrorism Plan, December 2016, p. 10.
[20] *Ibid.*
[21] *Ibid.*
[22] *Ibid.*, p. 10-11.
[23] Australian Government Department of the Prime Minister and the Cabinet, Review of Australia's Counter-Terrorism Machinery, January 2015, p. 2.
[24] *Ibid.*, p. 15.
[25] Council of Australian Governments, Australia's Counter-Terrorism Strategy, Strengthening Our Resilience, 2015, p. vi.
[26] In accordance with the national Countering Violent Extremism Program, more information available at: https://www.livingsafetogether.gov.au

communities'[27] and thereby 'enabling quick and effective information flows'[28] is an indisputable benefit with regard to countering violent extremism.

The Australian counter strategy draws the attention to the significant challenge of modern communication technologies associated with advances in online security and encryption, which make the access to terrorist communication very difficult.[29] This is further exaggerated in the post-Snowden era, wherein terrorist groups have a better insight into the technological capabilities of national authorities.

Particular attention is given to detecting and undermining terrorist activities by 'blocking the flow of support (finances, goods and people) to or from terrorists and their networks'[30]. Reports relating to suspicious transactions can offer reasonable indicators of increased terrorist financing activities[31] and indirectly provide valuable information on attempts acquiring weapons-usable materials, however they may not reflect malicious intentions that aim to know more about CBRN materials.

Conclusions

Both the EU-level and the Australian counter policy have articulated that the CB terrorism-related risk assessment procedure should take a proactive – rather than the previous reactive – approach.[32] There is a clear need to be better at anticipating the threat of weapons-usable materials becoming available to criminals. Policies combating weapons of mass destruction

[27] Australian Government Department of the Prime Minister and the Cabinet, Review of Australia's Counter-Terrorism Machinery, January 2015, p. 17.
[28] *Ibid.*
[29] *Ibid.*, p. 12.
[30] *Ibid.*, p. 2.
[31] *Ibid.*, p. 18.
[32] COM (2014) 247 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a new EU approach to the detection and mitigation of CBRN-E risks, pp. 5.; 17172/08 Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 2008, pp. 9. and Review of Australia's Counter-Terrorism Machinery, January, 2015, p. 18.

can only be effective if there are distinguished and focused strategies that are 'aimed at specific adversaries'[33] who intend to resort to WMD warfare. As the *NATO Science for Peace and Security (SPS) Program* stresses, future research efforts need to address topics such as 'understanding the actor behind the CBRNE attack [whilst also] constantly endeavor to produce outcome that is the best for use by end-users [and] practitioners in the field'[34]. Academic studies on criminal profiles that are involved in the illegal procedures with regard to WMD-usable materials or technologies[35] could offer highly valuable contributions to these efforts.

Arguably, counterstrategies are predominantly based on 'terrorists' technological capabilities'[36] and give insufficient weight to psychological motivations. Available technical intelligence on terrorist or extremist capabilities should be contrasted with the 'formidable inhibitors'[37] and facilitators of the criminal entity. The terrorist or extremist groups' ideology, their demographics and security environment, the perpetrators' historical experience, perceptual biases and risk thresholds[38] are all predispositional elements when attempting to understand the 'potential non-state actors by identifying salient characteristics of past CB adversaries'[39]. As Forest suggests, theories of practical – technical and environmental – as

---

[33] Albert J. Mauroni, *A Counter-WMD Strategy for the Future*, in James J. Forest and Russell D. Howard (Eds.), *Weapons of Mass Destruction and Terrorism Second Edition*, New York: McGraw-Hill, 2012, p. 456.

[34] https://www.nato.int/nato_static_fl2014/assets/pdf/2013_10_pdf/20131125_19_Side_Panel_CBRN_WS_Farshad_2.pdf

[35] 17172/08 Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 2008, p. 9-10.

[36] Jerrold M. Post, *Prospects for Nuclear Terrorism: Psychological Motivations and Constraints* in Paul Leventhal and Yonah Alexander (Eds), *Preventing Nuclear Terrorism*, Lexington, MA: D. C. Heath, 1987, p. 91.

[37] Alex P. Schmid, 'Terrorism and the use of weapons of mass destruction: From where the risk?', *Terrorism and Political Violence*, 1993, 11:4, p. 106-132.; Gary A. Ackerman and Kevin S. Moran, *Bioterrorism and Threat Assessment, Prepared for the Weapons of Mass Destruction Commission*, 2006.

[38] Gary A. Ackerman, *More Bang for the Buck: Examining the Determinants of Terrorist Adoption of New Weapons Technologies,* London, UK: King's College, 2014, p. 27, available at: https://kclpure.kcl.ac.uk/portal/en/theses/more-bang-for-the-buckexamining-the-determinants-of-terrorist-adoption-of-new-weaponstechnologies(992afd2a-bdeb-46b2-8cb7-cd29d77ebd64).html

[39] Gary A. Ackerman, Jeffrey M. Bale, Victor Asal, R. Karl Rethemeyer, Amanda Murdie, Mila Johns, and Markus K. Binder, *Anatomizing Chemical and Biological Non-State Adversaries: Identifying the Adversary*, College Park, MD.: National Consortium for the Study of Terrorism and Responses to Terrorism, 2014, p. 1.

well as strategic constraint theories, should be applied on a 'case-by-case analysis of each terrorist group'[40]. Applying these perspectives could offer deeper insights into the prevailing factors of non-state actors' decision-making processes. Furthermore, they could inform considerations as to whether violent non-state actors would really engage in CBRN weapons if the acquisition of these weapon-usable materials became easier. EU INTCEN maps the criminal trends and evaluates the associated risks and threats.[41] These reports could be enhanced by academic studies on criminal profiles that are involved in the illegal procedures with regard to WMD-usable materials or technologies.[42] These new dimensions could offer valuable insights in relation to detecting the motivation for engaging in CBRN warfare.[43]

It should also be elucidated by the law enforcement and intelligence community as to the ways in which these motivational incentives interact with each other and thereby influence the decision-making of terrorist or extremist groups[44]. Understanding the internal dynamics of the armament and the elements that will shape the decision making of terrorist entities who intend to resort to CBRN weapons, would allow a broader understanding of the available intelligence on terrorist or extremist groups.[45] Organizing the most important factors related to the intent and interest to engage in CBRN weapons into a conceptual – preferably a computerized – model[46], would help analysts interpret the available information

[40] James JF Forest, 'Framework for Analyzing the Future Threat of WMD Terrorism', *Journal of Strategic Security*, 2012:4, p. 60.
[41] 17172/08 Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 2008, p. 9.
[42] *Ibid.*, p. 9-10.
[43] Note: e.g. National Consortium for the Study of Terrorism and Responses to Terrorism (START) project on Profiling the CB Adversary: Motivation, Psychology and Decision, 2017.
[44] Victor H. Asal, Gary. A. Ackerman, R. Karl Rethemeyer, 'Connections Can be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Weapons', *Studies in Conflict and Terrorism*, 2012, 35:3, p. 229-254.
[45] Jean Pascal Zanders, *Internal Dynamics of a Terrorist Entity Acquiring Biological and Chemical Weapons* in *Nuclear Terrorism: Countering the Threat.* Abingdon-on-Thames: Routledge, 2016, p. 26-55.
[46] Note: The model of terrorist weapon adoption by analyzing 'observable and inferable attributes' would make the work of analysists considerably easier. Moving beyond analyzing a complexity of influencing factors while focusing only on one certain terrorist or extremist entity, monitoring certain variables of great concern (such as new trends in the proliferation of CBRN materials or knowledge, novel terrorist ideologies or strategies, as well as novelties in organized crime, etc.) results in a more accurate risk assessment. Gary A. Ackerman, 2014, p. 102-103.

in a more systematic manner.[47] Specifically, the phenomenon should be examined from a 'multi- and interdisciplinary approach'[48]. Applying valuable academic research on the fuller understanding of the 'synthesis'[49] of all these factors, as well as investigating the internal dynamics of the group, would ensure a more precise forecast of the respective threat[50]. Likewise, tracking the impact of technological change in criminal modi operandi[51] or considering the rhetoric indicators[52] of such potential future incidents could measure the terrorist entity's engagement in WMD warfare. Such academic contributions would be valuable even for those efforts that aim to improve early warning mechanisms with regard to cross border threats[53].

There is only limited awareness among life scientists on the potential for the malicious misuse of their innovations. Scientists need to engage in biosecurity-related issues and their ethical, legal and social responsibilities.[54] 'New emerging technologies must remain secure and peaceful.'[55] Accordingly, university curricula are required to provide compulsory courses on responsible conduct of science.[56] More specifically, establishing trustful

---

[47] Mary D. Zalesny, Paul Whitney, Amanda White, Theodore R. Plasse, and Michael T. Grundy, 'A Conceptual Model to Identify Intent to Use Chemical-Biological Weapons', *Journal of Strategic Security* 10, no. 3, 2017, p. 54-86.

[48] Jean Pascal Zanders, 2016, p. 26-55.

[49] Gary A. Ackerman, 2014, p. 100.

[50] B. Cole, *The Changing Face of Terrorism: How Real is the Threat from Biological, Chemical and Nuclear Weapons?*, New York: I. B. Tauris, 2011, Jean Pascal Zanders, *Internal Dynamics of a Terrorist Entity Acquiring Biological and Chemical Weapons* in *Nuclear Terrorism: Countering the Threat.* Abingdon-on-Thames: Routledge, p. 26-55., Brecht Volders, *Assessing the likelihood of nuclear terrorism*, in Brecht Volders and Tom Sauer (Eds.) *Nuclear Terrorism: Countering the Threat.* Abingdon-on-Thames: Routledge, 2016, p. 12-26.

[51] Gary Ackerman, 2011, p. 391.

[52] Jeffrey M. Bale, 2018, p. 131-136.

[53] COM (2017) 610 final, p. 8-9.
Note: The European Early Warning and Response System (EWRS) – a confidential computer system, via which Member States could generate and send alerts of grave concern[53] – could be further enriched by the cumulative base of the features of contemporary terrorist entities or criminal trends.

[54] Koos van der Bruggen, *Biosecurity challenges in the 21st century: the case of gain-of-function experiments* in Simon Whitby, Tatyana Novossiolova, Gerald Walther and Malcolm Dando (Eds.), *Preventing Biological Threats: What You Can Do*, Bradford: Bradford Disarmament Research Centre, 2015, p. 42-43.

[55] Adriaan Van Der Meer, *Promoting a Scientist's Duty of Care 4.0.*, May, 2018.

[56] Lida A. Anestidou and Jay B. Labov, *Immersing students in responsible science through active learning pedagogies: lessons from education institutes in the MENA region* in Simon Whitby, Tatyana Novossiolova, Gerald Walther and

relationships between the security and scientific community could ensure the practice of an elevated level security culture around bio-use technologies. [57]

Having a strong emphasis on detection and response, there are multiple technological innovations in place to help first responders in managing a CBRN plot.[58] Incorporating cumulative knowledge on terrorist or criminal entities, and the rigorous analysis by academics on their capabilities and/or motivations could certainly provide precious information to practitioners who are responsible for the reconstruction of the criminal behaviour, and ultimately identify the responsible criminal actors in case of a deliberate criminal use of CBRN materials.

As the European Commission asserts, 'there exists a concern that not all CBRN transactions of terrorist or criminal nature are addressed, given that the existing mechanisms either focus on special specific types of materials or on certain instances of theft or loss only'[59]. Academic research that elaborates early warning signs and possible triggers for malicious acquisition of knowledge could help the intelligence community's efforts to unify the pieces of information, form their intelligence footprint, and finally, interdict the criminal activity.[60] At the same time, it would certainly support the EU intention to 'steer the development of a common criteria'[61] that ensures 'a more harmonized approach to what constitutes suspicious

Malcolm Dando (Eds.), *Preventing Biological Threats: What You Can Do*, Bradford: Bradford Disarmament Research Centre, 2015, p. 388-404.

[57] Koos van der Bruggen, 2015, p. 42-43.

[58] Note: For instance, the so-called CBRN Toolbox of Toolboxes (available at: http://www.preventionweb.net/files/45270_228.pdf) – developed by the EDEN Consortium funded by the European Community's Seventh Framework Programme (FP7/2012-2016) – provides useful tools for CBRN practitioners to successfully address the preparation, crisis response and recovery phases of a CBRN incident.

[59] European Commission Call for Tender No. HOME/2010/ISEC/PR/038-A1, p. 58.

[60] Combating Illicit Trafficking in Nuclear and other Radioactive Material, Technical Guidance, Reference Manual, IAEA Nuclear Security Series No. 6, 2007, p. 90.

[61] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 57.

behavior and transactions'[62]. The intelligence and law enforcement community may not have the capacity to see these suspicious behaviors in a broader context. Academic considerations on the possible ways of approaching a scientist or a stockpile of weapons-usable material, by contacting scientists and elaborating the reporting mechanisms in place, as well as drawing on past incidents and lessons from these previous failures, could offer a widespread trend analyses for practitioners who might only be considering current criminal trends based upon recent technical intelligence.[63] Research on criminal practices in terms of acquiring knowledge on weapons-usable material would contribute to those innovative means that aim to identify early signals of a terrorist attack[64].

Once in the possession of the necessary knowledge on the chosen chemical agent, the following sections consider the preparatory activities that aim to acquire chlorine, together with other specialized equipment necessary for the construction of the malicious device and personal protective equipment to ensure the safety of the development process.

4.2. Acquisition of chlorine, personal protective equipment and other equipment necessary for the construction of the malevolent device

Chlorine can be obtained essentially from two sources. First, high-purity chlorine is used in numerous industrial practices, therefore chemical facilities of a wide range store the chemical agent. On one hand, it is highly beneficial for non-state actors to get access to chlorine of a high concentrate as they can skip the purifying part of the development process since having immediately a weapon-usable material. On the other hand, taken into account the heightened

[62] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 57.

[63] Note: The demand for such studies is justified when considering, for example, the EU call – HOME/2010/ISEC/PR 038-A1 Lot No. 8 – for a stocktaking study on good practices in terms of reporting suspicious transactions in relation to CBRN materials.

[64] Friedrich Steinhäusler, *Gap Analysis of EU Counterterrorism Research Initiatives* in Erice International Seminars on Planetary Emergencies, 45th Session: The Role of Science in the Third Millenium, 2012, p. 30.

level of safety around these chemical facilities, perpetrators need to expose themselves to be detected by the law enforcement agencies. In addition, the digital age facilitated the development of black markets with encrypted messages and virtual payments. The use of darknets and cryptocurrencies offers secure and less traceable trading venues to procure illicit hazardous materials.[65] Considerable law enforcement effort aim to better understand this virtual environment and subsequently design effective actions to intervene criminal activities in these media.

And second, chlorine is publicly available in a diluted form in legitimate trading sources, selling for instance pooling chemicals. While the safety of such dual-use hazardous materials is less comprehensive, acquiring them in bulk without legitimate grounds requires careful and circumspect planning.

These conditions apply, when the non-state actor attempts to purchase specific equipment for the storage of chlorine or for the development of the malicious device, as well as acquiring the personal protective equipment to enhance the safety of the experimental trials. All these assistive devices and equipment can be obtained from facilities working with chlorine but also from ordinary trading channels, selling them for legitimate users.

