

## **CBRN Threats, Counter-Terrorism, and Collective Moral Responsibility**

### **Partnerships in preventing and preparing for terrorist attacks using common-use toxic and radiological substances as weapons**

Feltes, J.

#### **DOI**

[10.4233/uuid:b4c67cd7-a5ca-4ee4-b2a5-6f61bb25f66a](https://doi.org/10.4233/uuid:b4c67cd7-a5ca-4ee4-b2a5-6f61bb25f66a)

#### **Publication date**

2021

#### **Document Version**

Final published version

#### **Citation (APA)**

Feltes, J. (2021). *CBRN Threats, Counter-Terrorism, and Collective Moral Responsibility: Partnerships in preventing and preparing for terrorist attacks using common-use toxic and radiological substances as weapons*. [Dissertation (TU Delft), Delft University of Technology]. <https://doi.org/10.4233/uuid:b4c67cd7-a5ca-4ee4-b2a5-6f61bb25f66a>

#### **Important note**

To cite this publication, please use the final published version (if applicable).  
Please check the document version above.

#### **Copyright**

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

#### **Takedown policy**

Please contact us and provide details if you believe this document breaches copyrights.  
We will remove access to the work immediately and investigate your claim.

# **CBRN Threats, Counter-Terrorism, and Collective Moral Responsibility**

**Partnerships in preventing and preparing for terrorist attacks using common-use toxic and radiological substances as weapons**

Dissertation

for the purpose of obtaining the degree of doctor

at Delft University of Technology

by the authority of the Rector Magnificus, prof.dr.ir. T.H.J.J. van der Hagen,

chair of the Board for Doctorates

to be defended publicly on

Tuesday, the 13<sup>th</sup> of July 2021 at 12:30 o'clock

by

Jonas FELTES

Master of Science in History and Philosophy of Science, Utrecht University,  
the Netherlands

born in Kamp-Lintfort, Germany

This dissertation has been approved by the promotor.

Composition of the doctoral committee:

Rector Magnificus,	chairperson
Prof.dr. S.R.M. Miller	Delft University of Technology, promotor
Prof.dr.ir. I.R. van de Poel	Delft University of Technology, promotor

.....

Independent members,

Prof.dr.mr.ir N. Doorn	Delft University of Technology
Prof.dr. C. Enemark	University of Southampton, UK
Prof.dr. M.L. Gross	University of Haifa, Israel
Dr. M. Skerker	United States Naval Academy, USA
Prof.dr. M.J. van den Hoven	Delft University of Technology, reserve member



Printed by: Gildeprint

Cover image by: Christof Grobelski (Instagram @christofgrobelski)

Copyright © 2021 Jonas Feltes

Nur die halbe Welt ist Teflon und Asbest.

*(Einstürzende Neubauten – Feurio!)*



# Summary

The terrorist use of chemical, biological, radiological, and nuclear (CBRN) weapons is a worst-case scenario for most security agencies. However, the risk of CBRN-terrorism is traditionally characterized as a so-called “high impact – low probability” threat. Academics and analysts consider it challenging for terrorists to acquire these weapons and, hence, assign a low probability to the terrorist use of impactful CBRN weapons such as nuclear devices or weaponized microorganisms.

Most researchers, however, assess the impact of a terrorist weapon solely based on its capability to physically destroy structures or harm organisms. This one-dimensional assessment rules out those toxic substances that are commonly considered CBRN-agents but only possess limited destructive capabilities. Hence, these agents are not considered a priority for most security agencies. Rather, most resources in CBRN-defense are allocated to international non-proliferation efforts and the like, whereas commonly used toxins that are openly available in hardware stores are often overlooked.

The present study focuses on three of these common-use toxins: ricin, phosphine, and americium. It will be shown that, while arguably having limited physical impact in the hands of terrorists, these and other common-use toxins exhibit characteristics that could be of high value to the strategic and tactical goals of terrorist groups. For example, attacks using phosphine

have the potential to inflict massive amounts of fear and disruption and are capable of causing political damage and damage to security institutions.

The potential to inflict substantial amounts of non-kinetic damage, as well as the availability and ease of use of these substances, need to be properly acknowledged and met with a multi-layered web of counter-measures (web of prevention) by security institutions. Hence, this thesis follows the following research question: *How can we build a functioning web of counter-measures against terrorist attacks that use common-use toxins in a manner that includes a variety of cooperative actions executed by all stakeholders who are collectively responsible for combating these attacks?*

This thesis shows in detail that the security risks posed by the terrorist use of ricin, phosphine, and americium are pressing enough to call for such a web of prevention. Furthermore, it is argued that the suggested web of prevention ought to include not only government agencies but also other stakeholders such as manufacturers and vendors of these products, the press, researchers, internet service providers, social media users, and citizens. It is argued that all of these stakeholder groups share a joint moral responsibility to combat terrorist attacks using common-use toxins. This joint moral responsibility is based on the so-called No Means to Harm (NMH) principle and can be translated into specific actions of individuals in these groups of stakeholders. These specific actions may include, for example, the reporting of suspicious purchases in hardware stores or the flagging and deletion of weapon manuals on the internet.

In a critical analysis of the current measures to combat terrorist attacks using common-use toxic substances as weapons, it is shown that most of the current cooperative measures suffer from problems that can be traced back to the inability of the stakeholder groups to identify their respective responsibilities within the web of prevention. Furthermore, it is argued that security institutions miss opportunities to operationalize the moral responsibilities of stakeholder groups such as vendors of toxin products. In this analysis, the German security infrastructure will be used as a primary example of the current architecture of and issues with these cooperative measures. The counter-measures that are discussed in this thesis can be lumped into three groups: measures against the acquisition of relevant weapon materials, measures against the acquisition of relevant weapon expertise, and measures to ensure resilience in the aftermath of an attack.

Based on this assessment, this thesis provides recommendations on how to improve the current CBRN security architecture. It is shown that the responsibilities and actions of each stakeholder group have to be defined, discussed, and coordinated by all relevant stakeholder groups jointly. In order to do so, the theoretical concept of the web of prevention has to be turned into an institutionalized web in the form of, what I refer to as, a joint center. Such a joint center gives the stakeholder groups the opportunity to (1) assess the threat, (2) define tasks and actions of each group, and (3) equip each group with the means to perform these actions in an efficacious and ethically sustainable manner.

Specifically, the groups of stakeholders that are defined in this thesis are able to communicate and coordinate actions in the suggested joint center.



Thereby, different working groups that consist of changing partnerships between the groups of stakeholders can cooperate efficaciously and assess, define, and apply measures against the acquisition of materials and knowledge to use ricin, phosphine, and americium as terrorist weapons. In addition to that, the suggested joint center also offers the opportunity to improve and coordinate measures to prepare for the aftermath of an attack using common-use toxic substances as weapons.

Beyond these specific tasks of the joint center with regard to counter-measures against the terrorist use of ricin, phosphine, and americium, this thesis also gives some general conclusions regarding counter-terrorism efforts, CBRN, and collective responsibility. It is concluded that *thinking about the roles and responsibilities of a variety of stakeholders in the fight against terrorism and understanding the mechanisms behind terrorism as a collective phenomenon can offer a framework to address CBRN terrorist threats in an efficacious and ethically sustainable way.*

In order to arrive at these specific and general conclusions, this thesis discusses the above-expressed research question in four parts: The first part is dedicated to the threat and includes discussions on the definition of terrorism, WMD and CBRN as well as a threat assessment of the impact and availability of weapons to terrorists. The second part introduces the concept of collective moral responsibility and defines and discusses the groups of stakeholders that share a moral responsibility in combatting terrorist attacks with toxic substances as weapons. The third part entails critical assessments of current cooperative measures of these groups of stakeholders to combat the acquisition of toxins and specialized knowledge by terrorists. The fourth

part combines the concepts and moral responsibilities that were defined in part two with the critical assessment of part three and gives a list of suggested measures in the web of prevention to improve the cooperative fight against this branch of terrorism. Here, the institutionalization of the web of prevention as a joint center plays a central role.

Finally, this thesis concludes with a special focus on the joint and individual responsibilities of citizens in the aftermath of terrorist attacks using common-use toxic substances as weapons. It is shown that all of us are, at least to some degree, morally obligated to help efforts to ensure resilience after such an attack.

# Samenvatting

Het gebruik van chemische, biologische, radiologische en nucleaire (CBRN) wapens door terroristen is voor de meeste veiligheidsdiensten het slechtst denkbare scenario. Het risico van CBRN-terrorisme wordt echter van oudsher gekarakteriseerd als een dreiging met grote impact en lage waarschijnlijkheid. Wetenschappers en analisten denken dat het moeilijk is voor terroristen om aan deze wapens te komen en achten het daarom weinig waarschijnlijk dat terroristen gebruik zullen maken van CBRN-wapens met grote impact, zoals kernwapens of als wapen gebruikte micro-organismen.

De meeste onderzoekers beoordelen het effect van een terroristisch wapen echter alleen op basis van zijn vermogen om bijvoorbeeld gebouwen fysiek te vernietigen of organismen schade toe te brengen. Deze eendimensionale beoordeling houdt geen rekening met toxische stoffen die algemeen als CBRN-wapens worden beschouwd, maar slechts een beperkt destructief vermogen hebben. Daarom zien de meeste veiligheidsdiensten deze stoffen niet als een prioriteit. De meeste middelen voor verdediging tegen CBRN-wapens worden besteed aan zaken als internationale non-proliferatie, terwijl algemeen gebruikte toxines die vrij verkrijgbaar zijn in bouwmarkten, vaak over het hoofd worden gezien.

In deze studie concentreren we ons op drie van deze toxines voor algemeen gebruik: ricine, fosfine en americium. We laten zien dat deze en andere soortgelijke toxines, hoewel ze in de handen van terroristen waarschijnlijk

een beperkte fysieke impact hebben, kenmerken vertonen die van grote waarde kunnen zijn voor de strategische en tactische doelstellingen van terroristische groeperingen. Een aanval met fosfine kan bijvoorbeeld enorme angst en ontwrichting teweegbrengen, politieke schade aanrichten en veiligheidsdiensten beschadigen.

Het potentieel om aanzienlijke hoeveelheden niet-kinetische schade toe te brengen, alsmede de beschikbaarheid en het gebruiksgemak van deze stoffen, moeten op waarde worden geschat, en veiligheidsdiensten moeten een netwerk van tegenmaatregelen (preventienetwerk) inrichten dat uit meerdere lagen bestaat. Op basis hiervan hebben we voor dit proefschrift de volgende onderzoeksvraag geformuleerd: *Hoe kunnen we een effectief netwerk van tegenmaatregelen tegen terroristische aanslagen met toxines voor algemeen gebruik bouwen, met daarin diverse gezamenlijke acties, uitgevoerd door alle belanghebbenden die collectief verantwoordelijk zijn voor de bestrijding van deze aanslagen?*

In dit proefschrift laten we in detail zien dat de veiligheidsrisico's van terroristisch gebruik van ricine, fosfine en americium groot genoeg zijn om aanleiding te geven tot een dergelijk preventienetwerk. Daarnaast stellen we dat in het voorgestelde preventienetwerk niet alleen overheidsinstanties moeten zitten, maar ook andere belanghebbenden, zoals fabrikanten en verkopers van deze producten, de pers, onderzoekers, internetproviders, gebruikers van social media en burgers. We stellen dat al deze groepen belanghebbenden een gezamenlijke morele verantwoordelijkheid hebben om terroristische aanslagen met toxines voor algemeen gebruik te bestrijden. Deze gezamenlijke morele verantwoordelijkheid is gebaseerd op het

zogenaamde NMH-principe (No Means to Harm – dat we anderen geen mogelijkheden moeten bieden om kwaad te doen), en dat kan worden vertaald in specifieke acties van personen in deze groepen van belanghebbenden. Denk bijvoorbeeld aan het melden van verdachte aankopen in bouwmarkten of het markeren en verwijderen van wapenhandleidingen op het internet.

In een kritische analyse van de huidige maatregelen ter bestrijding van terroristische aanslagen waarbij toxische stoffen voor algemeen gebruik als wapens worden gebruikt, laten we zien dat de meeste van de huidige gezamenlijke maatregelen te lijden hebben onder onwetendheid bij belanghebbenden over hun verantwoordelijkheid binnen het preventienetwerk. Verder stellen we dat veiligheidsdiensten kansen laten liggen om de morele verantwoordelijkheden van belanghebbenden, zoals verkopers van toxische producten, te operationaliseren. In deze analyse gebruiken we de Duitse veiligheidsinfrastructuur als primair voorbeeld van de huidige architectuur van deze gezamenlijke maatregelen en de problemen ermee. De tegenmaatregelen die in dit proefschrift worden besproken, kunnen in drie groepen worden onderverdeeld: maatregelen tegen de verwerving van relevant wapenmateriaal, maatregelen tegen de verwerving van relevante wapenexpertise en maatregelen om de veerkracht na een aanval te waarborgen.

Op basis van deze beoordeling doen we in dit proefschrift aanbevelingen voor verbetering van de huidige architectuur van beveiligingsmaatregelen tegen CBRN-wapens. We laten zien dat de verantwoordelijkheden en acties van elke groep belanghebbenden moeten worden gedefinieerd, besproken en

gecoördineerd door alle relevante groepen belanghebbenden tezamen. Hiertoe moet het theoretische concept van het preventienetwerk worden omgezet in een geïnstitutionaliseerd netwerk in de vorm van een ‘gemeenschappelijk centrum’. Een dergelijk gemeenschappelijk centrum geeft de groepen belanghebbenden de gelegenheid om (1) de dreiging te beoordelen, (2) de taken en acties van elke groep te definiëren en (3) elke groep te voorzien van de middelen om deze acties op een doeltreffende en ethisch duurzame wijze uit te voeren.

In het bijzonder kunnen de in dit proefschrift gedefinieerde groepen belanghebbenden in het voorgestelde gemeenschappelijk centrum communiceren en acties coördineren. Zo kunnen verschillende werkgroepen, die bestaan uit wisselende samenwerkingsverbanden tussen de groepen belanghebbenden, efficiënt samenwerken, en kunnen ze maatregelen tegen de verwerving van materialen en kennis voor terroristisch gebruik van ricine, fosfine en americium beoordelen, definiëren en toepassen. Daarnaast biedt het voorgestelde gemeenschappelijk centrum ook de mogelijkheid om de maatregelen ter voorbereiding op de nasleep van een aanslag waarbij toxische stoffen voor algemeen gebruik als wapen worden ingezet, te verbeteren en te coördineren.

Naast deze specifieke taken van het gemeenschappelijk centrum met betrekking tot tegenmaatregelen tegen het gebruik van ricine, fosfine en americium door terroristen, geven we in dit proefschrift ook enkele algemene conclusies met betrekking tot terrorismebestrijding, CBRN, en collectieve verantwoordelijkheid. We concluderen dat *nadenken over de rollen en verantwoordelijkheden van diverse belanghebbenden in de strijd*

*tegen het terrorisme, en inzicht in de mechanismen achter terrorisme als collectief verschijnsel, een kader kunnen bieden om CBRN-terroristische dreigingen op een doeltreffende en ethisch duurzame manier aan te pakken.*

Voor deze specifieke en algemene conclusies wordt de bovengenoemde onderzoeksvraag in vier delen besproken. Het eerste deel is gewijd aan de dreiging en gaat over de definitie van terrorisme, massavernietigingswapens en CBRN. Ook wordt er een beoordeling gegeven van de impact van de dreiging en van de beschikbaarheid van wapens voor terroristen. In het tweede deel introduceren we het begrip collectieve morele verantwoordelijkheid en definiëren en bespreken we de groepen belanghebbenden die een morele verantwoordelijkheid delen bij de bestrijding van terroristische aanslagen met toxische stoffen als wapens. Het derde deel bevat een kritische beoordeling van de huidige gezamenlijke maatregelen van deze groepen belanghebbenden om de verwerving van toxines en gespecialiseerde kennis door terroristen tegen te gaan. In het vierde deel combineren we de in deel twee gedefinieerde concepten en morele verantwoordelijkheden met de kritische beoordeling van deel drie en geven we een lijst van voorgestelde maatregelen in het preventienetwerk om de gezamenlijke strijd tegen deze tak van terrorisme te verbeteren. Hierbij speelt de institutionalisering van het preventienetwerk als gemeenschappelijk centrum een centrale rol.

We besluiten het proefschrift met speciale aandacht voor de gezamenlijke en individuele verantwoordelijkheden van burgers na terroristische aanslagen waarbij giftige stoffen voor algemeen gebruik als wapen zijn gebruikt. We laten zien dat we allemaal, op z'n minst tot op zekere hoogte, moreel

verplicht zijn ertoe bij te dragen dat we de veerkracht bezitten om een dergelijke aanval op te vangen.





# Abbreviations

AML	Anti-money laundering
AN	Ammonium nitrate
ANALFO	Ammonium nitrate aluminum fuel oil
ANALNM	Ammonium nitrate nitromethane
ANFO	Ammonium nitrate fuel oil
AQI	Al Qaeda in Iraq
BAMF	Bundesamt für Migration und Flüchtlinge ( <i>German Federal Office for Migration and Refugees</i> )
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe ( <i>German Federal Office for Civil Protection and Disaster Assistance</i> )

BFE+	Beweissicherungs- und Festnahmeeinheit plus der Bundespolizei <i>(Tactical Counter terrorism unit of the German Federal police)</i>
BfV	Bundesamt für Verfassungsschutz <i>(German Federal Domestic Intelligence Service)</i>
BJA	Bundeskriminalamt <i>(German Federal Criminal Police Office)</i>
BMAP	Bomb making materials awareness program
BND	Bundesnachrichtendienst <i>(German Federal Intelligence Service)</i>
BSI	Bundesamt für Sicherheit in der Informationstechnik <i>(German Federal Office for Information Security)</i>

BWC	The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction
CBRN	Chemical, biological, radiological, nuclear
CBRNE	Chemical, biological, radiological, nuclear, explosives
CCA	United Nations Commission on Conventional Arms Control
CISA	Cybersecurity and Infrastructure Security Agency
CLP	Classification, Labelling and Packaging Regulation
CSAC	Chemical Security Analysis Center
CT	Counter-terrorism

CUTA	Coordination Unit for Threat Analysis
CWC	Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction
DHS	Department of Homeland Security
DOD	Department of Defence
ECHA	European Chemical Agency
ECTC Centre	European Counter Terrorism
EPA	Environmental Protection Agency
ETA	Euskadi Ta Askatasuna
EU	European Union
GBA	Generalbundesanwalt ( <i>German Federal Public Prosecutor General</i> )

GETZ	Gemeinsames Extremismus- und Terrorismusabwehrzentrum ( <i>German Joint Counter- extremism and Counter terrorism Centre</i> )
GIZ	Gemeinsames Internetzentrum ( <i>German Joint Internet Centre</i> )
GSG9	Grenzschutzgruppe 9 der Bundespolizei ( <i>Border Protection Unit 9 of the German Federal Police</i> )
GTAZ	Gemeinsames Terrorismusabwehrzentrum ( <i>German Joint Counterterrorism Centre</i> )
GTD	Global Terrorism Database
HAZMAT	Hazardous materials
IAEA	International Atomic Energy Agency
ICBM	Intercontinental ballistic missile

ICRC	International Committee of the Red Cross
IED	Improvised explosive device
IP	Internet protocol
IRA	Irish Republican Army
IRU	Internet Referral Unit
ISIL	Islamic State of Iraq and the Levant
ISP	Internet Service Provider
JTAC	Joint Terrorism Analysis Centre
LfV	Landesamt für Verfassungsschutz <i>(German State Domestic Intelligence Services)</i>
LKA	Landeskriminalamt <i>(German Criminal Police Offices of the Federal States)</i>
MAD	Militärischer Abschirmdienst <i>(German Military Counter Intelligence Agency)</i>

NATO	North Atlantic Treaty Organization
NCTV	National Coordinator for Security and Counterterrorism
NIAS	Nachrichtendienstliche Informations- und Analysestelle ( <i>Intelligence Information and Analysis Unit in the German GTAZ</i> )
NMH	No means to harm
NRC	Nuclear Regulatory Commission
NTI	Nuclear Threat Initiative
OPCW	Organization for the Prohibition of Chemical Weapons
PCCTS	Pauperes commilitones Christi Templique Salomonici
PFLP	Popular Front for the Liberation of Palestine



PIAS	Polizeiliche Informations- und Analysestelle ( <i>Police Information and Analysis Unit in the German GTAZ</i> )
POICN	Profiles of Incidents Involving CBRN and Non-state Actors
PPE	Personal protective equipment
PTSD	Post-traumatic stress disorder
RAF	Rote Armee Fraktion ( <i>Red Army Faction</i> )
RED	Radiological exposure device
RDD	Radiological dispersal device
RUP	Restricted Use Pesticides
SS	Schutzstaffel ( <i>National socialist military unit</i> )
SSA	Chemical Sector-Specific Agency
ST	Staatsschutz ( <i>German State Security</i> )

START	Strategic Arms Reduction Treaty
TATP	Triacetone triperoxide
TIC	Toxic industrial chemical
TNW	Tactical nuclear weapon
UN	United Nations
UP KRITIS	Umsetzungsplan Kritische Infrastrukturen ( <i>German Action Plan Critical Infrastructure</i> )
USFA	United States Fire Administration
VNSA	Violent non-state actors
WHO	World Health Organization
WINS	World Institute for Nuclear Security
WMD	Weapon of mass destruction
WME	Weapon of mass effect

ZKA

Zollkriminalamt (*Central Office  
of the German Customs  
Investigation Service*)

## List of tables

<i>Table 1: Obligations and actions of stakeholder groups in the web of prevention</i>	212-213
<i>Table 2: Web of prevention – materials</i>	337-338
<i>Table 3: Web of prevention – expertise (only dangerous knowledge)</i>	338-339
<i>Table 4: web of prevention – resilience</i>	339
<i>Table 5: Web of prevention – expertise (dual-use knowledge)</i>	340-341