4.2.1. Acquiring high-purity chlorine from a chemical facility or a research institute

The non-state actor may seek employment at chemical facilities that have direct access to high-purity chlorine and to specialized equipment necessary for the construction of the device. The same considerations apply, if the perpetrator intends to acquire personal protective equipment to ensure his or her safety while developing the chemical device. If non-state actors are unable to obtain the material themselves, they may coerce an employee working at a chemical facility, or a researcher of an institute that uses high-purity chlorine

[65] Press release, "A primer on DarkNet marketplaces," Federal Bureau of Investigation, November 1, 2016.

for its experiments to steal the chemical agent. The following section attempts to evaluate the provisions of counterstrategies that aim to prevent or thwart these malicious interactions.

European-level countermeasures

In Europe, the security of high-risk substances – including chlorine – is regulated in three EU lists with respect to weapon-usable materials in the chemical, biological and radiological-nuclear strands. A widespread forum of private and public experts was involved in the development process that was based upon a robust and rigorous risk-assessment.[66] The program aimed to enhance the security of high risk CBRN materials by establishing EU-wide security standards.[67] Accordingly, the European Commission (hereinafter EC) has advised to put in place security management systems and good practices to ensure a graduated level of security in these high-risk chemical facilities.[68] In keeping with this increased security culture[69], the EC has set the demand for establishing responsible behaviors regarding persons who work with, have access, handle or provide the security of these hazardous materials.[70] The EC has suggested building trusted relationships between security managers and law enforcement counterparts and has exhorted industry to replace the use of high-risk chemicals as well as reduce their transport.[71] Common criteria for background checks and vetting requirements of personnel having access to CBRN materials of concern would ensure a consistent and graduated policy.[72] Similarly, the EC has suggested identifying good practices concerning the security of high-risk chemical facilities and developing a 'good practice

[66] 15505/1/09 REV 1 – Council conclusions on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union – an EU CBRN Action Plan, 2009, p. 13.
[67] *Ibid.*, p. 15.
[68] *Ibid.*, p. 17.
[69] *Ibid.*, p. 28.
[70] *Ibid.*, p. 27.
[71] *Ibid.*, p. 20.
[72] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 33-35.

document'[73] of these effective security measures. Unfortunately, other EU suggestions encouraging the chemical industry to replace high-risk chemical substances with other suitable alternates of lower risk could not yet achieve their goals.[74]

In case of a theft or loss of high-risk CBRN material, both the horizontal and the vertical flow of information requires improvement.[75] Consequently, in relation to CBRN incidents and CBRN-related threats or suspicions, an early warning system at two levels should be established.[76] The concept could be similar to the functioning ECURIE (European Community Urgent Radiological Information Exchange) system, which facilitates early notifications and exchange of information in the case of a radiological or nuclear emergency.[77]

Australian counter provisions

Chlorine is one of the 96 chemicals of concern, that are included in the list compiled by the Council of Australian Governments (COAG) and accordingly its handling is regulated in accordance with a priority risk assessment.[78] States, Territories and the Commonwealth share a joint responsibility and set the regulation of these hazardous materials.[79] The risk assessments are conducted by government experts having widespread experience in both chemical regulation and security-related aspects, but jurisdictional police are also engaged at the earliest possible stage of the assessment process.[80] The outcome of this risk assessment sets the *National Chemical Management Framework* which outlines the security-related regulation on the storage, sale and handling of hazardous materials.[81] There is a close

[73] 15505/1/09 REV 1, 2009, p. 21.
[74] European Parliament Briefing on CBRN Terrorism: threats and the EU response, January 2015, p. 7.
[75] COM (2017) 610 final, p. 2.
[76] COM (2017) 610 final, p. 2.
[77] available at: https://rem.jrc.ec.europa.eu/RemWeb/activities/Ecurie.aspx
[78] An Australian Government Initiative, Chemicals of Security Concern, p. 1.
[79] National Counter-Terrorism Plan, 2012, Point. 77.
[80] An Agreement on Australia's National Arrangement of Security Risks Associated with Chemicals, 2 October 2008, p. 14.
[81] National Counter-Terrorism Plan, 2012, Point. 79.

collaboration between governments and industry when developing these control and capability countermeasures.[82] In accordance with these frameworks, states and territories provide the consistent standards for the use, transport, reuse or ultimate disposal of the chemical. New South Wales CBRN-terrorism counter arrangements deploy security strategies that aim to manage the 'illegal or unauthorized use of CBRN agents'[83]. They do so by means of control measures such as 'educating, training and awareness raising, licensing, tracking of chemical, reporting of unaccounted losses, security of premises, [and] vetting of people with access to specified materials and point of sale identification systems'[84]. Local governments are responsible for the implementation of state and territory regulations and take care of aspects such as waste disposal.

Raising community and industry awareness on risks posed by chemicals of security concern is another valuable component of this framework.[85] These regulations endeavor to achieve a four-fold security outcome: 'an informed and vigilant community and industry'[86] that understands the security risk associated with chemicals and is able to assist law enforcement and security agencies to prevent, deter or detect the malicious use of these chemicals. Moreover, this framework intends to achieve informed government agencies that 'act in partnership with the community and industry to manage the security risks from the use of chemicals for terrorist purposes'[87] together with 'appropriate security around priority chemicals of security concern'[88]. More specifically, control measures should be proportionate to the assessed risk; should be nationally coordinated and nationally consistent; should be built on existing industry and/or government arrangements; should be cost effective; and developed in partnership between government and industry.[89]

---

[82] An Agreement on Australia's National Arrangement of Security Risks Associated with Chemicals, p. 14.
[83] New South Wales Counter Terrorism Plan, December, 2016, p. 15.
[84] New South Wales Counter Terrorism Plan, p. 15.
[85] National Counter-Terrorism Plan, 2012, Point. 79.
[86] An Agreement on Australia's National Arrangements for Management of Security Risks Associated with Chemicals, 2 October 2008, p. 11.
[87] *Ibid.*
[88] *Ibid.*
[89] *Ibid.,* p. 12.

There are various forms of self-regulation across all chemical sectors and all phases of industry's supply chain.[90] To help prevent chemicals of concern falling into the wrong hands, Australian governments in partnership with industry have developed a voluntary *National Code of Practice for Chemicals of Security Concern*. This document encourages industry to put in place 'good security planning'[91] practices and integrate the measures into their existing business practices and thereby promote effective chemical security management throughout the chemical supply chain.[92] The Code sets out a series of recommended security measures concerning how to reduce the identified security risks in an effective manner.[93] The document dwells on a number of provisions: employee and contractor checking; personnel security awareness; inventory control measures; the receipt of chemicals; the risk of stolen or diverted chemicals, and also considers how to improve physical and personnel access.

Another key stakeholder in this regard is the Australia Group, constituting an informal forum of countries, 'which through the harmonization of export controls, seeks to ensure that exports do not contribute to developing chemical or biological weapons'[94]. The effectiveness of the group lies upon a 'shared commitment by the participants to chemical and biological weapon non-proliferation goals', who do not undertake legally binding obligations'[95]. This informal arrangement's control lists and guidelines for its participants aim to 'be practical and reasonably easy to implement'[96], and to 'be effective in impeding the production of CB

[90] Attorney General's Department, Decision Regulation Impact Statement, Chemical Security: Toxic Chemicals of Security Concern, November 2014, p. 28.
[91] Australian Government, National Code of Practice for Chemicals of Security Concern, 2016. p. 2.
[92] Australian Government, National Code of Practice for Chemicals of Security Concern, p. 5.
[93] *Ibid.,* p. 9-12.
[94] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 13, International Conventions and Agreements, 2014, p. 3.
[95] *Ibid.*
[96] Australia Group, Common Control List Handbook, Volume II: Biological Weapons-Related Common Control Lists, Revision 3, February 2017, p. ix.

weapons'[97]. They should not impede the normal trade of materials and equipment used for legitimate purposes.[98]

To demonstrate their compliance with the *Chemical Weapons Convention (CWC)*, Australia has destroyed its chemical weapons stockpiles; has undertaken to declare information on certain chemical activities to the Organization for the Prohibition of Chemical Weapons (OPCW); and now allows OPCW to inspect relevant chemical facilities.[99] By using the categories of Scheduled chemicals – above specified thresholds – facilities must have permits for conducting certain activities with these materials. Undertaking such actions without a requisite permit constitutes a criminal offence. The use of toxic chemicals, however – being outside the CWC verification framework – are insufficiently regulated by Australian legislation, thereby undermining the effectiveness of controls on chemicals of security concern.[100]

4.2.2. Obtaining chlorine of high-concentrate while being in transit

High-purity chlorine is used in numerous industrial practices. This requires the daily transportation of the material and provides excellent opportunities for criminals to steal it while being in transit.

European-level counter measures

[97] *Ibid.*

[98] *Ibid.*

[99] The Chemical Weapons Convention, A Guide for Australian Industry Producing, Using or Trading Chemicals, 2014, p. 2, available at: https://dfat.gov.au/international-relations/security/non-proliferation-disarmament-arms-control/chemical-weapons/cwc/Documents/Chemical_Weapons_A%20Guide.pdf

[100] Faiza Patel King, 'Implementing the Chemical Weapons Convention: A comparative case study of the legislation of Australia and France', in Ramesh Chandra Thakur and Ere Haru (Eds.), 'The Chemical Weapons Convention: Implementation, Challenges and Opportunities', Tokyo: United Nations University Press, 2006, p. 108-109.

Grave concerns exist with respect to the European control of CBRN markets. Member States have different standards in terms of the surveillance and monitoring of CBRN materials and related transactions.[101] There are states where licensing requirements do not meet the European standards, and likewise, there are different procedures in place for tracking weapons-usable materials.[102] Because electronic tracking systems for the cross-border transport of high-risk materials have not been introduced, tracking procedures and the reporting of suspicious transactions vary per Member States. The communication between the security personnel and the law enforcement community is still far from effective. Furthermore, there are national users of CBRN materials who do not have a sufficient level of security awareness. Therefore, the control of CBRN markets needs better coordination.[103]

In case of export of dual-use materials, the European Commission aims to produce good practice guides for control procedures.[104] Such efforts endeavor to 'improve the free movement of chemical substances and mixtures within the internal market without distortions of competition'[105], but at the same 'ensure a high level of protection of the safety of the general public'[106]. Chlorine, as a chemical precursor for more sophisticated weapons is also regulated by the *Chemical Weapons Convention (CWC)*. The focus of *CWC*'s legislation is, however, on large-scale uses of these hazardous materials. It does not address transactions that aim to acquire smaller amounts of these substances that, however, may be enough for a successful CBRN attack.[107]

---

[101] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strenghtening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 11-12.
[102] *Ibid.*, p. 12.
[103] SEC (2009) 791, p. 11-12.
[104] 17172/08 Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 2008, p. 14.
[105] C (2017) 6950 final Commission Recommendation of 18.10.2017 on immediate steps to prevent misuse of explosive precursors, p. 2 (4)
[106] *Ibid.*
[107] Jeffrey M. Bale and Gary A. Ackerman, 'Profiling the WMD Terrorist Threat', in Stephen M. Maurer, 'WMD Terrorism: Science and Policy Choices', Cambridge, MA: MIT Press, 2009, p. 29.

As the *EU WMD Strategy* highlights the transit of these weapons-usable substances must happen in a controlled way in order to facilitate the identification and interception of these illegal transportations.[108] Accordingly, the EU external borders should be further enhanced against the illegal trafficking in CBRN materials.[109] In case of a theft or a loss of high-risk CBRN materials it is paramount to have in place efficient incident notification systems to ensure the quick transfer of information.[110]

Further EU recommendations with respect to the transport of hazardous chemicals suggest reducing the transport of these high-risk chemical materials if it is economically and technically possible.[111] Likewise, the EC and the Member States should ensure that high-risk chemicals and equipment are not delivered to illegitimate users. The establishment of a proper customer qualification scheme could enhance the effectiveness of the national provisions being already in place. In addition, in terms of high risk chemicals, a licensing scheme should also be considered.[112]

Australian counter measures

The aforementioned voluntary *National Code of Practice for Chemicals of Security Concern* encourages the adoption of point of sale and distribution procedures, together with effective physical security and inventory control processes that enhance the secure transportation of these chemicals.

---

[108] 15708/03, The European Council, Fight against the proliferation of weapons of mass destruction, 2003, p. 12. The significance of intercepting the proliferation flows of these materials emerges in the updated version of the *EU WMD Strategy.* 17172/08 Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 2008, p. 8.
[109] 17172/08 Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 2008, p. 17-19.
[110] 15505/1/09 REV 1, 2009, p. 35.
[111] 15505/1/09 REV 1, 2009, p. 20.
[112] *Ibid.*, p. 24.

4.2.3. Acquiring chlorine of a lower concentrate from legitimate trading channels

Diluted chlorine is publicly available − for instance − in stores selling pooling chemicals. Accordingly, non-state actors may attempt to purchase the chemical agent in person or via an online transaction. The same considerations apply if an innocent agent acts on behalf of the non-state actor and turns up at a store or will arrange the purchase of the chemical online.

European-level counter measures

While EU-level strategic provisions do not address how to detect and counter malicious intents in such situations, national reporting mechanism of a wide spectrum exist, interpreting suspicious actions in this regard. Without aiming to give an exhaustive list, the *German Special Reporting Service* covers 'all illicit actions and transaction concerning CBRN materials, including: unauthorized use related to production, sale, acquisition, transfer, import, export, transit, ownership, exercise of control; and theft of CBRN materials as well as illicit offering of CBRN materials for sale'[113]. Although the list of criteria concerning what qualifies as a suspicious transaction has not yet been communicated to the reporting units, it is planned to happen in the future.[114] The *Dutch mechanism for reporting suspicious transactions with regard to chemicals* − a dual system, that is applied even for drug-precursors – has developed a set of simple criteria to help operators identify suspicious transactions.[115] The *French Code of Conduct on Drug Precursors* gives full details in its Appendix about those questionable circumstances that must be reported, including suspicious orders or requests for information.[116] In a similar vein, the *Code of Conduct of the UK Chemical Business Association and the Chemical Industry Association* on chemical trade controls, stress that economic operators 'should draw upon their own experience to assess whether an order or enquiry is

[113] *Stocktaking study on good practices on reporting of suspicious transactions in relation to CBRN materials*, Final Report for DG Home Affairs, 2013, p. 28.
[114] *Ibid.*
[115] *Ibid.*, p. 30.
[116] *Ibid.*, p. 32.

suspicious'[117]. To assist these intuitive processes, an extensive guide of 38 criteria has been compiled and grouped under four topics: client identification; business practices; delivery methods and use of the product.[118]

The London bombings in 2005 revived the *UK Know Your Customer awareness-raising campaigns* operated by the *National Counter Terrorism Security Office* in close collaboration with the relevant trade associations. These voluntary campaigns are effective instruments in detecting malevolent intentions at the end of the supply chain. They aim to raise awareness among relevant traders or economic operators about the risks from the illicit use of their products and give basic advice about ensuring that they supply those products to known customers.[119] For that purpose, 'leaflets and posters with a six-point check list are disseminated amongst traders, addressed at client-facing staff'.

Australian countermeasures

To minimize the risks associated with their work, manufacturers and industrial end users of chemicals have broad responsibilities. They need to obey regulative provisions, codes of practice, with regard to the whole life cycle of chemicals that are of security concern. This product stewardship trend presumes a closer interaction with different industrial stakeholders, and thereby extends the responsibility of the producer. There are many chemicals available for households, and this situation means that members of the community have a responsibility to use them safely in accordance with the directions.[120]

[117] *Ibid*., p. 35.
[118] *Ibid.*
[119] Stocktaking study on good practices on reporting of suspicious transactions in relation to CBRN materials, 2013, p. 37.
[120] New South Wales Environment Protection Authority, Review of the Environmentally Hazardous Chemicals Act 1985, Background Paper, 2003, p. 1-2.

To ensure the security management at the end of the chemical supply chain, good security practices include the need to verify that all customers are legitimate.[121] Additionally, the National Security Hotline (1800 123 400) has been established to welcome the reporting of any suspicious behavior with regard to the sale and/or use of these concerned chemicals and all security breaches. A long list of examples is cited clarifying what constitutes a suspicious behavior in this regard. There are separate guides for retailers and businesses that sell wholesale or store chemicals, together with transporters who deliver chemicals of security concern. These guidelines not only detail possible suspicious indicators of such situations, but also make recommendations on how to make notes in these cases.[122]

In spite of widespread Australian regulatory enactments in this field, existing controls on chemicals of security concern address risks posed by 'the accidental or negligent misuse of chemicals, rather than intentional misuse'[123]. There are also gaps in businesses' capabilities to deter, prevent, identify or manage their existing security gaps even in case of a theft of diversion of these chemicals.[124] There have been narratives from the industry that suggest, 'the risk posed by toxic chemicals are very low'[125] and the security of these chemicals are already regulated in a robust manner. There have been other suggestions on applying exemptions to certain businesses, for example to those facilities that use only a minor quantity of these chemicals.[126] The use of toxic industrial, agricultural or veterinary chemicals in Australia have been associated with criminal activities such as attempted or actual poisoning, murders and suicides.[127] The current National Code is the instrument for setting even 'more efficient mechanisms to raise awareness'[128] in the field. Awareness raising applies to the community, the industry and even to government to build capacity by targeted

[121] Australian Government, National Code of Practice for Chemicals of Security Concern, 2016. p. 13.
[122] *Ibid.*
[123] Attorney General's Department, Decision Regulation Impact Statement, Chemical Security: Toxic Chemicals of Security Concern, November 2014, p. 71.
[124] *Ibid.*
[125] *Ibid.*, p. 72.
[126] *Ibid.*, p. 73.
[127] *Ibid.*, p. 71.
[128] *Ibid.*, p. 74.

programs in the form of training or guiding materials.[129] As the Australian Security Intelligence Organization (ASIO) has summarized, the concept can 'create a culture of security awareness'[130], where retailers request identification details from the purchaser and create an auditable trail of transaction records'[131] that 'will have a deterrent effect and thereby reduce the risk of acquisition of precursor chemicals for malicious purposes'[132].

Conclusions

The first shortcoming in terms of the EU-level counter strategy that the above analysis has revealed is the lack of a comprehensive approach for regulating CBRN materials of concern. There are provisions on certain hazardous substances, but the systematized, overall regulatory framework exposes a daunting demand for the field.[133] There are various international, national and EU-level lists of hazardous substances, but the purpose, criteria and perspective of each list differs, and more importantly, does not necessarily focus on the security-related risks of the material.[134]

While the exchange of information and best practices is a founding pillar of the respective EU counter strategy, private stakeholders, especially the representatives of industry, have only limited access to the relevant platforms. In addition, several EU-level early warning systems operate with the mission to exchange information in case of a CBRN-related

[129] An Agreement on Australia's National Arrangements for Management of Security Risks Associated with Chemicals, 2 October, 2008, p. 14.
[130] Attorney General's Department, Decision Regulation Impact Statement, Chemical Security: Toxic Chemicals of Security Concern, November 2014, p. 53.
[131] *Ibid.*, p. 53.
[132] *Ibid.*, p. 53.
[133] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 17.
[134] *Ibid.*, p. 19-20.

emergency (e.g. RAS BICHAT, EWS, RAS CHEM, ECURIE), although there is no cross-border platform for suspicious transactions or loss of CBRN materials.[135]

One of the main concerns in relation to the regulation of the CBRN-related field is that it mainly focuses on safety matters rather than on terrorism-related security aspects.[136] Even if some of them have an impact on security, it is about diminishing the toxic consequences of these materials on people or on the environment.[137] As Paturej et al note, however, 'to move towards improved global chemical safety and security management […] chemical security should no longer be separated from chemical safety'[138].

Another important aspect pinpoints the significance of addressing insider threats.[139] Passive, active or violent insiders[140] who become persons of security concern – whether they are self-motivated, recruited, infiltrated, inadvertent or coerced perpetrators[141] – are of particular note in two regards. First, they are a source of valuable information on weapons-usable materials and second, they represent a direct link to procurement of these hazardous substances. EU provisions regarding the non-proliferation of weapons of mass destruction and their delivery systems[142] set the demand for strengthening measures to combat intangible transfers of knowledge and know-how. As these measures suggest, this could be achieved

[135] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 18.

[136] 12653/10 ADD 1, Commission Staff Working Paper, Tacking Stock of EU Counter-Terrorism Measures Accompanying document to the Communication from the Commission to the European Parliament and the Council, The EU Counter-Terrorism Policy: main achievements and future challenges, 2010, p. 23-24.

[137] *Ibid.*

[138] Krzysztov Paturej and Pang Guanglian, *Meeting Growing Threats of Misuse of Toxic Chemicals: Building a Global Chemical Safety and Security Architecture and Promoting International Cooperation*, in: M. Martellini, A. Malizia (Eds.), *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges, Terrorism, Security, and Computation*, Springer, 2017, p. 307.

[139] As noted in COM (2017) 610 final, p. 7.

[140] Matthew Bunn and Scott D. Sagan (Eds.), *Insider Threats*, Ithaca and London: Cornell University Press, 2016, p. 4.

[141] *Ibid.*

[142] 17172/08 Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 2008, p. 11-13.

by establishing consular vigilance procedures[143], exercising vigilance in protecting scientific and technical assets[144] and further, by increasing the awareness of scientific and academic communities engaged in nonproliferation issues concerning potential risks related to their activities[145]. Meanwhile, the Australian Security Intelligence Organization (ASIO) has further substantiated the significance of targeting insider threats when asserting in its 2016-17 Annual Report, that 'we remain alert to and promptly investigated threats from malicious insiders […] A critical element of our response to this threat has been to conduct targeted outreach with government and industry executives and agency security advisers, to improve their capabilities to detect malicious insiders and mitigate the harm caused by their actions.'[146]

'Learning about both successes and fails'[147] with respect to past incidents related to insider threats can help leaders better understand the complexity of the problems[148] that they need to tackle. Scholarly literature drawing on previous case studies, and thereby elaborating 'worst practices'[149] in this regard, aims to challenge Otto von Bismarck's thoughts, namely that only a fool learns from his own mistakes; a wise man learns from the mistakes of others. In examining the failures that high-security organizations have made, Zegart sheds light on the root causes of these errors. She argues that while academic literature is particularly engaged in the organizational dynamics of terrorist groups, the organizational dynamics of law enforcement and intelligence agencies have not been adequately discussed.[150] Her

[143] 17172/08 Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 2008, p. 11-13.
[144] *Ibid.*, p. 11.
[145] *Ibid.*, p. 13.
[146] Australian Security Intelligence Organization, Annual Report 2016-17, p. 5.
[147] Matthew Bunn and Scott D. Sagan (Eds.), *Insider Threats*, Ithaca and London: Cornell University Press, 2016, p. 9.
[148] *Ibid.*
[149] Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats*, in Matthew Bunn and Scott D. Sagan (Eds.), *Insider Threats,* Ithaca and London: Cornell University Press, 2016, p. 146.
[150] Amy B. Zegart, *The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies*, in Matthew Bunn and Scott D. Sagan (Eds.), *Insider Threats*, Ithaca and London: Cornell University Press, 2016, p. 44.

implications raise issues such as the fact that 'surprise attacks are almost never really surprises'[151], as well as 'the hidden hazards of routines'[152], that drive individuals in bureaucracies to follow the old-fashioned ways even if they react in a different way. All this highlights that organizations do matter[153]. Zegart concludes that to tackle such issues appropriately, 'a vibrant culture of safety and security'[154] is necessary.

In accordance with this somewhat shaky safety and security culture, numerous prerequisites have been articulated. Accordingly, organizational leaders are required to address the disgruntlement of employees by establishing 'a strong, performance-oriented culture'[155] where people and their complaints and ideas are well-treated. In case of family or financial problems, occupational health programs should be available for the employees of high-security facilities, and leadership training programs should be promoted in this respect to reduce dissatisfaction.[156] To broaden the scope of this advanced safety and security culture, recruitment checks should be expanded − even to visitors and contractors of high-risk facilities. The process of checking their references could include a personal interview at their home and further information should be obtained about the candidate from the respective authorities. Additionally, periodic inventory checks should be put in place to enforce a regular control, together with effective incident-reporting mechanisms. At the same time, appropriate IT infrastructure should provide cyber security and protect sensitive information stored and handled by such an organization.

4.3. Development of a chemical weapon

[151] Amy B. Zegart, *The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies*, in Matthew Bunn and Scott D. Sagan (Eds.), *Insider Threats*, Ithaca and London: Cornell University Press, 2016, p. 45.
[152] *Ibid.*
[153] Amy B. Zegart, *The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies*, in Matthew Bunn and Scott D. Sagan (Eds.), *Insider Threats*, Ithaca and London: Cornell University Press, 2016, p. 47.
[154] *Ibid.*, p. 63.
[155] Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats*, in Matthew Bunn and Scott D. Sagan (Eds.), *Insider Threats*, Ithaca and London: Cornell University Press, 2016, p. 161.
[156] *Ibid.*

Once in the possession of the necessary knowledge together with the materials and the equipment, violent non-state actors need to apply the know-how and modify (purify) the chemical agent in accordance with their malicious purposes and construct the malevolent device. This development phase can be broken into two parts. The first section of the discussion elaborates the challenges, terrorists or extremists need to tackle when *transporting the already acquired material to the place where the development will take place*. The second part of this discussion considers *the process of constructing the device*.

4.3.1. Transporting the acquired chlorine to the place of the construction

European-level counter provisions

Transporting toxic chemicals is the most vulnerable area when compared with the development, storage or trade of these hazardous materials.[157] Therefore, there is a stressed emphasis to develop capabilities and detect the illegal transport of hazardous materials. If such movements cross EU external borders, body scanners, explosive trace detection equipment, trained K9 dogs or behavior detection officers offer several layers of detection to identify the deceitful purposes.

The right for free movement makes the control of the sensitive materials' transport between Schengen States extremely difficult as by the establishment of the Schengen Zone internal border checks have been abolished.[158] It is only in the case of a serious threat to internal

[157] Krzysztov Paturej and Pang Guanglian, *Meeting Growing Threats of Misuse of Toxic Chemicals: Building a Global Chemical Safety and Security Architecture and Promoting International Cooperation*, in: M. Martellini, A. Malizia (Eds.), *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges, Terrorism, Security, and Computation*, Springer, 2017, p. 307.

[158] available at: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en

security, when the Schengen State is entitled to temporarily reintroduce border control at its internal borders for – in principle – a limited period of no more than thirty days.[159]

To combat these challenges, the European Commission urges the Member States to work together on identifying the necessary technical requirements for the sampling and detection of CBRN materials, and thereby establish an EU wide validation, testing and trialling system that can evaluate the quality of detection tools and systems.[160] To identify these technical details, and help in the efficiency of these endeavors, further research needs to be done on the features of sensitive materials. Additionally, the *EU CBRN Action Plan* highlights that Member States need to collaborate in terms of both how to operate these detection devices, and how to respond, if CBRN materials of concern have been identified.[161] Similarly, better cargo information from the trade and the enhancement of detection capabilities for customs could contribute to the interception of suspicious CBRN materials at the borders of the EU.[162]

Australian counter provisions

The nature of the challenges is different in relation to Australian borders. Under the aegis of prevention, disrupting the movement of terrorists and support for terrorism involve activities such as 'stopping terrorists, violent extremist propaganda and weapons from entering Australia'[163]. The Department of Home Affairs (more specifically the Australian Border Force — ABF) is 'the primary Commonwealth agency'[164] performing the border protection and immigration roles at air and sea ports. ABF – working in close collaboration

[159] 1051/2013 Regulation of the European Parliament and of the Council of 22 October 2013 amending Regulation (EC) No 562/2006 in order to provide for common rules on the temporary reintroduction of border control at internal borders in exceptional circumstances
[160] 15505/1/09 REV 1, 2009, p. 45.
[161] 15505/1/09 REV 1, 2009, p. 50.
[162] COM (2017) 610 final, p. 6.
[163] Council of Australian Governments, Australia's Counter-Terrorism Strategy, Strengthening Our Resilience, 2015, p. 16.
[164] Australia New-Zealand Counter-Terrorism Committee, National Counter Terrorism Plan, 4th Edition, 2017, p. 16.

with other government agencies – is responsible for the 'monitoring, assessing, detecting and preventing the illegal movement of people and goods across Australia'[165] in relation to counter-terrorism activities. The Australian Government controls the import and export of certain goods with the following legal instruments. In case of levying an absolute prohibition, the concerned goods cannot be exported or imported under any circumstances. If certain goods are restricted, a written permission is required before importing or exporting them.[166] *Customs Act 1901* executed through *Regulation 13E of Customs (Prohibited Exports) Regulation 1958* entitles the Minister for Defence to compile the list of goods which require a defence permit or license for being exported.[167] The *Weapons of Mass Destruction (WMD) Act 1995* controls the items that are not listed on any other registers, but that could be an essential element of a WMD weapon.[168] The *Defence Export Control Office* is authorized to issue permits and licenses of goods that are either listed or that fall under the WMD Act's controls as being weapons-usable materials.[169] The Office of Transport Security is the regulator for aviation and maritime transport. By taking a 'proactive and forward-looking approach'[170], its continuous reviews of regulation ensure that the transport security system are targeted towards high-risk areas.

4.3.2. The process of development

The process of developing the malicious chemical device offer tangible indicators to detect and identify such malevolent endeavors. Non-state actors leave numerous traceable evidence behind such as accidental releases, bad or unusual odors, fumes and vapors, the presence of special laboratory or personal protective equipment, as well as suspicious deliveries or

[165] Australia New-Zealand Counter-Terrorism Committee, National Counter Terrorism Plan, 4th Edition, 2017, p. 16.
[166] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 12, Domestic Legislation, 2014, p. 2.
[167] *Ibid.*, p. 3.
[168] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 12, Domestic Legislation, 2014, p. 3.
[169] *Ibid.*
[170] available at: https://infrastructure.gov.au/security/

dumped waste containers. The following discussion aims to map whether or not there are policies in place to exploit these opportunities for detecting such indicators of malevolent preparatory activities.