## List of figures

<i>Fig. 1: Necessary elements in an act of terrorism</i>	59
<i>Fig. 2: Yengst's criteria for mass effect</i>	74
<i>Fig 3: Graph to display the risk assessment of terrorist weaponry</i>	92
<i>Fig. 4: Multi-layered joint action</i>	166
<i>Fig 5: Multi-layered joint (moral and institutional) responsibility</i>	167
<i>Fig. 6: Moral responsibilities of relevant stakeholder groups</i>	316
<i>Fig. 7: Web of prevention</i>	342

# Table of contents

General introduction	1
----------------------	---

## Part I: The threat

1. The definition of terrorism	19
2. Concepts and frameworks of WMD and CBRN	61
3. Threat assessment of selected common-use toxins – Ricin, phosphine, americium	95

## Part II: Responsibilities and stakeholders

4. The concept of collective moral responsibility	153
5. Critical stakeholders in the fight against attacks using common-use toxins	171
6. Moral obligations and counter-measures in the web of prevention	187

## Part III: Current counter-measures

7. Preventing the acquisition of common-use toxins for terrorist purposes	217
---	-----

8. Denying terrorists access to the knowledge to use common-use toxins as weapons	249
--	-----

#### Part IV: The web of prevention

9. A web to prevent the acquisition of dangerous substances	277
10. A web to deny terrorists access to dangerous expertise	299

#### Special focus and general conclusion

The aftermath of an attack, the press, and the public	319
---	-----

General conclusion	337
--------------------	-----

References	345
------------	-----

Acknowledgments	387
-----------------	-----

About the author	390
------------------	-----

List of publications	391
----------------------	-----

## General introduction

*On June 12, 2018, German police forces stormed an apartment in Cologne and arrested the Tunisian Salafist Sief Allah H. on the basis of intelligence that he planned a terrorist attack. During the raid of his apartment, Special Forces were called in and found over 3,000 castor beans that contain the organic toxin ricin. According to the German police report of this incident, Sief Allah H. had already begun to grind the seeds and had apparently attempted to combine the ricin powder with an IED (improvised explosive device) to disperse the toxin in a populated area in Cologne (Rheinische Post, 2019; Spilcker, 2018; Staudenmaier, 2018).*

The threat of terrorist attacks using chemical, biological, radiological or nuclear (CBRN) weapons belongs among the most discussed issues in terrorism research. In addition to academic debates about the terminology and concept of CBRN, a large number of researchers have also discussed more applied matters in this field, such as CBRN counter-measures, dual-use issues with regard to CBRN and even ethical dimensions of CBRN response plans (A few examples are Asal et al., 2012; Ivanova & Sandler, 2006, 2007; Koehler & Popella, 2018; Lemyre et al., 2005; National Research et al., 2014; Rebera & Rafalowski, 2014; Ruggiero & Vos, 2015a; Spencer et al., 2012; Stenersen, 2009). Yet, many researchers in the field of CBRN threats characterize this phenomenon as a typical “low probability – high impact” threat (J. J. F. Forest, 2012 discusses this conservative view;



Ruggiero & Vos, 2015b, p. 146; also mentioned in Szinicz, 2005): for example, in the aftermath of the above-described plot in Cologne Sief H's plan to construct a ricin-based IED was portrayed as a singular and exceptional case of terrorism that had the potential to kill or wound tens of thousands of persons. H's device was repeatedly called the first "bio bomb" in the history of terrorism in Germany (Deutsche Welle, 2018).

This characterization of the incident that the German news media called the "Cologne Ricin Plot" fits all too well into the view of CBRN threats that many researchers maintain. H's device was publicly seen as a biological weapon with potentially devastating impact that has never been used before and, hence, remains an exceptional weapon type that is usually too complex to assemble and too resource demanding for small terrorist cells and lone operators (Flade, 2018).

This view corresponds with a popular understanding among researchers of what constitutes a CBRN weapon. In many publications, this weapon category is implicitly portrayed as the terrorist use of a weapon of mass destruction (WMD) such as, for example, a nuclear weapon or substances that are internationally classified as biological or chemical warfare agents (General discussion in Carus, 2012). The Cologne Ricin Plot was also portrayed in a manner consistent with this understanding of CBRN. This portrayal is clearly visible in the journalistic reporting on the incident. In many journalistic analyses of the plot, authors described ricin as a biological weapon agent and referred to the mention of ricin in the Chemical Weapons Convention (CWC) and in the Biological Weapons Convention (BWC) of the United Nations (UN) (Organisation for the Prohibition of Chemical

Weapons, 1992; United Nation Office of Disarmament Affairs, 1975; Westdeutscher Rundfunk, 2018).

Consistent with this interpretation of CBRN weaponry as primarily including UN-defined warfare agents and WMDs, most national security agencies<sup>1</sup> and international organizations focus their efforts to counter CBRN terrorism on non-proliferation (United Nations Office on Drugs and Crime, 2016). As CBRN weaponry is traditionally viewed as military-grade weapon agents with professional delivery systems, measures to counter their terrorist use aim at controlling and restricting access to military stockpiles of materials and to the means of production of these agents and delivery systems. These measures typically include diplomatic efforts in the context of disarmament (e.g., as part of the CWC and BWC) and rigorous controls of the proliferation of so-called dual-use technologies (See for discussion Miller, 2018). These technologies include materials and machinery that were initially designed for peaceful purposes (e.g., for the energy sector) but can be used in a belligerent way; for example, for the manufacturing or delivery of CBRN weaponry. In the context of CBRN defense, dual-use goods might include centrifuges (e.g. for uranium enrichment), certain spray mechanisms (for the dispersal of BC agents) or missile technology (as delivery systems for nuclear warheads) (Miller, 2018).

The restriction and implementation of controls of the production and trade of these dual-use products is a cooperative effort of international

---

<sup>1</sup> For example, in Germany CBRN defense is part of counter-espionage and non-proliferation efforts in the federal criminal police agency (*Bundeskriminalamt*) and in the foreign intelligence agency (*Bundesnachrichtendienst*) (Bundeskriminalamt, 2021; Bundesnachrichtendienst, 2021).

organizations, selected globally acting corporations and, especially, nation-states. The Organisation for the Prohibition of Chemical Weapons (OPCW) of the United Nations and the non-profit organization Nuclear Threat Initiative (NTI) are only two examples of many international programs to counter the proliferation of WMDs of state actors and non-state actors (NTI, 2021; OPCW, 2021).

Yet, these measures to combat CBRN terrorism clearly prioritize high-end military-grade weaponry and, thereby, tend to neglect improvised and crude CBRN devices that are not classified and internationally ostracized as the means to wage biological, chemical or nuclear warfare. The Cologne Ricin Plot is one example of this dangerous gap in the international and national counter-CBRN architecture. Rather than attempting to purchase or manufacture professional spray mechanisms or other dual-use materials for weapon delivery purposes, Sief H. purchased most materials to assemble his biological device legally and by recourse to the internet. The reason for this availability and lack of the security agencies' interest in relatively small purchases of ricin-based materials is the fact that this substance is naturally occurring in castor beans.

Therefore, purchases of small to medium amounts of castor beans are not restricted since the amount and purity of potentially extractable ricin from these beans would not classify as mass destructive in terms of the definition of a WMD.<sup>2</sup> Ricin that is extracted from a number of castor beans that can be processed without professional industrial processes is not considered by security agencies to be capable of killing or wounding a large number of

---

<sup>2</sup> For a detailed discussion, see chapters 3 and 7 of this thesis.

persons (in comparison to, for example, virulent biological weapons or nuclear warheads) if used in a terrorist attack by a small cell or lone operator.

Similar lack of interest with regard to CBRN counter-measures is visible in other chemical, biological, and radiological substances that are considered low or medium risk materials due to their incapacity to inflict mass casualties in an attack. The toxic gas phosphine and the radioactive element americium (especially americium-241) are, next to ricin, excellent examples of a group of substances that slip through the cracks of most CBRN security architectures in Europe and the USA.<sup>3</sup> This is not regarded as an important issue due to the fact that security analysts consider these three substances to exhibit only limited capabilities as impactful CBRN weapons.<sup>4</sup> Hence, in accordance with the above-mentioned “Impact – Probability” matrix that is used widely in CBRN security research, these three substances - while available to potential terrorists - do not enable terrorists to perform attacks with a large impact. This assessment characterizes phosphine, americium, and small amounts of ricin as low-impact toxic substances and, thereby, removes them from the focus of CBRN counter-measures.

However, the present thesis will focus on this category of CBRN weapons that are commonly considered low-risk, “common-use” toxic substances and that are, therefore, not a priority in CBRN defense and non-proliferation efforts. This thesis will discuss the concept of CBRN, the threats evolving

---

<sup>3</sup>A detailed justification to use these three substances as examples and focus of the present analysis will be presented in chapters 2 and 3 of this thesis.

<sup>4</sup>For example, phosphine is considered a “moderate risk” toxic industrial chemical with regard to terrorism according to the United States DHS (TRADOC, 2007, pp. II–14). See chapter 3 of this thesis.

out of the terrorist use of ricin, phosphine, and americium as well as the respective counter-measures to combat attacks using these substances. Since all of these substances are commonly used and widely available, a variety of agents (businesses, citizens, etc.) are (albeit unintentionally) providing terrorists with the environment to use them. Hence, and as this thesis will show, all of these stakeholder groups have to cooperate in combating the terrorist use of these substances. The overall aim of this endeavor is to shift the focus of CBRN research onto these toxins and to fill gaps in CBRN defense strategies. In order to achieve this goal, it will be asked:

***How can we build a functioning web of counter-measures against terrorist attacks that use common-use toxins in a manner that includes a variety of cooperative actions executed by all stakeholders who are collectively responsible for combating these attacks?***

This research question gives rise to three sub-questions. The first, and most obvious, of these questions is:

***(1) Why do we need such a web of counter-measures?***

As already mentioned in the beginning of this introduction, common-use toxins such as small amounts of ricin, phosphine or americium do not qualify as impactful terrorist weapons with regard to lethality or physical destructiveness. Hence, it seems reasonable to ask why one should dedicate an entire thesis to the design of a sophisticated web of security measures to combat the terrorist use of these substances. For someone might argue that current, general CT measures are sufficient in most nations to account for the manageable threat that these substances pose. Yet, this thesis will show

in detail that the premise that terrorist attacks using the mentioned common-use toxins only pose a minor threat to society cannot be maintained. First of all, it will be argued that the general concept of a terrorist attack involves much more than physical violence as its outcome. Instead, the concept of a terrorist attack will be defined as an interplay of the intentions of a terrorist and the consequences of an attack of which some are physical e.g. casualties and destroyed buildings, and others are not e.g., the spreading of fear in society.

Furthermore, it will be shown that current conceptualizations of weapon categories such as WMD or CBRN are primarily focused on the physical damage that weapons in these categories are able to inflict in an attack. The concept of impact associated with these weapon categories is primarily physical, i.e., deaths and other casualties, damage to buildings or infrastructure, and contamination of areas. I will argue that this interpretation of the impact that a terrorist attack can have on a target society is inadequate. It will be shown in a detailed analysis that terrorist attacks and their consequences affect a much broader audience than the group that is physically harmed by the attack. Psychological, economic, and political damage as well as uncertainty and distrust are consequences of terrorist attacks that can harm society to a significantly larger degree than the physical consequences of, for example, the detonation of a small IED.

Based on these findings in research, this thesis will show that substances that used to be considered low-risk terrorist weapons might, in fact, be capable of causing a catastrophic amount of harm to society. The specific properties and nature of ricin, phosphine, and americium in combination

with public anxiety concerning phenomena like bioterrorism or radioactivity in general make these substances powerful terrorist weapons despite not being capable of killing a very large number of persons.

This thesis will discuss the capabilities of the three common-use toxins in detail and, thereby, present the first detailed academic discussion of these substances<sup>5</sup> in terms of the multidimensional impact of terrorist attacks. This discussion will provide the justification for establishing a web of counter-measures against the terrorist use of common-use toxins such as ricin, phosphine, and americium. Yet, while the need for such a web might be accepted, the involvement of a variety of stakeholders in this web in addition to security agencies might be disputed. This brings us to our second question:

***(2) What stakeholders in addition to the security institutions ought to be involved in combating this form of terrorism?***

While the task of combating terrorism is clearly an institutional responsibility of governments and their security institutions, such as the police and intelligence agencies, it is not self-evident that other, non-government agencies, including private sector ones, ought to assist in this task.

---

<sup>5</sup>Note here that there are some short academic discussions of the terrorist use of ricin and of americium available (See e.g. Satterfield, 2011; Szinicz, 2005). Yet, all of these discussions present primarily technical analysis and risk modeling rather than a conceptual analysis of the impact and counter-measures with regard to these substances.

However, first of all, these additional stakeholders have to be determined, and whether these stakeholders are already involved in CBRN counter-measures. As already briefly mentioned in the beginning of this introduction, the current CBRN security infrastructure, and more specifically the parts of this infrastructure that are concerned with dual-use goods, includes, in addition to government agencies, also international organizations, think tanks and relevant global businesses. Yet, due to the global scope of this infrastructure, CBRN security partnerships with businesses currently consist of selected global corporations involved in high-end engineering products and chemistry. Local businesses, store owners or regional manufacturers only play minor roles or no role at all in the CBRN counter-measures of most European countries. Yet, precisely these stakeholders are the most promising partners in combating the terrorist use of common-use substances such as ricin, phosphine or americium.

This thesis will identify the most relevant stakeholders in the fight against terrorist attacks that might use these substances. It will be shown that not only security agencies and global businesses, but also local manufacturers and vendors of toxins, internet start-up companies, online users, the news media, CT-researchers, and even every single citizen in a society are able to help efforts to combat this kind of terrorism. However, the ability to help alone does not obligate a stakeholder to be part of this joint fight against terrorism. One has to find arguments in favor of the claim that these above-mentioned groups of stakeholders *ought* to join (i.e., possess the moral responsibility to join) the web of counter-measures. This thesis will show that all of the above-mentioned stakeholders, in fact, share a joint moral responsibility to combat the terrorist use of common-use toxins. In order to



show this, however, concepts of collective moral responsibility and, more specifically, joint moral responsibility have to be (and will be) conceptually analyzed. Based on this conceptual analysis, it will be argued that the moral responsibility to join the web of preventing the terrorist use of common-use toxins is based on the so-called No Means to Harm (NMH) principle (Miller, 2018). This moral principle obligates all groups of stakeholders identified in this thesis to undertake individual and joint actions in order to realize the common goal of successfully combatting this form of terrorist attacks.

Once the most relevant stakeholders in the web of preventing attacks using common-use toxins are identified, the measures in this web will raise another important question:

***(3) Why are current measures to combat terrorist attacks that make use of common-use toxins insufficient?***

While it might be justifiable that stakeholders such as manufacturers or vendors of toxins ought to help efforts to combat the terrorist use of these substances, it has to be shown in detail that the current ways in which these stakeholders cooperate with law enforcement are insufficient in order to fulfill their responsibilities in this regard. As this thesis will lay out in a descriptive section, almost all of the above-mentioned stakeholder groups are already, at least in some capacity, part of the web of measures to combat terrorist attacks using common-use toxins. That means specifically that most groups of stakeholders currently undertake some individual or joint actions in order to serve the common goal of fighting this form of terrorist attacks.

Yet, it will also be shown that examples of these current, cooperative measures lack either efficacy or ethical sustainability or both. These deficiencies in the current cooperative measures stem from the unawareness of almost all groups of stakeholders concerning their moral obligation to help counter-terrorism efforts in this field. It will be shown in a critical analysis of selected, current measures to combat terrorist attacks that use ricin, phosphine, and americium that these measures have gaps and raise unresolved ethical issues. The main reason for this is that cooperation between the government institutions and the other stakeholder groups is not coordinated in an efficacious and ethically sustainable way. This issue has its roots in the fact that many stakeholder groups do not view themselves as obligated to be part of this web of counter-measures or they are simply not provided with the information that would be necessary in order to participate in the cooperative measures to combat attacks using common-use toxins.

The above described three sub-questions will be addressed in this thesis and the generated answers will be synthesized in the concluding section. In this conclusion, it will be argued that structured cooperation and communication between all stakeholder groups within an institutionalized web of counter-measures is the key to combating terrorist attacks that use common-use toxins in an efficacious and ethically sustainable manner. The prerequisite for such an institutionalized web of prevention is the awareness of all stakeholder groups with regard to their individual and joint responsibilities in fighting this form of terrorist attacks. These responsibilities involve not only active communication among stakeholders but also a division of labor with regard to the tasks to be undertaken in the web. The establishment of a

Joint Center Against the Terrorist Use of Common-Use Substances will be recommended in order to provide stakeholders with a platform to communicate and collaborate in order to fulfill their joint responsibility to combat terrorist attacks that use these substances.

In order to answer the research question (and, hence, the three sub-questions), this thesis will need to be restricted to selected substances, issues, measures, and CT architectures. Hence, I will focus primarily on the following aspects of the cooperative fight against terrorist attacks using common-use toxic substances:

The most obvious constraint of the present thesis involves the discussion of three selected substances, ricin, phosphine, and americium. The choice to discuss these three commonly available, every day-use substances might seem to be (at least with regard to phosphine and americium) counter-intuitive from a counter-terrorism perspective. Yet, it will be shown that the potential use of these common-use toxins as weapons by terrorists is among the most concerning terrorist threats according to a weapon rating system that will be introduced in this thesis. Hence, it is necessary to discuss these substances in detail. Moreover, these substances can be used as examples to understand the much broader issues connected to the terrorist use of common-use and household substances. Hydrogen peroxide or chlorine would be two other examples that are comparable to the three selected substances. In addition to that, while there are at least some brief discussions to be found with regard to ricin in CBRN studies, the other substances have not been discussed yet and, hence, can be analyzed in this

thesis without reviewing the whole body of CBRN literature as it would be needed in a discussion of, for example, sarin or anthrax.

Another constraint and, hence, focus is on counter-measures against terrorist attacks that use these common-use toxins. Here, I primarily discuss measures designed to deny terrorists access to the substance, to deny terrorists access to the knowledge to assemble a weapon, and to ensure resilience in the aftermath of an attack. In the course of this thesis, it will be shown that these three groups of measures are necessary counter-measures in order to interrupt the process of successfully using a weapon by a terrorist group or lone operator. Furthermore, the selected measures point to generalizable counter-measures in CBRN defense. Finally, all of the counter-measures discussed in this thesis have been openly described in some context or other by law enforcement officials, journalists or academic researchers. Hence, in contrast to other covert counter-terrorism measures, it is possible to discuss these measures without reverting to an excessive degree of speculation.

The last focus of this thesis is a geographical one. A detailed discussion of all these counter-terrorism measures in every or most parts of the world would be a massive endeavor and exceed the limited space available in this thesis. Hence, I will focus on measures within the jurisdictions of European countries and the United States of America. Even more specifically, I will primarily focus on German counter-measures and will use the counter-terrorism architectures of the Netherlands, the United Kingdom, and the United States as comparative counterparts to the German counter-terrorism landscape in selected cases. This narrow approach enables an overview of

counter-measures and legislative frameworks with regard to the three substances that are commensurate with each other because they form part of the same kind of counter-terrorism architecture. Moreover, it will be shown that the German counter-terrorism architecture is structured in a similar way to its respective counterparts in the Netherlands, the UK, and the US. Hence, recommendations in relation to counter-terrorism measures in Germany are generalizable to the security arrangements in other European and North American countries. Furthermore, in contrast to the massive counter-terrorism apparatus of the United States, the German CBRN defense landscape, in particular, has not received detailed analysis and discussion in the academic literature.

My general aims in this thesis are as follows. I provide the first, critical overview of selected counter-measures against terrorist attacks that use common-use toxins. Based on this critical overview, counter-measures will be recommended to advance the fight against this form of terrorist attacks. In doing so, I hope to both shift the focus of CBRN research and academic debates concerning counter-terrorism, both at the level of normative frameworks, given my emphasis on collective responsibility and at the practical level, given my recommendations to assist counter-terrorism practitioners in their fight against CBRN terrorism. The thesis is in four parts:

The first part of this thesis will discuss the threat that we are facing. A definition of terrorism will be provided and concepts of terrorist weaponry such as WMD and CBRN will be critically reviewed. Based on this review, a terrorist weapon scoring system will be developed in order to identify

particularly dangerous weaponizable substances. This system will be applied in order to analyze the impact that ricin, americium, and phosphine could have if weaponized and used in terrorist attacks. Part II of this thesis is dedicated to the stakeholders that are, or ought to be, involved in cooperative measures to stop terrorist attacks that use these weapons. The foundation of this discussion will be a theoretical elaboration of the concepts of acting jointly and sharing responsibilities. Based on this discussion, key stakeholders in the fight against terrorist attacks that use common-use substances will be identified and it will be shown that each of these stakeholders is morally obligated to be part of this fight.

In part III of the thesis, the current, cooperative counter-measures to stop the terrorist acquisition of these substances and the knowledge on how to use them will be portrayed and critically reviewed. For each substance, one type of counter-measure will be analyzed. It will be shown that both lack of awareness of responsibilities and lack of communication between the stakeholders lead to ineffective and ethically questionable counter-terrorism practices. Part IV of the thesis uses the findings of part III (and the results of parts I and II) to design an institutionalized web of prevention in which all stakeholders can cooperate and communicate with each other in a structured and direct manner. This web features the establishment of what I refer to as the Joint Center. The Joint Center is to be the coordinating hub and within it national security institutions are in the command position and the other stakeholder groups have representatives. Importantly, specific counter-measures are recommended to fill gaps in the current suite of counter-terrorism measures against attacks that use common-use toxins.

A chapter on selected measures to ensure resilience in the aftermath of an attack will conclude this thesis. Here, it will be shown that the media, including social media platforms, and ordinary citizens should be part of the web to combat terrorist attacks that use ricin, phosphine, and americium. Hence, we all, including the readers of this introduction, may have a responsibility, jointly held with others, to assist in combating terrorist attacks that use common-use toxins.