EU-level counter provisions

Increasing vigilance in members of the public helps national law enforcement agencies get into better position to prevent or detect a terrorist attack. Recently, the *Action Plan to support the protection of public spaces* has explicitly declared the demand for 'raising public awareness'[171]. As the document asserts 'Greater public awareness will help ensure that suspicious behavior is swiftly reported'[172]. At the same time, it recommends sharing the already available effective, national awareness-raising campaigns with all other Member States.[173] Although prevention is one of the three main targets with respect to the CBRN-terrorism-related threat, it refers rather to 'ensuring that unauthorized access to CBRN materials of concern is as difficult as possible'[174] and does not address public awareness raising in this regard. The respective EU norms draw upon pooling 'all relevant stakeholders'[175] into the prevention phase, however the general public is not mentioned among these partakers. In a similar vein, one of the fundamental objectives of the *CBRN Action Plan*[176] is a more focused and coordinated approach to 'enhance our knowledge of CBRN risks'[177]. This CBRN expertise is pooled together to: i) 'maintain a comprehensive understanding of CBRN risks'[178]; ii) 'develop cooperation and coordination at operational level (e.g. exchange of information and best practices)'[179]; and iii) 'facilitate the civil-military

[171] COM (2017) 612 final, p. 6.
[172] COM (2017) 612 final, p. 6.
[173] *Ibid.*
[174] *Ibid.*
[175] *Ibid.*, p. 5.
[176] COM (2017) 610 final, p. 3.
[177] *Ibid.*, p. 4.
[178] *Ibid.*, p. 12-13.
[179] *Ibid.*

cooperation in the field'[180]. As the document presumes, 'we' refers to the governmental, academic and private actors at both strategic and operational levels, but not the public community. Therefore, however, the immediate environment of the perpetrator is crucial, raising public awareness of suspicious behavior with regard to the development phase of a terrorist attack is – unfortunately - outside the scope of this concept.

Australian counter provisions

The News South Wales Counter Terrorism Plan establishes that 'the community is a key resource in efforts to counter terrorism with the capacity to provide early warnings to risk'[181]. In this sense, in order to promote positive working relationships, the NSW Police Force Community Contact Unit actively engages with the community, although the law enforcement agencies develop these relationships 'to increase the understanding of NSW counter terrorism arrangements'[182]. Public communication is meant to enable 'resilience and vigilance in times of emergency'[183] 'especially during and following a terrorist attack'[184], but not beforehand.

In addition, a continual program of training and awareness-raising of first responders, health workers, across numerous industry fronts has been undertaken since 2007. These programs specifically targeted unusual, suspicious behavior and indicators of potential nefarious purchases.

Conclusions

[180] COM (2017) 610 final, p. 12-13.
[181] New South Wales Counter Terrorism Plan, December 2016, p. 11.
[182] New South Wales Counter Terrorism Plan, December 2016, p. 11.
[183] Council of Australian Governments, Australia's Counter-Terrorism Strategy, Strengthening Our Resilience, 2015, p. 5.
[184] *Ibid.*

The provisions of the *EU CBRN Action Plan* suggest thinking in scenarios when identifying work priorities in the detection field. The EC calls upon the Member States to exchange data and information on national incidents, to allow for a broad criminal trend in this regard.[185] There is an impressive amount of open-source material on incidents where illegal transports of weapons-usable material have been intercepted. If academic research could analyze this available dataset by applying the 'cumulative knowledge base[186]' on CBRN motivations, the outcome could offer new, outsider perspectives to the analytical work in this area.

Although there are effective awareness-raising materials for the public in place, such content may be further supplemented by other crucial information. While touching upon how to recognize suspicious behavior and thereby building a responsible citizen profile, there are early warning signs that are not given sufficient attention in this regard.[187] The available guidelines address the execution phase of a terrorist attack but do not offer suggestions for the suspicious indicators during the process of developing a CBRN weapon.

At the same time, future initiatives should entrench into the minds of all citizens not only the responsibility for recognizing suspicious signs of a terrorist activity but also need to establish the inherent commitment to report these identified early warnings. There are grave concerns whether communicating the methods how to identify suspicious individuals and rather keep these guides under an official secrecy, as it happened previously. On one hand, the arguments against bringing such guides to public may be justified, since they draw the attention of criminals to particularly suspicious indicators. On the other hand, however, benefits of such reestablished relationships between law enforcement agencies and the public

[185] 15505/1/09 REV 1, 2009, p. 42-43.

[186] Gary Ackerman, 2009. p. 17.

[187] Note: this resonates back from the lessons learned in conjunction with the August 2017 Attacks in Barcelona and Cambrils: *'The changes of the mood and habits of the young men, far from raising alarm within the Muslim community or inside their own families, were seen as either irrelevant or positive. This may have been a product of a lack of awareness inside the Muslim community and wider society about pointers toward radicalization.'* In Fernando Reinarez and Carola García-Calvo, '"Spaniards, You Are Going To Suffer": The Inside Story of the August, 2017 Attacks in Barcelona and Cambrils', in *CTC Sentinel*, 11:1, January, 2018, p. 9.

community would certainly outweigh the concerns in this regard. Terrorists and extremists are also human beings who make human errors and constantly leave traces behind. Having vigilant and sufficiently-informed public eyes around them will recognize these early warning signs. Law enforcement agencies then only need to make sure these identified suspicious indicators are reported to them.

While there is scholarly literature on public communication on CBRN threats, these contributions investigate risk and crisis communication together with recommended protective behaviors in case of a CBRN terrorist incident. The ultimate implications of these works, however, – such as ensuring that the messages are communicated by trusted spokespeople and via widely accessed sources'[188], as well as observations like the public 'appeared to be more receptive to official advice and rated messages coming from the authorities as more credible'[189] – have relevance even concerning public communication in terms of the prevention phase of a terrorist attack.

4.4. The execution of the attack

The final phase of the perpetration occurs when the individuals deploy the already constructed device. The logic of this research breaks this process into two segments: first, *the way to the scene of the plot;* and second, *delaying or compromising circumstances at the scene of the plot*.

4.4.1. The way to the scene of the plot

European-level counter provisions

[188] Aino Ruggiero and Marita Vos, 'Communication Challenges in CBRN Terrorism Crises: Expert Perceptions', in *Journal of Contingencies and Crisis Management*, 2015, 23:3, p. 138-148.
[189] *Ibid.*

Efforts towards increasing vigilance in the public have already been elaborated with regard to the development phase of the attack. As mentioned earlier, the addressees of policy efforts to enhance 'our' knowledge of CBRN risks are spread across governmental agencies, the industry and the academia, but do not refer to the general public. On the other hand, recognizing such suspicious indicators are rather a part of the counter policy on enhancing the security of public spaces, and therefore will be explored in the next section.

Australian counter provisions

There have been numerous terrorists who have been detected by onlookers who have acted upon their inherent suspicion and reported the identified indicators. Members of the public, therefore, play a pivotal role in detecting suspicious behavior. The Australian counter terrorism strategy repeatedly emphasizes the responsibility each member of the public has for reporting such suspicious behavior.

> 'We have this phrase, "Communities defeat terrorism." Terrorism has been defeated by good covert intelligence, and that's what we've relied upon over the years, whether it's the interception of communications by intelligence agencies or human intelligence sources. And those do still play a big part. But with the nature of this particular Daesh threat, it's becoming more important to have connectivity with the wider community [suspicious behavior] is not going to be intercepted necessarily by good intelligence coverage in Syria. But it might be intercepted by a schoolteacher actually spotting a young lad who's got beheading videos on his phone. […] It's still obviously important to have covert intelligence, but we're seeing an increase in reporting on people who are of concern from schoolteachers, health services, psychiatrists, and so on. When we get that information, we can interdict and we can prevent terrorism.'[190]

[190] Paul Cruickshank, 'A View the CT Foxhole: An Interview with Richard Walton, Head, Counter Terrorism Command, London Metropolitan Police', *CTC Sentinel*, January 2016, p. 5.

As the WMD Commission has noted: it is embracing the reality 'that the public can represent a vast early warning network. Cooperative relationships between citizens and law enforcement are becoming a major weapon in combating terrorism.'[191]

As the *Australian National Security Public Information Guidelines* specify, the main purpose of 'public information and media activities relating to national security issues and incidents'[192] is threefold: i) 'improve the understanding of the public of Australia's national security organizations and systems'[193]; ii) 'generate confidence in Australia's ability to respond to any terrorism threat or activity'[194], and iii) 'create public trust that governments and national security agencies are open and accountable and will release all information possible within the confines of operational and security considerations'[195]. With these goals in mind, key messages are to be non-political, simple, clear and relevant[196]. While these guidelines predominantly concern the preparedness and crisis management phases of a terrorist attack, the provision aiming to 'engage the community to play a role in prevention of attacks'[197] explicitly refers to the involvement of the public to keep a vigilant eye on suspicious acts and report them via a central reporting point - the National Security Hotline[198] – to the respective authorities. In a similar vein, the *NSW Counter Terrorism Plan* asserts that 'community is a key resource in efforts to counter terrorism with the capacity to provide early warnings to risk'[199], therefore highlighting the importance of engaging the community.

4.4.2. Deploying the device

[191] World at Risk, The Report of the Commission on Prevention of WMD Proliferation and Terrorism, Vintage Books, 2008, p. xxvii-xxviii.
[192] National Counter-Terrorism Committee, 'National Security Public Information Guidelines', 2010, p. 2.
[193] National Counter-Terrorism Committee, 'National Security Public Information Guidelines', 2010, p. 2.
[194] *Ibid.*
[195] *Ibid.*
[196] *Ibid.*, p. 6.
[197] *Ibid.*, p. 6.
[198] *Ibid.*, p. 17.
[199] New South Wales Counter Terrorism Plan, December 2016, p. 11.

European-level counter provisions

As the logical line of the argument in the thesis suggests, the chance to identify and interdict a CBRN attack in the final phase of its commission is significantly lessened. Regardless of the challenges to tackle and regulate this perpetration phase, the EU policy addresses the most tangible aspects in this regard.

The European terror attacks draw policymakers' attention to the so-called 'soft targets', namely open public places with high concentration of people.[200] The current anti-terrorism package compiled by the European Commission addresses an enhanced protection of these locations. The recently adopted countermeasures aim to support the Member States' efforts in detecting threats, reducing the vulnerability of these places, improving cooperation and ultimately mitigating the consequences of a terrorist attack.[201] Under the aegis of this objective, the EU provides two ways to protect public spaces. Firstly, by offering funding opportunities it aims to improve the exchange of best practices across borders to promote the development of 'innovative and discreet barriers'[202] that will not inhibit the open character of these places. This exchange of expertise must be further enhanced by testing activities to measure the effectiveness of these concepts. There is also a stressed need for further research to enhance the capability of CBRNE materials' detection.[203] Secondly, EU efforts aim to foster cooperation with a wide range of stakeholders to enhance the protection of these public spaces. The main idea is to exchange best practices in this regard. The scope of this cooperation entails local level specialists, representatives of the private sector, together with

[200] Europol Terrorism Situation and Trend Report 2017
[201] COM (2017) 608 final, Communication from the Commission to the European Parliament, the European Council and the Council, p. 2-4.
[202] *Ibid*., p. 3.
[203] COM (2017) 612 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Action Plan to support the protection of public spaces, p. 4.

exchanging best practices in relation to critical infrastructure protection concerning the preparedness against CBRN threats.[204]

Another valuable aspect here concerns the current criminal trend of the Islamic State, using unmanned aerial systems (UAS) for carrying out attacks with explosives. The recent Action Plan takes into consideration these innovative tactics and future EU work will put forward measures facilitating the detection of such hostile vehicles.[205]

There is pervasive interest in various CB disciplines to develop capabilities to detect, identify and quantify the indicators of exposure to CBRNE materials. Effective detection technologies in place at an entrance gate of a mass event (e.g. IMSK: integrated CBRN mobile security kit for large events[206]), can detect CBRN materials or weapons that the criminal intends to deploy at such gatherings. There are also technologies to detect vapor chemical threat agents, however there are only limited capabilities to identify liquid-based chemical droplets.[207] There are also limitations of current detection technologies. For instance, they cannot recognize low-level chemical threat agents, nor can they distinguish chemical threat agents of concern and 'urban environmental chemicals'[208]. Another notable point here is that most of this detection equipment requires laboratory-based analysis, that considerably delays the prompt response such attacks need.[209] As the European Union's Council observes, development of highly-mobile, deployable identification and sampling capabilities[210] could further enhance the success of counteractions.

---

[204] COM (2017) 612 final, p. 2.
[205] *Ibid*., p. 6.
[206] For more information see:
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/cbrn_case_study_cses_en.pdf
[207] Ronald J. Kendall, Stephen M. Presley and Seshadri S. Ramkumar (Eds.), *New Developments of Biological and Chemical Terrorism Countermeasures*, CRC Press, 2016, p. 12.
[208] A. A. Fatah, R. D. Arcilesi Jr., T. Chekol, C. H. Lattin, O. W. Sadik and A. O. Aluoch, *Guideline for the selection of biological agent detection equipment for emergency first responders, 2nd Edition*, US Department of Homeland Security, Washington, DC, 2007.
[209] Ronald J. Kendall, Stephen M. Presley and Seshadri S. Ramkumar, 2016, p. 12.
[210] 15505/1/09 REV 1, 2009, p. 51.

Australian counter provisions

Places of contained mass gathering provide terrorists with attractive targets for inflicting mass casualties with a strong symbolic value and high impact media coverage. At the same time, operators and owners of such crowded places face serious security-related challenges. Having recognized that, a nationally consistent approach sets the baseline for a systematic process to identify the appropriate security risk-management activities that can then be integrated into existing jurisdictional arrangements. The success of *Australia's Strategy for Protecting Crowded Places from Terrorism* 'rests on strong and sustainable'[211], business and government partnerships. The concept relies upon building stronger partnerships, thereby enabling better information sharing and guidance, implementing effective protective security and ultimately increase resilience.[212] To reduce the likelihood of a successful terrorist attack, the concept suggests applying a so-called layered-security. The model encompasses: physical and electronical target hardening measures to deter; visual detection and alerts systems to detect; as well as timely and coordinated reaction to respond; together with physical countermeasures and processes to delay a terrorist attack.[213] Accordingly, building multiple security layers can ensure that 'a failure in any single layer will not significantly compromise the overall security of the place being protected'[214]. At the same time, security counter measures should be prioritized in accordance with highest risk areas of a crowded place and should be consistently proportionate and cost effective.[215]

The *Australian Strategy for Protecting Crowded Places from Terrorism* has been supplemented by further guides – reflecting the current terrorist tactics and modes of operation – including attacks committed by a hostile vehicle, an active armed offender or an improvised explosive

[211] Australia's Strategy for Protecting Crowded Places from Terrorism, 2017, p. 2.
[212] Australia's Strategy for Protecting Crowded Places from Terrorism, 2017, p. 3.
[213] *Ibid.*, p. 14-15.
[214] *Ibid.*, p. 14.
[215] *Ibid.*, p. 15-16.

device.[216] In August 2017, Australian law enforcement and intelligence authorities disrupted a plot involving an improvised chemical dispersal device consisting of hydrogen sulphide gas.[217] The event drew the attention to the security of crowded places, especially concerning the threat of an attack where chemical weapons are involved. The addressees of the Australia- New Zealand Counter-Terrorism Committee's *Chemical Weapon Guidelines for Crowded Places* are the operators and owners together with the public community. A separate guide outlines the responsibilities of the medical staff in such a situation. The document further specifies the provisions of the *Australia's Strategy for Protecting Crowded Places from Terrorism*. After a concise introduction into the risks associated with a chemical weapon attack, a range of measures detail what owners, operates and the public should do to detect, delay and respond to a terrorist attack. The objective of all these efforts is to minimize the risk to people. A noteworthy aspect of these guidelines is the aspect of public communication on how to improve the chances of survival in case of a chemical attack.[218]

Conclusions

In Australia, a strong role has already been given to the community and the private sector to 'provide guidance and support to resist violent extremist messages'[219]. At the same time, community leaders, community groups, teachers and social workers are in the best position to identify suspicious profiles and gain tangible and timely information on alleged suspects. Radicalized individuals are well-trained to stay out of authorities' sight, communicating only in person or with encrypted messages, leaving only little or no digital footprint that could be tracked by intelligence or law enforcement agencies. Members of the community are the most

[216] Hostile Vehicle Mitigation Guidelines, Active Armed Offender Guidelines and Improvised Explosive Device Guidelines available at www.nationalsecurity.gov.au/CrowdedPlaces
[217] Andrew Zammit, 'New Developments in the Islamic State's External Operations: The 2017 Sydney Plane Plot', *CTC Sentinel*,10:9, October 2017, p. 13-18.
[218] Australia-New Zealand Counter-Terrorism Committee, 'Chemical Weapon Guidelines for Crowded Places', 2017, p. 5.
[219] Council of Australian Governments, Australia's Counter-Terrorism Strategy, Strengthening Our Resilience, 2015, p. 8.

appropriate persons to detect suspicious behaviors and get to know more about these individuals.