# **Part I: The threat**

# **1. The definition of terrorism**

## **1. Introduction**

Despite the fact that terrorism belongs to the most commonly used terms of our time, the question of how to define this term remains unanswered. A definition that most researchers and policymakers can agree upon appears to be far from established, and this vague status of the definition of terrorism seems to be an accepted state of affairs in academia. Although the terrorism scholar Alex P. Schmid devoted a lot of work to the search for a suitable definition by compiling several hundred definitions and surveying different researchers and professionals in the field of counter-terrorism, even his proposed “academic consensus definition” of terrorism (and its revised versions) did not become a broadly accepted definition of terrorism in research (A. P. Schmid, 2012).

However, a closer look at the reasons for this dissent reveals that it is actually not too difficult for both researchers and policymakers to agree upon what kind of acts should be considered terrorism in a very broad sense. Roughly speaking, most researchers and analysts would agree that terrorism constitutes an act of violence that spreads fear and communicates an ideology. On the other hand, most researchers concerned with this debate disagree about the roles that should be assigned to each of these three characteristics. In this regard, some researchers argue that certain characteristics used to define terrorism only have to be present in the form

of a threat or a mere intention of the perpetrator in order to constitute an act of terrorism. For example, in his academic consensus definition, Schmid is referring to the violent character of terrorism as to “physical violence or threat thereof” (A. P. Schmid, 2012). Seemingly, only the threat to use violence is sufficient to qualify an attack an act of terrorism for Schmid, if the other characteristics are in place. Moreover, if a mere threat to commit violence is sufficient to constitute terrorism, then presumably a mere intention to do so could also constitute terrorism (given the existence of certain other conditions, e.g., the intention to spread fear and communicate an ideology). This radical understanding of terrorism as a mere intention is problematic, as this chapter will show.

As the ongoing debate among researchers has shown, the distinction between merely intending and actually bringing about the three characteristics of terrorism is an excellent starting point to further specify what should count as a necessary condition to classify an act as terrorism. To further investigate this distinction, the philosophy of action and specifically action theory can be of help. Although researchers like David Rodin (Rodin, 2004), Frances Kamm (Kamm, 2011), and Seumas Miller (Miller, 2012) have already utilized action theory to distinguish certain elements of the definition of terrorism, a general discussion into this matter is still lacking. Thus, by deploying action theory, the present analysis aims at both producing new insights into problems and “grey zones” concerning the definition of terrorism and also responding to already existing attempts to deploy action theory, e.g., the account of Rodin.

Finally, this chapter will present a definition of terrorism that consists of a set of individually necessary and jointly sufficient conditions for an action to constitute an act of terrorism. Contrary to the existing accounts of terrorism, this definition discusses the intentions of the terrorist and presents them as a necessary, yet not sufficient, element in the definition of terrorism.

## 2. The definition of terrorism – Three characteristics that most researchers might agree upon

Despite the ongoing, controversial debates concerning the definition of terrorism among philosophers and terrorism researchers, it seems that at least three characteristics recur in most academic or non-academic definitions of terrorism. Thus, these three characteristics constitute a solid foundation for the construction of a definition of terrorism.

### 2.1. Characteristic of creating fear

The action of creating fear plays a crucial role in almost every academic or legal definition of terrorism. For example, the North Atlantic Treaty Organization (NATO) defines terrorism as a tactic to “intimidate governments or societies” (North Atlantic Treaty Organization, 2014, p. 5) and the U.S. Department of Defense characterizes terrorism as a tactic that “instill[s] fear” (U.S. Department of Defense, 2010, p. 1). Furthermore, Alex Schmid claims that terrorism is a “fear-generating” (A. P. Schmid, 2012) tactic and Igor Primoratz acknowledges that terrorism has the “aim of

intimidating” (Primoratz, 1997, p. 129) innocent people. Additionally, Seumas Miller states that terrorism needs a “high degree of publicity” (Miller, 2008, p. 41) in order to spread fear in the “target political or social group” (Miller, 2008, p. 41). The creation of fear is connected to publicity and, thereby, creates a suitable audience for the terrorist to communicate her message. Thus, it seems reasonable to see the creation of fear as one of the central defining components of terrorism. Yet, none of the above-discussed definitions specify whether the creation of fear has to be an actual outcome of an attack in order for this attack to count as terrorism. This chapter will, amongst other things, show that a terrorist does not have to actually create fear to commit an act of terrorism but rather only has to have the intention to do so.

## 2.2. Characteristic of violence against [innocent] victims

To create fear, a specific kind of action is necessary. Here, most researchers and policymakers agree that an act of violence shall be a suitable candidate for this. Hence, a violent act is a defining characteristic of terrorism.

For example, NATO refers to terrorism in general terms as “[t]he unlawful use or threatened use of force or violence” (North Atlantic Treaty Organization, 2014, p. 5). However, this general notion leaves us with a central problem: what degree of violent action should we regard as sufficient to define terrorism? Alex Schmid and Seumas Miller provide a more detailed account of the nature of violence involved in terrorism. Thus, in the following, the vague term of violence shall be more precisely yet pragmatically delimited as “a type of violence that constitutes a human right

violation” (Miller, 2008, p. 54). Thereby, terrorism necessarily includes serious forms of violence “that ought to be criminalized” (Miller, 2008, p. 58) or, more specifically, “physical violence (...) [including] single-phase acts of lethal violence (...), dual- phased life-threatening incidents (...) as well as multi-phased sequences of actions” (A. P. Schmid, 2012).

A second problem with the characteristic of terrorism as a violent act has to do with the potential victims of this violence. It is controversially debated who the victim of a violent attack ought to be to call that attack an act of terror. Many authors state that terrorism either only targets innocent persons or, more generally, noncombatants. For example, in Schmid’s consensus definition, the victims of terrorism are characterized as being “(...) usually civilians, non-combatants or other innocent and defenseless persons” (A. P. Schmid, 2012), whereas C. A. J. Coady refers to the victims of terrorism as non-combatants (Coady, 1985, p. 54).

However, as Miller has pointed out in his book *Terrorism and Counterterrorism*, the two categories of innocents and non-combatants do not seem to be suitable candidates to define the victims of terrorist actions. He argues that the mere definition of innocence is too vague to be used in this discussion and shows that the claim that victims of terrorism are innocent persons would have to involve an ethical assessment of each case of suspected terrorism. Thereby, the use of the concept of innocence makes the definition of terrorism subject to extensive, normative considerations (Miller, 2008, p. 39).

In connection with this argument, Miller identifies convincing cases in which victims of terrorist attacks could not be considered innocent but were still clearly victims of terrorist attacks according to the above-defined criteria. A good example of such a case may be the abduction and murder of the German manager Hanns Martin Schleyer by the left-wing terrorist group Red Army Faction (RAF) (Varon, 2004). While one could argue that Schleyer's past employment in the "Schutzstaffel" (SS) of the German national socialist regime, as well as his radical actions against the labor movement in the 1960s, disqualify him from being "innocent," his abduction and murder by the RAF were clearly not primarily aimed at Schleyer as a person, but mainly a method of communicating a Marxist-Leninist and anticapitalistic ideology to the German government.

Thus, although Schleyer was arguably morally culpable in some sense, he was still the victim of a terrorist attack. To avoid these grey areas in the definition of terrorism, Miller proposes to exclude only serious, ongoing human rights abusers as potential victims of a terrorist act, i.e., if you are a serious ongoing human right abuser and you are the target of a lethal attack for political purposes, then you are *not* the victim of terrorism (Miller, 2008, pp. 50–58).

Since the concept of innocence does not seem to be suitable to define the victims of terrorism, some authors and institutions such as the US Department of State replaced this concept with the more broad concept of noncombatants. However, Miller shows that this term runs into problems as well. These problems mainly stem from the fact that the term combatant refers, just as the term innocent, to a somewhat vague concept. On the one

hand, a narrow definition of non-combatants excludes groups like police forces or security officers and, thereby, would exclude most attacks performed by groups like RAF, ETA or IRA from the definition of terrorism (Miller, 2008, p. 46). A broad definition, on the other hand, would eliminate the distinction between combatants and non-combatants altogether. In Miller's view, a more sensible distinction would be the distinction between *military* combatants on the one and noncombatants on the other side (Miller, 2008, Chapter 2).<sup>6</sup> Indeed, this distinction seems to hold for most of the cases and excludes acts of killing in wartime that seems conceptually different from acts of terrorism. In addition, I argue, this distinction has the advantage of excluding war crimes like the use of chemical warfare from the definition of terrorism.

Based on Miller's analysis, I propose to follow a pragmatic approach concerning the definition of the victims of terrorism. Hence, in the following, I will refer to said victims as [*innocent*] in the sense of neither being military combatants nor being serious, ongoing human rights violators.

### 2.3. Characteristic of communicating an ideology

A third important characteristic in most definitions of terrorism is the notion that terrorism is "usually intended to influence an audience" (U.S. Department of State, 2004, p. xii). This short statement implies that terrorism can be understood as a communication strategy. Several researchers explicitly claim that terrorism is a form of communication or

---

<sup>6</sup> Please note that police officers are considered noncombatants according to this definition.



political agendering (de Graaf, 2003, p. 1; de Graaff, 2012, p. x (10); Kock, 2014, pp. 52–56). This characteristic of terrorism is also visible in Schmid's academic consensus definition in which it is stated that terrorism is being "performed for its propagandistic and psychological effects on various audiences and conflict parties"(A. P. Schmid, 2012). Hence, according to Schmid, terrorism can be seen as a "threat-based communication process[ ]"(A. P. Schmid, 2012).

The claim that terrorism is a form of communication was further developed by Peter de Kock, who discussed the definition of terrorism by referring to elements of communication studies (Kock, 2014, pp. 52–56). With this approach, it becomes visible that terrorism can be identified as a form of indirect communication since the victims of an attack are usually not the receivers of the message but were chosen by the sender (the terrorist) to transfer an ideological message to a third party (e.g., governments, public) that is the receiver of the message. This indirect communication approach is also represented in Schmid's consensus definition in which it is stated that "[t]he direct victims are not the ultimate target (as in a classical assassination where victim and target coincide) but serve as message generators (...)"(A. P. Schmid, 2012).

However, by analyzing terrorism as an act of communication to a large audience - as well as an act of violence intended to cause fear - one has to distinguish between several stages of the communication process: First of all, the terrorist intends that her act of violence receives a high degree of publicity: the terrorist intends that the public come to know that the terrorist's violent attack against an [innocent] person has occurred.

Secondly, the terrorist intends that the public's knowledge of the violent attack generates fear and outrage.<sup>7</sup> Thirdly, the terrorist intends that the audience (the public) receive and understand the perpetrator's ideological message. Finally, the terrorist intends that her audience not only understands but also *believes* her message. Since terrorists usually intend by their violent acts to cause a government, group, or society to change its policies, alter specific ways of life, or even embrace the terrorist ideology, they intend their attacks to coercively persuade, i.e., the persuasion does not simply rely on the plausibility of the content communicated. Terrorist use of coercive persuasion is a form of communication that involves not only an intention that a message be understood but also that it be believed and, ideally, that the ideological background of the message be embraced (For a general view on theories of communication, see Taillard, 2000, pp. 145; 154–155, 2002, p. 190).

### 3. Action theory as a tool to analyze terrorist attacks

The beginnings of the philosophy of action date back more than two millennia. Hence, even the attempt to give a short overview of this field would exceed the limits of this chapter. However, to apply a basic account of action theory to the problems in defining terrorism, it is necessary to identify at least some of the core elements of an action. Of course, this

---

<sup>7</sup> A study by Michael Gross et al showed that the attribution of an attack to a specific terrorist group influences the reaction (fear, stress, political militancy) in the target population (Gross et al., 2016, p. 6). Hence, it is essential for groups like ISIL that the target population clearly associates their attacks with them as a group.

identification should be understood as anecdotal and tailored to serve the aim of this chapter rather than being an exhaustive overview.

The philosopher Donald Davidson maintained that an action is a concept that involves an agent doing something that can be seen as “intentional under some description” (Davidson, 1980, p. 50). This view was further discussed by numerous authors, including Alfred Mele (Mele, 1992; Mele & Moser, 1997) and Michael Bratman (M. Bratman, 1997; M. E. Bratman, 1999). In a more applied approach, Seumas Miller characterizes an individual action as “the intentional behavior of an individual (...) person” (Miller 2001, p.1) by distinguishing it from joint or social actions. As seen in these definitions of an action, a core element of an action is the notion of intention.

Just as in the case of an action, there is no general definition of what is supposed to be an intention, but one of the most influential researchers in this regard, Elizabeth Anscombe, characterized an intention as a threefold phenomenon. Anscombe claims that a person can have an intention *to* act, but this person can also have an intention *in* acting. Finally, a person can also perform an *intentional* action (Anscombe, 2000, Chapter 1). Anscombe’s definition served as a stepping stone for the above-mentioned philosophers of action to further discuss and problematize the nature and relevance of the concept of intention. Amongst others, the existence and order of multiple intentions in one action have been discussed and applied to concrete ethical and moral dilemmas (Miller, 2012). However, in the present chapter, the notion of intention refers to what some philosophers might call the primary intention of an action. While I acknowledge that a wide range of

(secondary) intentions, plans, or desires might be involved in an action, I will restrict this analysis to the primary intention for reasons of clarity.

Another concept that is crucial to describe an action is the concept of consequences. One can identify at least two major groups of consequences that follow an action: First of all, an action of a certain agent has consequences that match the intention of said agents and can, thus, be called the realized intention of this agent. Secondly, in the course of an action, other consequences may arise that are not intended, but unintended outcomes of the agent's action (O'Connor & Sandis, 2011, Chapter 16 "Prospects and Consequences"; Quinn, 1989). These outcomes can be either foreseeable or unforeseeable, unintended outcomes – a distinction that especially plays a large role in the ethical assessment of a certain action (Miller, 2001, p. 236, 2006, p. 178).

Obviously, the philosophy of action discusses not only definitions but mostly problems and dilemmas in the conceptualization of human actions including, but not limited to, questions concerning free will, causation, collective actions, and the ethical relevance of actions (M. E. Bratman, 1999; Mele, 1992; Miller, 2001; O'Connor & Sandis, 2011). However, these discussions are beyond the scope of this chapter that only served as an introduction to some key elements of action theory. Hence, in summary, four elements of an action are most relevant for the further discussion in this chapter: the prior intention to act, e.g., the intention to torture a known terrorist, the intention constitutive of the action, e.g., the intentional pulling out of the terrorists fingernails using pliers, the foreseen (yet unintended) consequences of an action, e.g., the anger generated in the terrorist's

community, and the unforeseen consequences of an action, e.g., riots caused by the act of torture.

#### 4. Action sensitive analysis of what constitutes terrorism

In the following chapters, the two preparatory discussions of core characteristics in terrorism and action theory will be combined. Specifically, it will be investigated to what degree (intention only, realized intention, or unintended outcome) each of the three characteristics of terrorism has to be present in an attack to qualify this attack as an act of terror. Since an exhaustive investigation of all thinkable combinations of these characteristics would exceed the size of this chapter, I will discuss each of the three characteristics separately. Furthermore, I will only focus on particularly problematic and, hence, interesting cases in which it does not seem clear if such scenarios would qualify as terrorism.

##### 4.1. Act of creating fear

###### A) As intention only

As discussed above, it is a necessary condition of a terrorist attack that said attack involves fear to some extent. However, in some cases of what one would consider terrorism, this characteristic of fear is not the actual consequence of an attack, although the attacker most certainly intended to create fear with said attack. Should these cases still be regarded as

terrorism? To investigate this question, a lone-wolf terrorist attack can be used as a case study.

On October 17, 2015, the German right-wing extremist Frank S. attacked the candidate for mayor of Cologne Henriette Reker at a rally in Cologne Braunsfeld with a bowie knife. After stabbing the politician in the neck, S. assaulted and wounded four bystanders (Rath, 2015; The Irish Times, 2015). The assault was stopped by German federal police officers. After his arrest, the attacker repeatedly named the refugee-friendly policies of Reker, German chancellor Angela Merkel, and other German politicians as a motive for the attack. During the trial against S., the German Federal Prosecutor General characterized the attack as “intended to create a climate of fear among all persons engaged with refugee affairs” (Rath, 2015)<sup>8</sup>. S. was sentenced to 14 years in prison for attempted murder and grievous bodily harm in four cases (Deutsche Welle, 2016).

However, although clearly intended by S., the attack did not create widespread fear in society. Reker was elected mayor of Cologne only one day later while still being in a coma and her political opponent, Jochen Ott, stopped his campaign on October 17 out of solidarity (Rath, 2015). Furthermore, because Frank S. was arrested during the attack and was clearly identified as a lone operator, the citizens of Cologne did not expect further attacks. Rather than fear, anger, outrage, and fury dominated the public discourse after the attempted assassination of Henriette Reker. Thus,

---

<sup>8</sup> Translated from the German original: “(...) S. habe ein „Klima der Angst“ bei allen in der Flüchtlingsunterbringung engagierten Personen erzeugen wollen.”.

it seems that Frank. S. committed an act of terrorism that, although intended, did not spread a large amount of fear in society

However, does this mean that one should abolish the requirement of fear as a necessary condition of a terrorist attack entirely? Surely, that would run the risk of losing a key explanatory feature of terrorist attacks; namely how terrorists create the necessary publicity (or audience) to communicate their ideological aims. Rather, I argue one should not entirely eradicate fear from the core characteristics of a terrorist attack but widen this characteristic. Instead of the rather narrow emotion of fear, it seems more accurate to assume that a terrorist attack produces a wide variety of negative emotional responses ranging from fear and horror to powerlessness and further to anger, fury, and rage.

Thus, I argue that not fear alone but *moral outrage*<sup>9</sup> as a consequence of an attack is a necessary condition to define said attack as terrorism.<sup>10</sup> This approach both includes lone wolf terrorist attacks that do not manage to create widespread fear and it introduces moral outrage as a causal factor for

---

<sup>9</sup> Moral outrage is commonly defined as “anger at the violation of a moral standard” (Batson et al., 2007; Johansen et al., 2018; O’Mara et al., 2011, p. 173). Yet, while I generally agree with this definition, it is noteworthy that moral outrage can be seen as including – or at least as being highly influenced – by anxiety or horror at a morally abhorrent event (Johansen et al., 2018, p. 4). This abhorrent event is often capable of causing moral injury in terms of involving the loss or threatened loss of what we deeply care about (e.g. family members, friends etc.) (Miller, in press). Chapter 2 of this thesis will discuss the psychological impact of terrorist attacks including fear and moral outrage in detail.

<sup>10</sup> Note here that the creation of moral outrage does not necessarily have to be the intention of the attacker to define her act as terrorism. Rather, it is a sufficient condition if the attacker intends to create fear instead. For example, a religiously motivated terrorist might not expect to create moral outrage with her violent act, simply because she firmly believes that her attack is the morally just thing to do. Yet she might very well intend to create fear among the “immoral unbelievers”.

the publicity element in terrorist activities. However, this approach does not come without issues. For example, it seems not entirely clear what degree of public moral outrage is necessary to ensure a proper audience for the terrorist to communicate her ideology.

To sum up, it has been shown that widespread fear does not have to be the actual consequence (or realized intention) of an attack to call this attack an act of terrorism. Rather, the more general term of moral outrage seems to be sufficient to characterize the response to an act of violence against [innocent] persons. However, while Frank S. clearly had the intention to create fear and indeed produced moral outrage, other cases come to mind in which a would-be terrorist might not intend to create moral outrage and fear but did so unintentionally. These cases will be analyzed in the following segment.

#### B) As unintended outcome

At first sight, it seems hard to think of cases in which a person commits an act of violence against [innocent] persons without intending to spread moral outrage or fear. The intentional, indiscriminate killing of [innocent] persons seems to be inevitably bound to the intention to create an atmosphere of fear, anger, and horror. Thus, it does not seem too farfetched to conclude that the intention to create moral outrage and especially fear should be a necessary condition to call such violent actions acts of terror. This initial intuition can be supported by a theoretical discussion of the actions and intentions involved in an act of terrorism:



Although not a necessary outcome of a terrorist attack, the characteristic of creating fear among an audience has to be an intention of the perpetrator to call an attack an act of terrorism for a simple reason: as briefly discussed in chapter 1.3., the perpetrator of a terrorist attack intends to alter the behavior of a target audience with her attack. The intention to make an audience “believe” the ideological message that is transported with the attack can have various forms ranging from altering the behavior of society (e.g., avoiding public events like Christmas markets) to influencing policy making (e.g., accepting the autonomy of certain regions). While this intention to make an audience believe a certain ideological message does not necessarily have to be a consequence of an action to call said action terrorism, it is a necessary *intention* of every perpetrator of a terrorist attack. Section 4.3. of this chapter will give detailed reasons for this assumption.

However, for the current discussion, it is most important to note that, if the characterization of making an audience believe an ideology is a necessary intention for terrorism, then the creation of fear also has to be a necessary intention of a terrorist as well: the terrorist aims to convince the audience of the strength of her ideology in order to alter the behavior of this audience. The rationale behind this strategy is that the audience will alter its behavior because the members of this audience are *intimidated*. For example, the assailant in the attack against Henriette Reker did not only intend to communicate his right-wing ideology with his violent act but also intended to spread fear in order *to alter the behavior* of the refugee supporters in Germany. He hoped that his attack might frighten volunteers and politicians enough to end their support in fear of getting attacked as well. Thus, the

intention to create fear is necessarily bound to one of the core strategical aims of terrorism – to influence society and policymaking.

Of course, this argument does not come without certain difficulties. For example, attacks by certain religious cults would not count as terrorist attacks according to this analysis, if the cult members have the (somewhat abstruse) intention to spread love or other positive emotions with their attacks. Arguably, the Japanese death cult Aum Shinrikyo could serve as an example of such cults. However, if the members of Aum Shinrikyo did, in fact, performed their attacks in the strong believe to *only* save the souls of their victims and to save humanity from Armageddon (a view that is contested), then also other characteristics like the communication of an ideology are absent in Aum's attacks (Watanabe, 1998). Hence, if Aum was, in fact, an entirely delusional cult with the sole aim to save their victims' souls by killing them, it does not seem too farfetched to reconsider the choice to call this group a terrorist organization.

To sum up, it has been shown that the characteristic of creating fear is a necessary condition of terrorism in terms of being an intention of an attacker. However, it has further been shown that this characteristic does not have to be the *realized* intention to define an attack as terrorism. Here, the broader term of moral outrage is more accurate to account for the variety of emotions that are involved in the public response to a terrorist attack.