In addition, individuals on their way with the constructed device to the planned plot can behave in a suspicious manner that can be identified by citizens travelling on the very same public transport vehicle or walking past at the crowded square. There cannot be enough sensors to detect each and every malicious material in public places. Counteractions are required to rely also on well-prepared public eyes. Therefore, in keeping with the WMD Commission's recommendation, 'this effort should start by developing a public education program that goes well beyond the vague admonition to report "suspicious activities". The public must be aware of what activities are suspicious and of their responsibility to inform authorities.'[220] Public guides elucidating special indicators of such suspicious behavior compiled by practitioners, psychologists or other professionals in the field would open up the public eyes, who can thereby share the responsibility to interdict terrorist attacks. Importantly, these public guides need to refer to all likely forms of a terrorist attack, including a low-tech or even a CBRN attack. Law enforcement and intelligence administration need to encourage citizens to actively participative in tackling current challenges.

Another step forward is the willingness of the public to report the identified warning indicators. In general, people recognize these suspicious behaviors, but authorities need to make sure, citizens will communicate these early warning signs. Establishing a prompt communication channel between law enforcement agencies and the public on terrorist threats could be an appropriate start to build this necessary cooperative relationship. On the

[220] World at Risk, The Report of the Commission on Prevention of WMD Proliferation and Terrorism, Vintage Books, 2008, pp. xxviii.
This effort is taking shape in Kortunov's argument, when stating 'The international community has to rise to the challenge and to reconsider its current approach to CWs. This implies a new level of public awareness, […]' in Andrey Kortunov, 'Are Chemical Weapons Getting More Dangerous Than Nuclear?', *American Herald Tribune*, January, 30, 2018, available at: https://ahtribune.com/world/2118-chemical-weapons-nuclear.html

other hand, to overcome the fear that reporting may have negative consequences on the reporter, citizens should be advised as to what to expect if building such trusting relationships with the law enforcement authorities.

Chapter Five

Biological Scenario

A biological agent is dispersed inside a ventilation system of a conference hall during an international conference. [1]

It is sometimes claimed that biological terrorism is the most likely and most dangerous threat we face. The development of nuclear weapons faces noteworthy challenges (given the limited amount of readily available fissile material and the nuclear programs in place) that make it particularly difficult to maintain the secrecy of such malicious intentions. At the same time, chemical weapons can be obtained much more easily, however a substantial quantity is necessary for a large-scale attack. Meanwhile, biological weapons are extremely potent, causing severe psychological effects. They are also easily accessible and can be developed from available source material by applying dual-use equipment.[2] Additionally, while a chemical, radiological or nuclear incident would induce effect on people 'in a spatially limited area, disease agents have a much greater chance of sickening random individuals in unconnected regions'[3].

5.1. Acquisition of the knowledge on biological agents

Expertise necessary for constructing viral biological agents can be obtained in numerous ways. Besides the common means of acquiring knowledge on biological agents and toxins, there are three special sources for gaining credible information. First, experts recruited and

[1] Monica Endregard, Hanne Breivik, Hege Schultz Heireng, Elin Enger, Therese Sandrup and Dominic Kelly, *D2.1 Scenario template, existing CBRN scenarios and historical incidents*, PRACTICE WP2 Deliverable, 2011, p. 56.
[2] Daniel M. Gerstein, *Bioterror in the 21st Century: Emerging Threats in a New Global Environment*, Annapolis, MD: Naval Institute Press, 2009, p. 154.
[3] Jean Pascal Zanders, *Internal dynamics of a terrorist entity acquiring biological or chemical weapon*, in: Brech Volders and Tom Sauer (Ed.), *Nuclear Terrorism: Countering the Threat*, Abingdon-on-Thames: Routledge, 2016, p. 28.

trained in the US or Soviet bioweapon programmes during the Cold War have the expertise to build biological weapons of concern.[4] Second, national biodefense programmes engaging in banned activities have been thriving recently, offering access to biowarfare knowledge to an ever-growing number of individuals.[5] And third, the development of biotechnology enables the civilian use of hazardous pathogens, further exacerbated by the fact that these civilian research facilities may not be adequately secured.[6] More importantly, 'unlike nuclear technologies'[7], biotechnological advancements have not been developed 'in classified settings at government-run labs', and therefore both the required materials and trainings are readily available to the public.

European-level counter provisions

The European provisions on suspicious transactions and behavior applies to all four strands of CBRN terrorism. This legislation has been widely interpreted with regard to the chemical scenario, therefore will not be repeated here.

Australian counter provisions

In a similar vein, the same Australian counter provisions on preventing a terrorist attack – previously elaborated in the chemical chapter - apply to this section also, except for the unique instrument of the National Health Security Check (NHS). This background check encompasses a national criminal history check and a national security assessment of persons who will be authorized to handle biological agents of concern thereby providing 'another

[4] European Parliament Briefing on CBRN Terrorism: threats and the EU response, January 2015, p. 4.
[5] *Ibid.*, p. 4.
[6] *Ibid.*, p. 4.
[7] Benjamin Wittes, *Innovation's Darker Future: Biosecurity, Technologies of Mass Empowerment, and the Constitution*, in R. D. Howard and J. J. F. Forest (Eds.), *Weapons of Mass Destruction and Terrorism 2nd Edition*, New York: McGraw Hill, 2012, p. 159.

layer of security to reduce the risk of persons with malicious intent gaining access to security sensitive biological agents, facilities or sensitive information'[8].

Conclusions

There is a general belief, that developing a bioweapon requires only the procurement of biomaterials, scientific data and equipment. However, the challenge is not about the acquisition of these essential elements, but the use of the material and the technologies required for their development[9]. This science-based knowledge and technology is not 'universal, independent of context impersonal public or cumulative[10]'. As Ben Ouagrham-Gormley argues, this knowledge is far from 'free flowing[11]'. Constructing a viable biological device requires both tacit and explicit knowledge from widespread disciplines. Acquiring this nuanced expertise is a complicated and long process, that needs to be taken into account when assessing the threat of bioterrorism.

A point of note here is that keeping abreast of the constantly evolving technological advancements constitutes serious challenges for national authorities. These developments represent copious amounts of effort for analysists in reassessing the related threat according to the emergence of new technological innovations. As such, security concerns of so-called dual-use technologies should be addressed from a different angle. As Ackerman suggests, 'rather than imposing blanket restrictions on all new technologies that might pose some danger, which would no doubt become a Sisyphean, if not downright counterproductive, task'[12], policymakers should rather identify 'technology-organizational dyads of greatest concern and thereby prioritizing technology control and non-proliferation efforts'[13]. 'It makes

[8] Available at: http://www.health.gov.au/internet/main/publishing.nsf/Content/ssba-fs-15
[9] Sonia Ben Ouagrham-Gormley, *Barriers to Bioweapons, The Challenges of Expertise and Organization for Weapons Development*, Cornell University Press: Ithaca and London, 2014, p. 1-2.
[10] *Ibid.*, p. 8.
[11] *Ibid.*, p. 8.
[12] Gary A. Ackerman, 2014, p. 247.
[13] *Ibid.*

more sense to focus on constraining and negating the relevant organizations, rather than controlling the spread of the technology.'[14] 'A better strategy might be to monitor more closely those organizations with the motivation and capability to exploit these technologies, in search of indications of their interest, once again arguing for a focus on organizations in conjunction with technologies, rather than on the technologies in isolation.'[15]

5.2. Acquisition of biological agents

Biological agents substantially differ from chemical substances, nuclear or radiological materials, as they can be found in nature and thus do not need to be produced.[16] Alternatively, agents and the necessary production equipment are produced for pharmaceuticals, vaccines or even for cosmetics and therefore can be acquired from legitimate sources. [17] These so-called dual-use sources are one of the gravest concerns in relation to counter policies. Another important factor with regard to the bio strand – unlike the radiological, nuclear or chemical realm - is that it is open-source. While chemical, radiological or nuclear materials of security concern are 'highly regulated'[18], biological advancements can be either dual or multi-use. Biological agents are readily available, and most of the necessary equipment can easily be obtained as they do not fall under any regulatory regime.[19]

European-level counter provisions

[14] Gary A. Ackerman, 2014, p. 247.
[15] *Ibid*., p. 248.
[16] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 14.
[17] Melissa Gillis, *Disarmament – A Basic Guide Fourth Edition*, p. 61.62, available at: https://www.un.org/disarmament/wp-content/uploads/2017/09/Basic-Guide-4th-Edition-web.pdf
[18] Kristina Hummel, 'A View from the CT Foxhole: Edward You, FBI Weapons of Mass Destruction Directorate, Biological Countermeasures Unit', *CTCT Sentinel*, August 2017, p. 11.
[19] *Ibid.*

The *EU CBRN Action Plan of 2009*[20] sets the material scope for the regulation when establishing the need for developing EU lists of high-risk biological agents and toxins in line with well-substantiated risk assessment and criteria, as mentioned in the chemical scenario. Establishing and maintaining high-level biosecurity and biosafety[21] of these materials and facilities is the central piece of the relevant legislation. In this vein, the *Action Plan* specifies that Member States should establish a registry of the facilities[22] possessing any of these hazardous biological agents and toxins. While keeping a precise inventory of the stored materials, facilities should regularly review the need for keeping these biological substances.[23] A special emphasis is given to the implementation at the so-called laboratory bench level.[24] Likewise, the storage of clinical samples of any of the concerned high-risk biological agents or toxins should – in principle – be avoided.[25]

Establishing laboratory safety in biolabs is of paramount importance. The physical protection of these facilities together with developing bio-safety guidelines with regard to the personnel working there must be consistently regulated. Besides developing biosecurity and biosafety at the aforementioned facilities, Member States should make reasonable efforts to form a high security culture for the staff of these facilities by delivering trainings, sharing relevant best practices[26] and adopting codes of conduct[27]. In order to establish this increased biosafety culture, academic and scientific communities need to be involved in training programs that aim to develop a bio-ethical ground for their operation.[28] Another valuable aspect here is to put in place notification mechanisms for reporting the loss, theft or accident with regard to

[20] 15505/1/09 REV 1, 2009
[21] *Ibid.*, p. 17.
[22] *Ibid.*
[23] *Ibid.*
[24] *Ibid.*, p. 16.
[25] *Ibid.*, p. 17.
[26] *Ibid.*, p. 27.
[27] *Ibid.*, p. 28.
[28] SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 32.

the dangerous biological pathogens stored in these legitimate facilities. Outreach programs with the aim of increasing bioterrorism awareness of industry and the academic community can ensure another level of bio-security. Additionally, more precise legislation must be developed on the transport of biological agents regulating export, import and inventory controls. Security measures also need to address sensitive information in research data.

The European Commission calls upon the Member States to develop detection models for biological pathogens and toxins.[29] The *Action Plan*'s provisions on improving the detection capabilities need to be taken into account in two ways. First, when considering the illicit transport of hazardous biological agents and toxins. And second, when deploying the constructed biological weapon at the plot of the terrorist attack. In addition, provisions on the development of mobile detection capabilities have relevance here.[30] Once having established minimum requirements for validating detection systems in the European Union, testing and trialling schemes should evaluate the effectiveness of detecting mechanisms.[31] In terms of the detection of biological agents, reference material should be developed to improve the quality of detection.[32] In order to further ensure a minimum quality requirement for detection, a network of reference laboratories should be established.[33] Additionally, a smooth flow of information is required within and across Member States with respect to threats of biological agents or toxins.[34] The EU-level legislation on detection[35] needs to take

[29] 15505/1/09 REV, 2009, p. 44.
[30] *Ibid.*, p. 51.
[31] *Ibid.*, p. 45.
[32] *Ibid.*, p. 48.
[33] *Ibid.*, p. 52.
[34] *Ibid.*, p. 34.
[35] *Ibid.*, p. 42-53.

into consideration the characteristics of biological agents and toxins, together with their means of dissemination. Scholarly literature on these topics[36] could engender a deeper understanding.

Australian counter provisions

International conventions (Biological and Chemical Weapons Conventions), domestic laws and initiatives govern the use, importation and exportation of biological agents.[37] Having acknowledged the harm that the deliberate release of a biological agent may induce, the Council of Australian Governments' (COAG) Report of 2006 on the Regulation and Control of Biological Agents assessed the Australian regulation that at that time compromised only a few controls on the security of biological agents, and concluded that it has a safety, rather than a security-centered focus. Moreover, to reduce the risk that biological agents falling to the wrong hands, it is necessary to put in place a regulation on the secure storage, possession, use and transport of security sensitive biological agents.[38] Accordingly, the *National Health Security Act 2007* sets the legislative framework for the regulation of security sensitive biological agents in Australia, including a national register of the concerned bio-agents.[39] A national regulatory scheme, administered by the Office of Health Protection[40] within the Australian Government Health portfolio[41] , controls the registration, reporting and transport

[36] E.g. J. Pichtel, *Terrorism and WMDs: Awareness and Response, Second Edition*, CRC Press, 2016; or D. M. Gerstein, *Bioterror in the 21st Century: Emerging Threats in a New Global Environment*, Annapolis, MD: Naval Institute Press, 2009 or G. Koblentz, *Living Weapons: Biological Warfare and International Security*, Ithaca, NY: Cornell University Press, 2009 or A. Wenger and R. Wollenmann (Eds.), *Bioterrorism: Confronting a Complex Threat*, Lynnie Rienner Pub, 2007 and the Australia Group *Common Control List Handbook, Volume II: Biological Weapons-Related Common Control Lists*, 2017.

[37] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 13, International Conventions and Agreements, 2014, p. 1.

[38] available at: http://www.health.gov.au/ssba#what's

[39] Australian Government Department of Health, Security Sensitive Biological Agent (SSBA) Standards, 2013, p. 7.

[40] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 2, About Us, 2014, p. 1.

[41] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 1, Overview, 2014, p. 2.

requirements of biological agents of security concern, together with the necessary education and awareness raising activities.[42] 'The controls apply to an entity or facility that handles SSBAs and is not an exempt entity.'[43] The system is based upon a two-tiered list of *Security Sensitive Biological Agents (SSBA)* – posing the highest (Tier 1) or a high (Tier 2) biosecurity risk – and 'requires entities and facilities to comply with a range of control and reporting requirements'[44]. This regulatory Scheme - building upon the *respective Australian Biological and Toxins Weapons Convention* and the *UN Security Council Resolution 1540* - provides the legislative framework for managing the security of SSBAs.[45] The *SSBA Regulatory Scheme* includes the *National Health Security Act 2007, the National Health Security Regulations 2008, the SSBA Standards, the National Register of Security Sensitive Biological Agents*, registration and reporting processes, an inspection program and an education and awareness raising campaign.[46] The concept is based upon risk management principles that aim to balance counter-terrorism concerns and the interests of the regulated community, maintaining a full access to the legitimate users[47]. The *SSBA list* has been developed in accordance with the following three prerequisites. First, the intelligence community measures the level of terrorist or criminal groups' interest in acquiring biological agents.[48] Second, it takes into account the impact of the biological agent, 'including factors such as morbidity, transmissibility, economic impact and the ease of treatment'[49]. And third, it considers the feasibility of the use of a biological agent, in relation to its availability, ease of production, and dissemination.[50] To adapt to the changes in the aforementioned principles, the list of SSBAs are regulatory

[42] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 1, Overview, 2014, p. 1.
[43] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 4, Execptions, 2014, p. 1.
[44] National Counter Terrorism Plan, 3rd Edition, 2012, Point 80.
[45] available at: http://www.health.gov.au/ssba#what's
[46] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 2, About Us, 2014, p. 1.
[47] available at: http://www.health.gov.au/ssba#what's
[48] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 5, List of Security Sensitive Biological Agents, 2014, p. 1.
[49] *Ibid.*
[50] *Ibid.*

revised.[51] The first comprehensive review of 2015 reassessed the security risks of biological agents, and as a result of this analysis, Salmonella Typhi and Vibrio cholerae have been removed from the list.[52]

Under Part 3 of the *National Health Security Act 2007,* the *Security Sensitive Biological Agent Standards* sets the physical, personnel, transport, information management, inactivation and decontamination security requirements for non-exempt entities when handling SSBAs.[53] *SSBA Guidelines* have been developed to support the *SSBA Regulatory Scheme*, by providing information to entities, facilities and individuals about special security-related aspects of handling SSBAs, such as the registered and non-registered facilities reporting requirements, and defining loss and theft of SSBAs or SSBAs in the natural environment.[54] Additionally, *SSBA factsheets* foster the education and awareness of the regulative framework.[55] In accordance with the inspection program, all facilities are evaluated by SSBA inspectors on a regular basis after an initial inspection, which constitutes a comprehensive examination covering all parts of the SSBA standards. In addition, the *SSBA Regulatory Scheme* has introduced spot checks and desktop inspections. Spot checks are designed for routine monitoring, while desktop inspections are 'paper-based assessments of the facilities'[56] that comply with SSBA Standards' without on-site activities.

As mentioned with respect to chemicals, the Australian Customs and Border Protection Service is responsible for the security and integrity of Australian borders. It works in close collaboration with the Australian Federal Police, Biosecurity, the Department of Immigration and the Department of Defence, 'to detect and deter unlawful movement of goods and people

[51] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 5, List of Security Sensitive Biological Agents, 2014, p. 3.
[52] available at: http://www.health.gov.au/internet/main/publishing.nsf/Content/ssba-review.htm
[53] Australian Government Department of Health and Ageing, Security Sensitive Biological Agent (SSBA) Standards, 2013, p. 3.
[54] available at: http://www.health.gov.au/internet/main/publishing.nsf/Content/ssba-guidelines.htm
[55] available at: http://www.health.gov.au/internet/main/publishing.nsf/Content/ssba-factsheets.htm
[56] available at: http://www.health.gov.au/ssba#what's

across the border'[57]. The import and export of certain goods of concern are controlled by imposing absolute prohibitions or restrictions. Biosecurity Australia conducts science-based risk assessments and provides quarantine policy advice to protect Australia's animal and plant health status and natural environment. In the same vein, *Regulation 13E of Customs (Prohibited Exports) Regulations 1958* and the *WMD Act 1995* enforces export controls on weapons-usable materials.[58]

Conclusions

Counter strategies place the emphasis on the technicalities related to biothreats. The constantly evolving technological advancements require ongoing vigilance in terms of regulating the emerging new biotechnologies.[59] Taking into account the rapid pace of advances in the proliferation of biotechnologies, it would be more practicable to address the motivations – instead of the capabilities - of criminals, as well as the deepening of our understanding with regard to the psychological factors that influence whether or not criminals resort to biowarfare[60]. As noted earlier, modern biotechnological innovations and the willingness or intent of the criminal to apply available developments should also be taken into consideration when assessing the criminal potential for engaging in these advancements.[61] In the same vein, the ever-evolving innovative technological advancements will not necessarily be adapted by a certain terrorist or extremist group. Understanding the dynamic behind terrorist weapon adoption and exploring their decision-making processes'

[57] Council of Australian Governments, Australia's Counter-Terrorism Strategy, Strengthening Our Resilience, 2015, p. 12.
[58] Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, Fact Sheet 12, Domestic Legislation, 2014, p. 3.
[59] Note: In this regard, the 2*017 EU CBRN Action Plan* indicates biohacking[59] as a field where further research is necessary, in: COM (2017) 610 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, p. 15.
[60] Gerstein, *Bioterror in the 21st Century: Emerging Threats in a New Global Environment*, Annapolis, MD: Naval Institute Press, 2009, p. 205., 150.
[61] Gregory D. Koblentz, *Living Weapons: Biological Warfare and International Security*, Ithaca, NY: Cornell University Press, 2009.

technological and organizational mechanisms would assist policy makers in distinguishing violent non-state actors, who will and will not embrace the opportunities offered by technological innovations.[62]

To eliminate the possibility of biotechnology-related scientific advancements falling into malicious hands, governments aim to restrict the publication of these scientific papers.[63] It needs to be highlighted, however, that 'any government attempt to keep the existence of emerging technology secret is unlikely to work and, in fact, may be counterproductive in the sense of attracting terrorists' attention by lending the technology the allure of the forbidden'[64].

Dual-use biological agents pose real challenges to the security-related perspective. To address the anomalies around this legislation, what constitutes the legitimate and the illegitimate use should be clarified, thereby making a clear distinction between these categories and thus eliminating the criminal, unauthorized use of these biological agents.[65] In terms of the worries around gene synthesis, monitoring the use of these specific pieces of equipment together with the facilities and employers who get access to them, might offer a far more 'promising avenue'[66]. These regulatory mechanisms should entail licensing, registration, surveillance of the use of gene-synthesis equipment and data mining provisions on individuals or legal persons who intend to get access to biotechnologies of concern.[67]

5.3. Development of the biological weapon

[62] Gary A. Ackerman, 2014, p. 2.
[63] Benjamin Wittes, *Innovation's Darker Future: Biosecurity, Technologies of Mass Empowerment, and the Constitution*, in R. D. Howard and J. J. F. Forest (Eds.), *Weapons of Mass Destruction and Terrorism 2nd Edition*, New York: McGraw Hill, 2012, p. 166.
[64] Gary A. Ackerman, 2014, p. 248.
[65] Jeffrey M. Bale and Gary A. Ackerman, *Profiling the WMD Terrorist Threat*, in Stephen M. Maurer, *WMD Terrorism: Science and Policy Choices*, Cambridge, MA: MIT Press, 2009, p. 30-31.
[66] Benjamin Wittes, 2012, p. 166.
[67] *Ibid.*, p. 168-169.

Both the respective EU-level and Australian provisions – with regard to the transport of the acquired material as well as the development of the device – concern all four strands of CBRN terrorism and have been mentioned in the previous part of this thesis. Here the analysis aims to focus on measures designed to counter the bioterrorism-related threat.

As noted earlier in the chemical section, there are numerous indicators during the development phase of a bioattack, however they obviously differ from the ones mentioned previously. Besides the already cited warning indicators, a sudden or unexplained illness in the surrounding animal or human population, the modification of premises for experimenting, as well as the theft or loss of equipment required for constructing a biological weapon, should all receive elevated attention in the awareness-raising campaigns designed for developing vigilant public eyes.

5.4. Execution of the biological attack

Generally speaking, it is easier and more obvious to identify a chemical incident, for instance, because of the smell emerging after a chemical attack. In case of a radiological incident, the radiation can be measured by special devices. In this sense, however, it is particularly challenging to identify a biological agent. Usually there is no smell or odor after a biological incident. The biological agent cannot be detected by the naked eye. The symptoms of infection can only be identified some hours after the incident.[68] It goes without saying that counter policies need to address this obstacle.

European-level counter provisions

[68] What are biological and Toxin Weapons, The United Nations Office at Geneva, available at: https://www.unog.ch/80256EE600585943/(httpPages)/29B727532FECBE96C12571860035A6DB?OpenDocument

As the EU regulation on enhancing the security of public spaces[69] points out, the capacity to detect CBRN materials requires further research. There are research grants for improving the detection capacities which therefore ensure a more effective consequence-management process[70]. Early warning systems similar to the BioWatch program should also be taken into consideration. This concept is about deploying large numbers of air samplers in metropolitan cities 'to detect a limited number of biological threat agents of critical concern'[71] that have been intentionally released into the air.

Australian counter provisions

The definition of a chemical weapon - put forward in the *Chemical Weapon Guidelines for Crowded Places* - extends to biological toxins. Since these guidelines have already been interpreted in the chemical scenario, the same implications apply for this section.

Conclusions

Effective identification of the released biological agent requires detection equipment with high-sensitivity to enable a quick and accurate discrimination between 'biological threat agents and nonpathogenic, naturally occurring biological organisms'[72]. Detection should firstly have airsampling capabilities in relation to aerosolized release which is the most common type of dissemination. Aerosolized biological agents, however, will soon settle onto other surfaces[73], therefore specific detection equipment facilitating the sampling of these

[69] COM (2017) 612 final, p. 4.
[70] Note: such as TWOBIAS - a two-stage rapid biological surveillance and alarm system for airborne threats - and BIO-PROTECT – an ionization-based detector of airborne bio-agents, viruses and toxins for fast-alert and identification (Security of the Citizens, European Commission project catalogue, available at: file:///C:/Users/petho/Downloads/SRcatalogueSecurityofthecitizens_6900.pdf)
[71] Ronald J. Kendall, Stephen M. Presley and Seshadri S. Ramkumar (Eds.), *New Developments of Biological and Chemical Terrorism Countermeasures*, CRC Press, 2016, p. 12.
[72] *Ibid.*, p. 10.
[73] *Ibid.*, p. 10-11.

surfaces is also necessary[74]. Moreover, such sampling devices must be able to identify multiple types of biological agents, not only a certain kind of biological threat pathogen.[75] Meanwhile, as Gerstein argues, 'instead of attempting to have sensors that identify the pathogen'[76], differences in the air quality should be measured to detect possible anomalies.

[74] A. A. Fatah, R. D. Arcilesi Jr., T. Chekol, C. H. Lattin, O. W. Sadik and A. O. Aluoch, *Guideline for the selection of biological agent detection equipment for emergency first responders, 2nd Edition*, US Department of Homeland Security, Washington, DC, 2007.
[75] *Ibid.*
[76] Gerstein, 2009, p. 204.

PART IV

Chapter Six

Conclusions

This concluding discussion summarizes the implications of the chapters and outlines areas where academic research could refine and improve policy efforts to prevent or disrupt such malicious attacks. The conclusion aims to underline the crucial need for an academic approach in conjunction with practical policy perspectives on CB terrorism.

6.1. Summary of the results

The analysis of plausible scenarios has presented the complexity that national authorities need to tackle when countering malicious criminals who attempt to acquire, construct or use chemical or biological weapons. This thesis has introduced a novel perspective based on an examination of the respective EU-level and Australian counter CB policies. The discussion has taken a retrospective approach from the emergence of a hypothesized terrorist attack where chemical or biological agents are involved and has guided the reader along the phases of perpetration. The analysis has attempted to identify unregulated or insufficiently regulated areas of the aforementioned counter strategies and has suggested where policy gaps can be addressed by the inclusion of academic considerations.

Concerning the first crucial step towards mounting a CB attack, regulative provisions on the acquisition of knowledge about potential chemical or biological agents show definitional anomalies. These early signs are insufficiently or rather indirectly addressed by the respective legislations. More importantly, such provisions leave the interpretation of 'suspicious interactions' on those who are in the best position to identify these warning indicators. Counter policies should apply proactive, instead of the previous reactive attitudes and improve the anticipation of CB-terrorism related threats. Therefore, there is a need for better understanding the actor(s) behind such malevolent endeavors and take into consideration not only the capabilities, but the motives together with other influencing

factors. In a similar vein, dual-use technologies should be addressed from a different angle. Instead of only controlling the spread of certain technologies, criminal entities' motivations should also be investigated.

In terms of the acquisition of potential chemical or biological components, special provisions on high-risk weapons-usable materials together with awareness programs and self-regulation in the respective sectors aim to ensure a heightened level of security. However, there is still no comprehensive regulation on materials of security concern and the focus of the existing norms is still on safety instead of security. To eliminate the revealed policy gaps, academic discussions on previous insider threat-related precedents could elucidate the root causes of the past failures and would thereby help establish the vigilant culture that would be necessary in these realms.

In terms of the development phase of malicious CB weapons, it is important to note that hazardous chemical and biological materials are particularly vulnerable when in transit. In the similar vein, while raising public awareness about potential terrorist endeavors is an important pillar of counter strategies, these efforts address only the crisis management of such incidents, and do not imply guidelines on suspicious indicators that may help detect the development of malevolent devices. There is a need to establish responsible citizen-profiles and make sure that members of the public not only identify these warning signs but will also report them to the national authorities.

Detecting criminal efforts in the final phase draws attention to the importance of engaging with the general public as representing a remarkable early warning network. Accordingly, available guidelines aim to mitigate the consequences of a terrorist attack in open or crowded public spaces. The Australian counter provisions have already set a prominent role for the community in terms of identifying radicalized individuals, although further efforts are necessary to raise public awareness about the suspicious indicators and utilize that members of the community are in the best position to detect warning individuals around them.

In the light of this, the research's three main recommendations are:

- To improve the anticipation of CB-terrorism related threats, intelligence and law enforcement agencies are to better understand the actor(s) behind these deceitful endeavours and accordingly consider the capabilities, motives and other influencing factors of criminal entities. This would also facilitate a more effective legislative approach in terms of the concerns of dual-use technologies.
- By providing insightful analyses of past incidents where insiders compromised the safety of hazardous CB agents, academic discussions would shed light on those loopholes that undermine the necessary elevated level of security around these materials.
- Having acknowledged that the general public plays a remarkable role in detecting the indicators of these malicious endeavours, public awareness raising campaigns should be extended to the potential early warning signs during the development phase of a CB-terrorist incident, and not only concern the crisis management of the attacks.