## 4.2. Act of violence against [innocent] victims

### A) As intention only

Some researchers, as well as institutions, argue that the characteristic of violence against [innocent] persons only has to be intended (or threatened) to count as terrorism or to prosecute the perpetrator/conspirator as a terrorist. For example, Schmid states that terrorism consists of “physical violence or threat thereof” (A. P. Schmid, 2012) and NATO refers to terrorism as “[t]he unlawful use or threatened use of force or violence” (North Atlantic Treaty Organization, 2014, p. 5). Furthermore, also the U.S. Department of Defense defines terrorism, amongst others, as the “unlawful use of violence or threat of violence” (U.S. Department of Defense, 2010, p. vii). As seen in these definitions, especially in legislative definitions, an act in which violence is only intended (or here threatened) but not committed can count as terrorism under the condition that the other two core characteristics of terrorism are present.

However, this position includes a variety of problems. If a person only threatens to use violence against [innocent] persons, an act of violence has not happened. Hence, it seems counterintuitive to call such a threat an act of terrorism – even if this threat caused fear and communicated ideological aims to some degree. Intuitively, one could argue by analogy that it would also be absurd to call the threat of committing a school shooting an actual school shooting. Yet again in the case of terrorism, one could argue that the characteristic of communicating ideological aims by issuing threats of violence is sufficient.

However, on a more theoretical level, it can be shown that the threat of violence is *a different kind of action* compared to an actual act of violence. A threat to commit an act of violence is a communicative action involving – if it is not an empty threat – an intention to commit violence. This communicated intention is the intention to commit an act of violence against the [innocent]. A convincing reason for treating threats as separate actions can be identified by looking at the role of intentions involved in an act of threatening to commit violence against the [innocent]. It does not seem obvious at all to assume that every person who threatens to commit an act of violence also *intends to act* in such a manner. Rather, practitioners in the field of counter-terrorism report that most threats of violence by would-be terrorists turn out to be hoaxes (UK National Counter Terrorism Security Office, 2016, Chapter 5).

From the perspective of action theory, this poses a serious problem to the approach to call threats to commit violence against the innocent terrorism: since we cannot be certain about the real intention behind a threat, it may very well be the case that a person that threatens to kill or seriously harm [innocent] people for ideological reasons does not intend to harm anybody. Calling such a threat terrorism would leave us with a definition of terrorism in which the characteristic of seriously harming [innocent] people does not play a role at all – not even in the form of an intention to seriously harm.

In practice, such a position would lead to a dangerous slippery slope: According to this interpretation of threats, even hoax calls or tweets threatening – but not actually intending - to commit a violent act against innocents for ideological reasons should be regarded as actual terrorism.

Even worse, the inclusion of such empty threats as constituting terrorism has the untoward consequence that simple ideological statements that induce fear to a certain degree would count as terrorism.

Another possible scenario in which the characteristic of killing or harming [innocent] victims is only present as an intention is the attempted terrorist attack. Contrary to the case of the threat, the act of attempting to commit an act of violence against the [innocent] includes the intention of the perpetrator to do so in almost any case.<sup>11</sup> Thus, such a scenario would include all three characteristics (i.e., seriously harming the [innocent], communicating an ideology, creating fear). Note that the characteristic of killing or harming [innocent] people is an unrealized intention of the perpetrator, if it is an unsuccessful attempt. In this case, the judgment of whether such an attempt would count as terrorism is not as obvious as in case of a threat.

One could argue that even an attempted act of terrorism (especially with unconventional weapons like CBRN weaponry<sup>12</sup>) involves the actual, as well as intentional, communication of ideological aims and intends to create and spread fear to some considerable degree. An outrageous plot with CBRN agents has the capability to communicate the message to the audience that everyone could *potentially* be the target of an attack. However, I argue that an unsuccessful attack should not be called an act of terrorism.

---

<sup>11</sup> Of course, in all of the discussed cases, multiple layers of deceptive behavior in the sense of *pretending to attempt to commit an act of terrorism* are possible. However, for reasons of simplicity, these cases are excluded from the present analysis.

<sup>12</sup> See, e.g., the case of the Cologne ricin plot.

From a theoretical perspective, it can be argued that the unrealized intention of harming the [innocent] renders other characteristics to define terrorism invalid. Specifically, this unrealized intention does not create an extensive amount of moral outrage. Yet, as will be shown in the last section of this chapter, only extensive publicity and, thereby, an audience to receive and understand the ideological message that the perpetrator would like to send. For example, if a terrorist stabs a random, [innocent] person on the streets, this act would cause a large extent of publicity.<sup>13</sup> The random nature of the attack against the [innocent] victim suggests that anyone could be targeted and killed at any time. Hence, people tend to identify themselves with the victim and, thereby, become responsive to the perpetrator's message.

Yet in some cases of attempted attacks against [innocent] persons, the created publicity might be extensive, but the extent of moral outrage is arguably too weak to create a responsive audience, let alone a fearful one. For example, on December 10, 2012, an undetonated IED was found and defused by German police officers in the train station of Bonn (Deutsche Welle, 2014; Hudson, 2014). In the aftermath of this incident, the responsible investigators identified a radicalized German Muslim, Marco G., as perpetrator of the plot. Currently, Marco G. is awaiting trial and, if prosecuted, is facing charges such as attempted murder and attempted detonation of an IED (Hudson, 2014). The IED turned out to be full of construction mistakes and, thus, never posed a threat to the people at the train station. This attempted attack was mentioned in national media and, to some degree, started a discussion concerning Islamist lone operators and

---

<sup>13</sup> This effect is observable in the media coverage of stabbings in which the perpetrator has (suspected) ties to terrorists.

security measures on train stations in Germany (Deutsche Welle, 2014; Hudson, 2014). However, it did not achieve what Marco G. intended with the attack, namely to successfully communicate his Islamist beliefs to the German public.

Due to the failure of his attack, the German public was certainly outraged to a certain degree but not (or not enough) able to identify themselves as the recipients (or audience) of G.'s action. In fact, many people were relieved that the attack did not happen and that the perpetrator was arrested. Thus, the absence of violence in Marco G.'s attempted attack meant that there was a lack of moral outrage and, as a result, his attempted attack did not allow him to widely communicate his ideology. Marco G.'s attempt to commit an act of terrorism failed.

Yet, as will be shown in this thesis, especially in case of attempted or prevented attacks that involved CBRN weapons, the moral outrage and, furthermore, the publicity could be sufficient to enable these attacks to count as acts of terrorism. However, in practice, the inclusion of these cases would blur the border between terrorism and conspiracies to commit an attack to the degree that generates counterintuitive border-line cases. For example, if we define *all* cases of attempted terrorist attacks as terrorism, then we would be obliged to not only include cases like Marco G.'s failed attack but also every failed or averted conspiracy to plan an attack. Even a conversation between activists about the intention to plan a violent attack against the [innocent] would be an act of terrorism according to this inclusive definition. This does not only seem counterintuitive but also raises the question of what stage of planning or attempting to commit an attack is

necessary to call this attempt terrorism. The border between terrorism and formulating an intention to commit such an attack is blurred. Furthermore, such an inclusive approach can be criticized from a normative perspective: to commit to this interpretation would mean that every attempt or prevented plan to commit an act of terrorism would count as terrorism. That would unduly credit groups like the self-proclaimed Islamic State of Iraq and the Levant (ISIL) with successes that they do not have – thereby greatly enhancing their status - since ISIL could claim every single attempt as a successful act of terrorism and another win for their ideology.

Closely related to the case of attempted terrorism are cases of attempted violence against the [innocent] that are successful in the case of the violence but unsuccessful in directing this violence at [innocent] people. A thought experiment might clarify this species of border cases: A radicalized individual with a kitchen knife has the intention to kill a random, [innocent] person to communicate his ideological beliefs to the public. He picks a random person and stabs his victim. After this attack, he places a written claim of responsibility next to the dead body, quickly leaves the crime scene and gets to a hide-out in the belief that his act of terrorism was a success. However, the next morning the perpetrator buys a newspaper and reads the following headline:

*Gruesome foreign dictator assassinated. The assassin appears to be a political opponent or avenger who “(...) killed this person to show that my God will judge every single one of you” according to a written claim of responsibility that was*



*found next to the dead. The killed dictator was responsible for one of the largest genocides in the twenty-first century.*

In this thought experiment, the perpetrator had the intention to kill an [innocent] person but did not manage to realize this intention: While he certainly committed an act of violence, he did not succeed in aiming this act towards *an [innocent] person*. Yet one could argue that this case should be added to the definition of terrorism since the perpetrator intended to kill [innocent] people as well as *actually* killed a person and communicated his ideological message.

However, I argue that this case is not terrorism. Similar to the case of the attempted attack of Marco G., the necessary, extensive moral outrage in this thought experiment is missing because the victim was not [innocent]. The newspaper article shows that the assassination of the dictator received public attention to some degree and that the attack sent an ideological message. However, it was not the message the perpetrator intended to send. His intended message did not reach anyone because his attack did not manage to create the intended moral outrage: since a serious human right abuser was killed in the attack, it was impossible for [innocent] people<sup>14</sup> to identify themselves as the recipient of the ideological message (“I killed this person to show that my God will judge every single one of you”). Thus, the attack failed and should not be considered an act of terrorism.

---

<sup>14</sup> Of course, to some degree dictators around the world might have been morally outraged and understood the message, but that surely was not the intended audience of the perpetrator.

To sum up, rather than adding cases of threatened or attempted attacks to the definition of terrorism, we should call these cases what they are in terms of the actions: The threat of terrorism as an own action and attempted terrorism as an unsuccessful intention to commit an attack against the [innocent].

#### B) As unintended outcome

Another interesting problem in defining terrorism are cases in which the act of violence against the [innocent] is not intended but an unintended consequence. Examples are cases in which the perpetrator intended to communicate ideological aims without using violence but unintentionally caused the death of [innocent] people with his or her action. A prominent case for such a scenario is a failed act of sabotage such as the Sterling Hall bombing:

In the night from August 23 to August 24, 1970, an explosive device detonated behind the Sterling Hall Research Center at the University of Wisconsin in Madison and killed the physicist Robert Fassnacht (Cronon & Jenkins, 1999, p. 517; Madison Capital Times, 1970). The perpetrators of this attack were later identified as Dwight Armstrong, his brother Karleton Armstrong, David Sylvan Fine, and Leo Burt. The Armstrong brothers planned and executed the attack together with their co-conspirators as members of the radical leftwing group “New Year’s gang” (Cronon & Jenkins, 1999, p. 517; Madison Capital Times, 1970). According to the group, no civilians should get hurt in the attack that was aimed at the Army Mathematics Research Center (AMRC) in the Sterling Hall Building (New Year’s Gang, 1970). However, although the group executed a warning call,

the detonation occurred prematurely and, thereby, killed Fassnacht, who happened to be in the building at that time (Bates, 1992, p. 307; Fellner, 1986).