6.2. Implications

Expertise in the field of CB terrorism is spread across different domains, such as government, academic and private stakeholders. EU-level endeavors intend to bring these 'multidisciplinary and geographically spread pool of experts and practitioners'[1] together and combine their experience to identify those areas where further research is necessary.[2] While both academia and policy discuss the risks of CB terrorism and make reasonable efforts to detect criminal purposes, there is little interaction between these two realms. EU documents on CBRN-related counter provisions mention strategic academic contributions only with

[1] Policy Department for Citizens' Rights and Constitutional Affairs, 'The European Union's Policies on Counter-Terrorism, Relevance, Coherence and Effectiveness', 2017, p. 19, available at: file:///C:/Users/petho/Desktop/MRES%20PROJECT/2/EU%20CBRN/IPOL_STU(2017)583124_EN.pdf
[2] COM (2017) 610 final, p. 12.

reference to pre-9/11 assumptions[3], referring to the widespread consensus that terrorists are not likely to engage in unconventional weaponry.

In the European Parliament's briefing[4], Hoffman, Ackerman and Asal are cited to establish the context for the threat of CBRN terrorism. At the same time, the European Commission explicitly calls upon academia – together with the Member States industry and other stakeholders – 'to work together to pinpoint and define the needs that CBRN-E research should meet'[5]. As the Progress Report on the EU Action Plan in 2012 concluded 'further work and a structured approach' is necessary for enhancing connections with for example the academia.[6] With regard to the implementation of the respective EU research projects, academia and RD institutions face a considerable dominance by the EU defence industry.[7] The evolving threat of CBRN terrorism demands an 'interdisciplinary cooperation for research enhancement'[8] between academic research and government laboratories. To cite a useful example in this regard, the Australian efforts to counter violent extremism 'have built closer relationships between Australian governments, academia and the communities'[9].

The EU Bomb Data System (EBDS) provides a platform for the timely sharing of relevant information on incidents involving explosives and CBRN materials. The European Explosive Ordnance Disposal Network (EEODN) facilitates the cooperation among CBRN experts from

[3] Brian Michael Jenkins, 'International Terrorism: A New Mode of Conflict', *International Terrorism and World Security*, London, 1975 or Water Laqueur, *Terrorism*, London, 1977, cited in SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment, p. 7.
[4] European Parliament Briefing on CBRN Terrorism: threats and the EU response, January 2015, p. 2.
[5] COM (2014) 247 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a new EU approach to the detection and mitigation of CBRN-E risks, p. 6.
[6] Progress Report on the Implementation of the EU CBRN Action Plan, 2012, p. 2.
[7] Friedrich Steinhäusler, *Gap Analysis of EU Counterterrorism Research Initiatives* in Erice International Seminars on Planetary Emergencies, 45th Session: The Role of Science in the Third Millenium, 2012, p. 1.
[8] Ronald J. Kendall, Stephen M. Presley and Seshadri S. Ramkumar, 2016, p. 171.
[9] Australian Government Department of the Prime Minister and the Cabinet, Review of Australia's Counter-Terrorism Machinery, January 2015, p. 17.

EU Member States, Europol, Interpol, Norway, Australia and the United States. The system gathers all technical intelligence with regard to occurred CBRN incidents to raise awareness of criminal capabilities as well as the applied countermeasures. Besides these incident databases, EBDS maintains several libraries and platforms for the interaction of professionals in the field.[10] Experts meet at least once a year to 'compare their respective protocols'[11]. In the form of an annual meeting, academic achievements could also be shared with the law enforcement community. This rich technical database, therefore, could be enhanced by a broader, theoretical context, allowing for a deeper understanding of the criminal trends.

6.3. Conclusion

This research has demonstrated that bridging distinct practitioner and academic standpoints on the risk of CB terrorism will bring valuable and practicable outcomes. This thesis has devised a novel approach how to bring together theoretical and practitioner standpoints to strengthen one another in the fight against chemical and biological terrorism. While the confidential nature of counter-terrorism policies hindered the holistic evaluation of these respective counter strategies, this research has given a considerable indication of the applicability and usefulness of employing academic standpoints in policy-maker approaches.

[10] 'Europe blows up', *CBRNe World*, April 2012, p. 62-63.
[11] https://www.europol.europa.eu/annual_review/2015/networks.html

Sources consulted

Cited bibliography

Ackerman Gary A. and Moran Kevin S., *Bioterrorism and Threat Assessment, Prepared for the Weapons of Mass Destruction Commission*, 2006.

Ackerman Gary A. and Pinson Lauren E., 'An Army of One: Assessing CBRN Pursuit and Use by Lone Wolves and Autonomous Cells', *Terrorism and Political Violence*, 2014, 26:1, pp. 226-245.

Ackerman Gary A. and Tamsett Jeremy (Eds.), *Jihadists and Weapons of Mass Destruction*, CRC Press, 2009.

Ackerman Gary A. et al (START National Consortium for the Study of Terrorism and Responses to Terrorism), *Profiling the CB Adversary: Motivation, Psychology and Decision-Research Brief*, 2017.

Ackerman Gary A., 'Defining knowledge gaps within CBRN terrorism research', in Magnus Ranstorp and Magnus Normark (Eds.), *Unconventional Weapons and International Terrorism, Challenges and new approaches*, London and New York: Routledge, 2009.

Ackerman Gary A., 'WMD Terrorism Research: Whereto from Here?' in The Forum: Nonstate Actors, Terrorism, and Weapons of Mass Destruction', *International Studies Review*, 2005:7, pp. 140-143.

Ackerman Gary A., Bale Jeffrey M., Asal Victor, Rethemeyer R. Karl, Murdie Amanda, Johns Mila, and Binder Markus K., *Anatomizing Chemical and Biological Non-State Adversaries: Identifying the Adversary*, College Park, MD.: National Consortium for the Study of Terrorism and Responses to Terrorism, 2014.

Ackerman Gary A., *Defining knowledge gaps within CBRN terrorism research*, in Magnus Ranstorp and Magnus Normark (Eds.), *Unconventional Weapons and International Terrorism, Challenges and new approaches*, UK and USA, Routledge, 2009.

Ackerman Gary A., *More Bang for the Buck: Examining the Determinants of Terrorist Adoption of New Weapons Technologies*, London, UK: King's College, 2014, available at: https://kclpure.kcl.ac.uk/portal/en/theses/more-bang-for-the-buckexamining-the-determinants-of-terrorist-adoption-of-new-weaponstechnologies(992afd2a-bdeb-46b2-8cb7-cd29d77ebd64).html

Ackerman Gary A., *WMD Terrorism Research* in J. Horgan and K. Braddock (Eds.), *Terrorism Studies: A Reader*, New York: Routledge, 2011.

Anestidou Lida A. and Labov Jay B., *Immersing students in responsible science through active learning pedagogies: lessons from education institutes in the MENA region* in Simon Whitby, Tatyana Novossiolova, Gerald Walther and Malcolm Dando (Eds.), *Preventing Biological Threats: What You Can Do*, Bradford: Bradford Disarmament Research Centre, 2015, p. 388-404.

Anthony Ian and Grip Lina, *Strengthening the European Union's Future Approach to WMD Non-proliferation*, SIPRI Policy Paper No. 37, 2013.

Asal Victor H. and Rethemeyer R. Karl, 'Islamist Use and Pursuit of CBRN Terrorism', in Gary Ackerman and Jeremy Tamsett (Eds.), *Jihadists and Weapons of Mass Destruction*, CRC Press, 2009.

Asal Victor H., Ackerman Gary A. and Rethemeyer R. Karl, 'Connections Can be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Weapons', *Studies in Conflict and Terrorism*, 2012, 35:3, pp. 229-254.

Bale Jeffrey M., *The Darkest Sides of Politics, Volume II, State Terrorism, "Weapons of Mass Destruction", Religious Extremism and Organized Crime*, New York: Routledge, 2018.

Bale Jeffrey M. and Ackerman Gary A., *Profiling the WMD Terrorist Threat*, in Maurer Stephen M., *WMD Terrorism: Science and Policy Choices*, Cambridge, MA: MIT Press, 2009.

Ben Ouagrham-Gormley Sonia, *Barriers to Bioweapons, The Challenges of Expertise and Organization for Weapons Development*, Cornell University Press: Ithaca and London, 2014.

Bruggen Koos van der, *Biosecurity challenges in the 21st century: the case of gain-of-function experiments* in Simon Whitby, Tatyana Novossiolova, Gerald Walther and Malcolm Dando (Eds.), *Preventing Biological Threats: What You Can Do*, Bradford: Bradford Disarmament Research Centre, 2015.

Bunn Matthew and Sagan Scott D. (Eds.), *Insider Threats*, Ithaca and London: Cornell University Press, 2016.

Bunn Matthew and Sagan Scott D., *A Worst Practices Guide to Insider Threats*, in Matthew Bunn and Scott D. Sagan (Eds.), *Insider Threats*, Ithaca and London: Cornell University Press, 2016.

Cole Benjamin, *The Changing Face of Terrorism: How Real is the Threat from Biological, Chemical and Nuclear Weapons?*, New York: I. B. Tauris, 2011.

Cruickshank Paul, 'A View the CT Foxhole: An Interview with Richard Walton, Head, Counter Terrorism Command, London Metropolitan Police', *CTC Sentinel*, January 2016.

Davies, in Schmid Alex P. (Ed.), *The Routledge Handbook of Terrorism Research*, London and New York: Routledge, 2011.

Dishman Chris, 'Understanding Perspectives on WMD and Why They Are Important', *Studies in Conflict and Terrorism*, 2001:24, pp. 303-313.

Dolnik Adam, 'Conducting Field Research on Terrorism: a Brief Primer', *Perspectives on Terrorism*, 2011, Volume 5, Issue 2.

Ellis P. D., 'Lone Wolfe Terrorism and Weapons of Mass Destruction: An Examination of Capabilities and Countermeasures', *Terrorism and Political Violence*, 2014, 26:1, pp. 211-225.

Endregard Monica, Breivik Hanne, Schultz Heireng Hege, Enger Elin, Sandrup Therese and Kelly Dominic, *D2.1 Scenario template, existing CBRN scenarios and historical incidents*, PRACTICE WP2 Deliverable, 2011.

Fatah A. A., Arcilesi Jr. R. D., Chekol T., Lattin C. H., Sadik O. W. and Aluoch A. O., *Guideline for the selection of biological agent detection equipment for emergency first responders, 2nd Edition*, US Department of Homeland Security, Washington, DC, 2007.

Forest James JF, 'Framework for Analyzing the Future Threat of WMD Terrorism', *Journal of Strategic Security*, 2012:4.

Fredholm M. (Ed.), *Understanding Lone Actor Terrorism: Past Experience, Future Outlook, and Response Strategies*, New York, NY: Routledge, 2016.

Friedman Thomas L., *Longitudes and Attitudes: Exploring the World After September 11*, New York: Farrar, Straus and Giroux, 2002.

Gerstein Daniel M., *Bioterror in the 21st Century: Emerging Threats in a New Global Environment*, Annapolis, MD: Naval Institute Press, 2009.

Gillis Melissa, *Disarmament – A Basic Guide Fourth Edition*, available at: https://www.un.org/disarmament/wp-content/uploads/2017/09/Basic-Guide-4th-Edition-web.pdf

Gohel M. J., in Schmid Alex P. (Ed.), *The Routledge Handbook of Terrorism Research*, London and New York: Routledge, 2011.

Gurr Ted Robert, *Which Minorities Might Use Weapons of Mass Destruction?* in T*he Forum: Nonstate Actors, Terrorism, and Weapons of Mass Destruction*, in *International Studies Review*, 2005:7.

Hayden Nancy K., *Terrifying landscapes Understanding motivations of non-state actors to acquire and/or use weapons of mass destruction*, in Magnus Ranstorp and Magnus Normark (Eds.), *Unconventional Weapons and International Terrorism, Challenges and new approaches*, UK and USA, Routledge, 2009.

Heireng H. S., Endregard M., Breivik H., Erikkson H., Fonteyne P. A., Kelly D. and Sandrup T., 'The development and use of CBRN scenarios for emergency preparedness analyses', Conference paper, 11th International Symposium on Protection Against Chemical and Biological Warfare Agents, 3-5 June, 2013, Stockholm.

Hoffman Bruce, *The Debate Over the Future Use of Chemical, Biological, and Radiological, and Nuclear Weapons* in *Hype or Reality: The "New Terrorism" and Mass Casualty Attacks*, Alexandria, VA: Free Hand Press, 2000.

Hoffman Bruce, *Change and Continuity in Terrorism*, in Bruce Hoffman and Anders Strindberg (Eds.), *Terrorism and Beyond: A 21st Century Perspective*, Routledge Library Editions, Terrorism and Insurgency, Routledge, London and New York, 2015.

Howard Russell D., 'Preemptive Military Doctrine: No Other Choice' in James J. Forest and Russell D. Howard (Eds.), *Weapons of Mass Destruction and Terrorism Second Edition*, New York: McGraw-Hill, 2012.

Hummel Kristina, 'A View from the CT Foxhole: Edward You, FBI Weapons of Mass Destruction Directorate, Biological Countermeasures Unit', *CTCT Sentinel*, August 2017.

Hummel Stephen, 'The Islamic State and WMD: Assessing the Future Threat', *CTC Sentinel*, 2016, avaliable at: https://ctc.usma.edu/posts/the-islamic-state-and-wmd-assessing-the-future-threat

Hype or Reality: The "New Terrorism" and Mass Casualty Attacks, Alexandria, VA: Free Hand Press, Chemical and Biological Arms Control Institute, 2000.

JASON The Mitre Corporation, *Rare Events*, McLean, VA: MITRE Corporation, 2007.

Jenkins Brian Michael, *Will Terrorists Go Nuclear?*, Santa Monica, CA: RAND, 1975.

Jenkins Brian, 'Terrorism and Beyond: A 21st Century Perspective', *Studies in Conflict and Terrorism*, 2001.

Jenkins Brian, *The WMD Terrorist Threat: Is There a Consensus View?*, in Brad Roberts (Ed), *Hype or Reality? The „New Terrorism" and Mass Casualty Attacks*, Alexandria, VA: Chemical and Biological Arms Control Institute, 2000.

Kendall Ronald J., Presley Stephen M. and Ramkumar Seshadri S. (Eds.), *New Developments of Biological and Chemical Terrorism Countermeasures*, CRC Press, 2016.

King Faiza Patel, 'Implementing the Chemical Weapons Convention: A comparative case study of the legislation of Australia and France', in Ramesh Chandra Thakur and Ere Haru (Eds.), 'The Chemical Weapons Convention: Implementation, Challenges and Opportunities', Tokyo: United Nations University Press, 2006.

Kobentz Gregory D., 'Predicting Peril or the Peril of Prediction? Assessing the Risk of CBRN Terrorism', *Terrorism and Political Violence*, 2011, 23:4, p. 501-520.

Koblentz Gregory D., *Living Weapons: Biological Warfare and International Security*, Ithaca, NY: Cornell University Press, 2009.

Kortunov Andrey, 'Are Chemical Weapons Getting More Dangerous Than Nuclear?', *American Herald Tribune*, January, 30, 2018, available at: https://ahtribune.com/world/2118-chemical-weapons-nuclear.html

Mackenzie Donald and Spinardi Graham, 'Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons', *American Journal of Sociology*, 101:1, 1995, pp. 44-99.

Maurer Stephen M., *WMD Terrorism: Science and Policy Choices*, Cambridge, MA: MIT Press, 2009.

Mauroni Albert J., *A Counter-WMD Strategy for the Future*, in James J. Forest and Russell D. Howard (Eds.), *Weapons of Mass Destruction and Terrorism Second Edition*, New York: McGraw-Hill, 2012.

Meer Adriaan Van Der, *Promoting a Scientist's Duty of Care 4.0.*, May, 2018.

NATIBO, "Biological Detection System Technologies Technology and Industrial Base Study: A Primer on Biological Detection Technologies," in *Book Biological Detection System Technologies Technology and Industrial Base Study: A Primer on Biological Detection Technologies*, (City: North American Technology and Industrial Base Organization, 2001)

National Consortium for the Study of Terrorism and Responses to Terrorism (START) project on Profiling the CB Adversary: Motivation, Psychology and Decision, 2017.

Nehorayoff Andrea A., Ash Benjamin and Smith Daniel S., 'Aum Shinrikyo's Nuclear and Chemical Weapons Development Efforts', *Journal of Strategic Security* 2016:1, available at: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1510&context=jss.

Ouagrham-Gormley Sonia Ben, 'Barriers to Bioweapons: Intangible Obstacles to Proliferation', *International Security*, 2012, 36:4, pp. 80-114.

Parachini John V., 'Comparing Motives and Outcomes of Mass Casualty Terrorism Involving Conventional and Unconventional Weapons', in Bruce Hoffman and Anders Strindberg (Eds.), *Terrorism and Beyond: A 21st Century Perspective*, Routledge Library Editions, Terrorism and Insurgency, Routledge, London and New York, 2015.

Paturej Krzysztov and Guanglian Pang, *Meeting Growing Threats of Misuse of Toxic Chemicals: Building a Global Chemical Safety and Security Architecture and Promoting International Cooperation*, in: M. Martellini, A. Malizia (Eds.), *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges, Terrorism, Security, and Computation*, Springer, 2017.

Pichtel J., *Terrorism and WMDs: Awareness and Response, Second Edition*, CRC Press, 2016.

Post Jerrold M., *Prospects for Nuclear Terrorism: Psychological Motivations and Constraints* in Paul Leventhal and Yonah Alexander (Eds), *Preventing Nuclear Terrorism*, Lexington, MA: D. C. Heath, 1987.

Post Jerrold, Sprinzak Ehud and Denny Laurita, 'Terrorists in Their Own Words: Interviews with Thirty-Five Incarcerated Middle Eastern Terrorists', *Terrorism and Political Violence*, 2003:15.

Ranstorp Magnus, 'Terrorism in the Name of Religion', *Journal of International Affairs*, 1996:1, pp. 41-62.

Rapoport David C., 'Terrorism and Weapons of the Apocalypse', in *National Security Studies Quarterly* 5:3, 1999.

Reinarez Fernando and García-Calvo Carola, '"Spaniards, You Are Going To Suffer": The Inside Story of the August, 2017 Attacks in Barcelona and Cambrils', in *CTC Sentinel*, 11:1, January, 2018.

Ruggiero Aino and Vos Marita, 'Communication Challenges in CBRN Terrorism Crises: Expert Perceptions', in *Journal of Contingencies and Crisis Management*, 2015, 23:3, p. 138-148.

Schmid Alex P. and Jongman Albert, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Oxford: North Holland, 1988.

Schmid Alex P. (Ed.), *The Routledge Handbook of Terrorism Research*, London and New York: Routledge, 2011.

Schmid Alex P., 'Statistics on Terrorism, The Challenge of Measuring Trends in Global Terrorism', *UNODA Forum on Crime and Society*, 2004, Volume 4, Issue 1, 2.

Schmid Alex P., 'Terrorism and the use of weapons of mass destruction: From where the risk?', *Terrorism and Political Violence*, 1993, 11:4, p. 106-132.

Silke Andrew, 'Research on Terrorism', *Terrorism Informatics*, 2008, Volume 18.

Simon Steven and Benjamin Daniel, 'America and the New terrorism', *Survival*, 2000, 42:1, p. 59-75.

Sinai Joshua and Forest James J. F., *Threat Convergence, A Framework for Analyzing the Potential for WMD Terrorism*, in James J. Forest and Russell D. Howard (Eds.), *Weapons of Mass Destruction and Terrorism Second Edition*, New York: McGraw-Hill, 2012.

Sinai Joshua, 'Forecasting Terrorists' Likelihood to Embark on „Conventional" to CBRN Warfare', in The Forum: Nonstate Actors, Terrorism, and Weapons of Mass Destruction', in *International Studies Review*, 2005:7.

Slater Robert O. and Stohl Michael, 'Introduction: Towards a Better Understanding of International Terrorism', *Current Perspectives on International Terrorism*, MacMillan, London, 1988.

Smith Brent L., Damphousse Kelly R. and Roberts Paxton, *Pre-Incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct*, May 2006. available at: https://www.hsdl.org/?abstract&did=464263

Sprinzak Ehud, 'The great superterrorism scare', *Foreign Policy*, 1998:112, p. 110-124.

Steinbruner John, 'Terrorism: Practical Distinctions and Research Priorities', in The Forum: Nonstate Actors, Terrorism, and Weapons of Mass Destruction', *International Studies Review*, 2005:7.

Steinhäusler Friedrich, *Gap Analysis of EU Counterterrorism Research Initiatives* in Erice International Seminars on Planetary Emergencies, 45th Session: The Role of Science in the Third Millenium, 2012.

Stenersen Anne, *Al-Qaeda's thinking on CBRN* in Magnus Ranstorp and Magnus Normark (Eds.), *Unconventional Weapons and International Terrorism: Challenges and New Approaches*, New York: Routledge, 2009.

Stohl Cynthia and Stohl Michael, *Approaching Global Organizing*, London: SAGE Publications, 2005.

Trujillo Horacio R. and Jackson Brian A., 'Identifying and Exploiting Group Learning Patterns for Counterterrorism', *Terrorism Informatics, Knowledge Management and Data Mining for Homeland Security*, 2008.

Trujillo Horacio R. and Jackson Brian A., 'Identifying and Exploiting Group Learning Patterns for Counterterrorism', *Terrorism Informatics, Knowledge Management and Data Mining for Homeland Security*, 2008.

Volders Brecht and Sauer Tom, *Introduction*, in Brecht Volders and Tom Sauer (Eds,): *Nuclear Terrorism: Countering the Threat.* Abingdon-on-Thames: Routledge, 2016.

Volders Brecht, *Assessing the likelihood of nuclear terrorism*, in Brecht Volders and Tom Sauer (Eds.) *Nuclear Terrorism: Countering the Threat.* Abingdon-on-Thames: Routledge, 2016, p. 12-26.

Wenger A. and Wollenmann R. (Eds.), *Bioterrorism: Confronting a Complex Threat*, Lynnie Rienner Pub, 2007.

Whitby Simon, Tatyana Novossiolova, Gerald Walther and Malcolm Dando (Eds.), *Preventing Biological Threats: What You Can Do*, Bradford: Bradford Disarmament Research Centre, 2015.

Wittes Benjamin, *Innovation's Darker Future: Biosecurity, Technologies of Mass Empowerment, and the Constitution*, in R. D. Howard and J. J. F. Forest (Eds.), *Weapons of Mass Destruction and Terrorism 2nd Edition*, New York: McGraw Hill, 2012.

Zalesny Mary D., Whitney Paul, White Amanda, Plasse Theodore R., and Grundy Michael T., 'A Conceptual Model to Identify Intent to Use Chemical-Biological Weapons', *Journal of Strategic Security* 10, no. 3, 2017, p. 54-86.

Zammit Andrew, 'Australian Jihadism in the Age of the Islamic State', *CTC Sentinel*, March 2017.

Zammit Andrew, 'New Developments in the Islamic State's External Operations: The 2017 Sydney Plane Plot', *CTC Sentinel*,10:9, October, 2017.

Zanders Jean Pascal, *Internal Dynamics of a Terrorist Entity Acquiring Biological and Chemical Weapons* in *Nuclear Terrorism: Countering the Threat.* Abingdon-on-Thames: Routledge, 2016, p. 26-55.

Zegart Amy B., *The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies*, in Matthew Bunn and Scott D. Sagan (Eds.), *Insider Threats*, Ithaca and London: Cornell University Press, 2016.

Cited policy papers

(19) Regulation (EC) No 1907/2006 of the European Parliament and of the Council

1051/2013 Regulation of the European Parliament and of the Council of 22 October 2013 amending Regulation (EC) No 562/2006 in order to provide for common rules on the temporary reintroduction of border control at internal borders in exceptional circumstances

12653/10 ADD 1 – Commission Staff Working Paper – Taking Stock of EU Counter-Terrorism Measures, Accompanying document to the Communication from the Commission to the European Parliament and the Council, The EU Counter-Terrorism Policy: main achievements and future challenges, 2010.

15505/1/09 REV 1 – Council conclusions on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union – an EU CBRN Action Plan, 2009.

15708/03, The European Council, Fight against the proliferation of weapons of mass destruction, 2003.

15894/1/10, 29 November 2010, Council of the European Union, 'EU Counterterrorism Strategy – Discussion Paper'

17172/08 Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 2008.

An Agreement on Australia's National Arrangement of Security Risks Associated with Chemicals, 2 October 2008.

An Australian Government Initiative, Chemicals of Security Concern

ASIO Annual Report, 2016-2017.

Attorney General's Department, Decision Regulation Impact Statement, Chemical Security: Toxic Chemicals of Security Concern, November 2014.

Australia Group *Common Control List Handbook, Volume II: Biological Weapons-Related Common Control Lists*, 2017.

Australia Group, Common Control List Handbook, Volume II: Biological Weapons-Related Common Control Lists, Revision 3, February 2017.

Australia New-Zealand Counter-Terrorism Committee, National Counter Terrorism Plan, 4th Edition, 2017.

Australia's Strategy for Protecting Crowded Places from Terrorism, 2017.

Australian Government Department of Health and Ageing, Security Sensitive Biological Agent (SSBA) Standards, 2013.

Australian Government Department of Health, Security Sensitive Biological Agents Regulatory Scheme, International Conventions and Agreements, 2014.

Australian Government Department of the Prime Minister and the Cabinet, Review of Australia's Counter-Terrorism Machinery, January 2015.

Australian Government, National Code of Practice for Chemicals of Security Concern, 2016.

Australian Government, The National Security Science and Innovation Strategy, 2009.

Australian Security Intelligence Organization, Annual Report 2016-17.

Australia-New Zealand Counter-Terrorism Committee, 'Chemical Weapon Guidelines for Crowded Places', 2017.

C (2017) 6950 final Commission Recommendation of 18.10.2017 on immediate steps to prevent misuse of explosive precursors

COM (2009) 273 final, Communication from the Commission to the European Parliament and the Council – an EU CBRN Action Plan

COM (2014) 247 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a new EU approach to the detection and mitigation of CBRN-E risks

COM (2017) 555 final, Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Tackling Illegal Content Online, Towards an enhanced responsibility on online platforms

COM (2017) 606 final, ANNEX 1 to the Proposal for a Council Decision on the conclusion, on behalf of the European Union, of the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196)

COM (2017) 607 final, ANNEX 1 to the Proposal for a Council Decision on the conclusion, on behalf of the European Union, of the Additional Protocol supplementing the Council of Europe Convention on the Prevention of Terrorism (CETS No. 217)

COM (2017) 608 final, Communication from the Commission to the European Parliament, the European Council and the Council

COM (2017) 610 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks

COM (2017) 612 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Action Plan to support the protection of public spaces

Combating Illicit Trafficking in Nuclear and other Radioactive Material, Technical Guidance, Reference Manual, IAEA Nuclear Security Series No. 6, 2007.

Council of Australian Governments, Australia's Counter-Terrorism Strategy, Strengthening Our Resilience, 2015.

Sources consulted

Directive (EU) 2017/541 of the European Parliament and of the Council on combating terrorism

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017

EU Internal Referral Unit Year One Report, 2017

European Commission Call for Tender No. HOME/2010/ISEC/PR/038-A1

European Commission President Jean-Claude Juncker, European Parliament, 12 April 2016

European Commission, Security Union, A Europe That Protects, October 2017.

European Parliament Briefing on CBRN Terrorism: threats and the EU response, January 2015.

Europol, Terrorism Situation and Trend report (TE-SAT), 2017.

Hostile Vehicle Mitigation Guidelines, Active Armed Offender Guidelines and Improvised Explosive Device Guidelines available at www.nationalsecurity.gov.au/CrowdedPlaces

Intergovernmental Agreement on Australia's National Counter-Terrorism Arrangements, 5 October 2017.

National Counter-Terrorism Committee, 'National Security Public Information Guidelines', 2010.

National Counter-terrorism Plan, 3rd Edition, 2012.

New South Wales Counter Terrorism Plan, December 2016.

New South Wales Environment Protection Authority, Review of the Environmentally Hazardous Chemicals Act 1985, Background Paper, 2003.

Policy Department for Citizens' Rights and Constitutional Affairs, 'The European Union's Policies on Counter-Terrorism, Relevance, Coherence and Effectiveness', 2017, p. 19, available at: file:///C:/Users/petho/Desktop/MRES%20PROJECT/2/EU%20CBRN/IPOL_STU(2017)583124_EN.pdf

Progress Report on the Implementation of the EU CBRN Action Plan, May 2012 (public version)

Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology

Review of Australia's Counter-Terrorism Machinery, January 2015.

SEC (2009) 791, Commission Staff Working Document Accompanying document to the Communication from the Commission to the European Parliament and the Council on Strenghtening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Impact Assessment

Stocktaking study on good practices on reporting of suspicious transactions in relation to CBRN materials, Final Report for DG Home Affairs, 2013.

The Chemical Weapons Convention, A Guide for Australian Industry Producing, Using or Trading Chemicals, 2014. available at: https://dfat.gov.au/international-relations/security/non-proliferation-disarmament-arms-control/chemical-weapons/cwc/Documents/Chemical_Weapons_A%20Guide.pdf

What are biological and Toxin Weapons, The United Nations Office at Geneva, available at: https://www.unog.ch/80256EE600585943/(httpPages)/29B727532FECBE96C12571860035A6DB?OpenDocument

World at Risk, The Report of the Commission on Prevention of WMD Proliferation and Terrorism, Vintage Books, 2008.

Cited newspaper articles

'Europe blows up', *CBRNe World*, April 2012.

'Melbourne terrorist plot: Four charged, one in custody over alleged Christmas Day attack plan', *ABC News*, 24, December 2016, available at: http://www.abc.net.au/news/2016-12-23/police-foil-alleged-christmas-day-terrorist-plot-in-melbourne/8143762

Riley Stuart and Louis Hall, 'Sydney terror plotters 'tried to blow up Etihad plane, unleash poison gas attack', *ABC News*, 4 August 2017, available at: http://www.abc.net.au/news/2017-08-04/sydney-terror-raids-police-say-plane-bomb-plot-disrupted/877375

Press release, "A primer on DarkNet marketplaces," Federal Bureau of Investigation, November 1, 2016.