This example is an interesting border case between sabotage and terrorism. Intuitively, many people would call – and have called – the New Year’s gang a terrorist group despite the fact that the group did *not intend* to use violence directly against human beings, as opposed to buildings, to communicate their cause. Philosophers like Frances Kamm (Kamm, 2011) and David Rodin (Rodin, 2004) would argue in favor of this view, as shown in another, slightly different, example below. The rationale behind this view is the fact that all criteria used to define terrorism seem, at first glance, to be present in the outcome of the action: the group killed an [innocent] person in an act to communicate ideological aims and spread fear. However, by analyzing this example more closely, a crucial problem arises: While it is obvious that the New Year’s gang managed to communicate their ideological agenda with the attack, it does not seem reasonable to assume that the Sterling Hall bombing created moral outrage comparable to cases like the assassination attempt of Henriette Reker.

I argue that the reason for this lack of moral outrage is the intention of the perpetrators not to kill an [innocent] person: Shortly after the attack, news media reported that the New Year’s gang issued a warning call to avoid casualties. In fact, the group regretted Fassnacht’s death in their claim of responsibility (New Year’s Gang, 1970). This information caused the audience of the incident to characterize the attack as an act of sabotage in which the perpetrators caused Fassnacht’s death by means of recklessness

and negligence. While the incident certainly caused a certain degree of moral outrage, the public seems not to have identified itself as the intended recipient of the message. Since it was never the intention of the New Year's gang to harm the [innocent], the US public arguably never understood the attack as being directed against them.<sup>15</sup> However, this creates the extent of moral outrage that is necessary to call an attack a terrorist attack. The lack of extreme moral outrage due to the *unintentional* killing of Fassnacht was also the basis for the indictments against the group that characterized the crime as an act of sabotage with manslaughter (third-degree murder) – and not as terrorism.

Another set of cases that involves the unintentional killing of [innocent] people is collateral damage as a result of a military airstrike that aims at targeting legitimate targets<sup>16</sup> only. These cases shall be the second border case of attacks in which the characteristic of harming [innocent] people is an unintended outcome in an action that communicates ideological aims. In contrast to most of the other border cases that have been discussed in this chapter so far, the case of collateral damage has already been discussed by several philosophers in connection to action theory. Thus, rather than presenting an own account of this dilemma, I will comment on the existing discussion on whether we should regard airstrikes with collateral damage as terrorism.

---

<sup>15</sup> Yet, admittedly people might have been scared to a certain degree to fall victim to another failed act of sabotage by being in the wrong place at the wrong time.

<sup>16</sup> Of course, the notion of a legitimate target in the theatre of war is troubling. However, this paper will define a legitimate target pragmatically and in accordance with the *Jus in Bello* doctrine as a military combatant or military infrastructure (more detailed discussions (Kamm, 2011; Miller, 2016; Schwenkenbecher, 2014)).

Proponents of this view are amongst others David Rodin and Frances Kamm (Kamm, 2011; Rodin, 2004). According to Rodin, not the intention of the perpetrator, but the wrongfulness of his or her action should determine whether the action should be included into the definition of terrorism that Rodin characterizes as “the deliberate, negligent, or reckless use of force against non-combatants” (Rodin, 2004, p. 755). Rodin explicitly proposes to call cases of reckless or negligent, yet unintended, killing of the [innocent] terrorism (Rodin, 2004, p. 755). Kamm presents a similar argument.<sup>17</sup>

Specifically, Rodin argues that a military operation that results in [innocent] casualties should be regarded as morally impermissible if said operation does not obey the doctrine of double effect. This doctrine maintains that one ought to apply a proper, very high standard of care to avoid civilian casualties in military operations. Since a case that does not adhere to this doctrine would generate [innocent] casualties by means of acting reckless or negligent (yet not intended), Rodin argues that those cases of collateral damage can be seen as morally equivalent to the deliberate targeting of [innocent] people in a terrorist attack. Thus, Rodin proposes to add the unintended but reckless or negligent harming of [innocent] people to the definition of terrorism.

---

<sup>17</sup> Kamm implicitly agrees with Rodin’s view by emphasizing that intention seems to play a minor role (or no role at all) in the moral assessment of an action (Kamm, 2011, pp. 73–118; Miller, 2012). However, while Kamm uses an example of a fictional terrorist group for her argument, she does not explicitly propose to include cases of collateral damage in the definition of terrorism. Specifically, Kamm presents the example of a fictional “Baby Killer Nation (BKN)” which intentionally kills infants but only if the deaths are legally permissible, collateral damage as part of an otherwise just airstrike (Kamm, 2011, p. 79; Miller, 2012). To Kamm, this action seems ethically equivalent to a scenario in which the same amount of infants were killed unintentionally in terms of being collateral damage of an otherwise just airstrike.

However, this position has been criticized. For example, Jeff McMahan, as well as Stephen Woodside and Seumas Miller, show in convincing arguments that intention, in fact, plays a crucial role in the moral assessment of an action (McMahan, 2009; Miller, 2012; Woodside, 2013). Seumas Miller argues that cases in which the [innocent] are killed as *unintended* collateral damage do not show that intention is irrelevant to the ethical assessment of terrorist attacks. Rather, according to Miller, multiple layers of (morally conflicting) intentions can be identified in the ethical assessment of terrorist attacks and these emphasize the importance of intentions in moral assessments (Miller, 2012).<sup>18</sup> Additionally, McMahan and Woodside show in more general arguments that the moral distinction between intentional and unintentional actions is not only a very strong, common intuition but also gives coherence to the core of our moral beliefs (McMahan, 2009, pp. 888–889; Woodside, 2013, pp. 258–259).

This critique renders Rodin’s claim to integrate cases of collateral damage into the definition of terrorism invalid from a normative perspective. It shows that just airstrikes with collateral damage should not be seen morally equivalent to terrorism. However, even if we would manage to discard this criticism and show that collateral damage is, in fact, morally equivalent to terrorism, it still seems implausible to call these cases terrorism. This becomes clear by including the other two characteristics of terrorism, i.e.,

---

<sup>18</sup> According to Miller, Kamm’s BKN example does not eradicate intention from the moral assessment of situations involving collateral damage. Following Miller, the action of the BKN group is not only motivated by the intention to kill infants, but also by another intention; namely the intention to comply with the legal concept of collateral damage in doing so. Thus, the fact that BKN can be seen as morally equivalent to cases in which infants are killed as *unintended* collateral damage does not show that intention is irrelevant for this ethical assessment. Rather, multiple layers of (morally conflicting) intentions (i.e., killing infants vs. obeying the rules of engagement) can be identified in the assessment.

the communication of ideological aims and the creation of fear, into Rodin's discussion. In doing so, it can be shown that moral equivalence alone does not qualify an action as terrorism.

For example, an act of genocide can be seen as, at least, morally equivalent to an act of terrorism. Yet, most researchers agree upon not including these cases into the definition of terrorism. Just as in the case of a military airstrike or bombing with collateral damage, an act of genocide does, first and foremost, not intend to communicate an ideological message to a broader audience. Rather than communicating an ideology to a group, genocide aims at eradicating said group for ideological reasons. A military airstrike usually intends to kill combatants or destroy infrastructure that is perceived to be a threat. The communication of an ideology can be involved in an attack against legitimate military targets but is, if at all, a secondary intention. For example, U.S.-lead airstrikes against ISIL training facilities in Iraq had the intention to destroy these facilities in order to contain the threat ISIL is posing to the region and the Western world.

Of course, such an attack also sends a political message to ISIL, a group of serious human rights violators. However, this communicative component of the attack is a byproduct since the U.S. military actively chose this specific training camp as victim *and* target of its attack – not as a random victim to send a message to a broad target audience.

One could object that such an airstrike very well sends a political message to a broader audience if [innocent] people were (unintentionally) killed in the course of this action. Collateral damage in the course of an airstrike

causes moral outrage and fear in societies, and this fear has repeatedly been used by groups like ISIL to recruit new members. In this line of reasoning, it can, in fact, be argued that these airstrikes are sending a political message and are causing moral outrage among [innocent] people in Pakistan, Iraq, Syria, and other countries. However, this communication of ideological goals and this spreading of moral outrage among an [innocent] audience was not intended by the perpetrator of the attack but is a byproduct of the attack. In fact, it harms the cause of the perpetrator more than it helps. As will be shown in section 4.3., such cases of unintentionally communicating ideological aims to an audience cannot (and ought not to) be seen as terrorism. However, this exclusion from the definition of terrorism does not mean that collateral damage during airstrikes might not be morally abhorrent and inexcusable in some cases. Yet, this is a normative debate that should be treated separately from the discussion concerning the definition of terrorism.

In summation, analyzing the characteristic of harming the [innocent] from the point of view of action theory reveals interesting border cases in the definition of terrorism. It has been shown that neither threats or attempts to perform a terrorist attack, nor failed acts of sabotage or airstrikes that produce collateral damage should be added to the definition of terrorism. Thus, not only the intention to kill or seriously harm [innocent] victims but also its realization is a necessary condition to call an action an act of terrorism.



#### 4.3. Act of communicating ideological aims

A last, yet essential, characteristic to define terrorism is the act of communicating an ideology to an audience. To regard an act of violence as an act of terrorism, the perpetrator of this attack has to have a political, religious or other ideological motivation for this attack that he or she communicates through this act to an audience. An act of violence against the [innocent] that spreads moral outrage but does not involve an ideology cannot qualify as terrorism but may, for example, be a school shooting or a case of mass murder. As seen in section 2.3., the communication process during a terrorist attack can be characterized as multistage communication of understanding and believing. While it seems clear that a case in which a violent action against the [innocent] involves the creation of moral outrage as well all of the above stages of communication should count as terrorism, other scenarios involving this characteristic are less clear and, hence, interesting to investigate.

##### A) As intention only

First of all, in order to call an act an act of terrorism, the perpetrator has to communicate the violent attack itself to the public. However, does this process of communication has to be a realized intention or is it sufficient if the perpetrator only intends to communicate his or her violent act to the public? Assume a thought experiment in which a would-be terrorist intends to send a political message by stabbing an [innocent] person. However, he stabs a homeless person on a bridge and the person falls into the river under the bridge. Nobody witnessed the attack. The perpetrator informs several

newspapers about the attack, but no journalist believes him since no missing person was reported and no body was found. The perpetrator clearly intended to communicate his crime to the public but did not succeed. Obviously, such an attack cannot qualify as terrorism since there is no publicity and, thereby, no chance to communicate ideological goals. The would-terrorist failed in his attempt to perform an act of terrorism but is obviously guilty of murder.

Secondly, let us assume that the perpetrator stabbed a person that did not fall into the river. The perpetrator realized his intention to communicate to the public that he killed an [innocent] person. However, he did not succeed to communicate his political agenda because the written claim of responsibility that he placed next to the body fell into the river. Thus, the attack is publicly believed to be a random murder. The obvious problem in assessing whether such a case should be called an act of terrorism or not stems from an epistemic uncertainty: If the perpetrator of the attack was driven by an ideological intention, but failed to communicate this intention, then the public is unable to know that he had the intention to communicate a certain ideology in the first place. While this seems comparable to a case of an (unsuccessfully) intention to commit an act of violence that nobody knows about (which would clearly not be terrorism), the case of an unsuccessfully intended act of communicating an ideology is different in an essential part: it can be realized through persons other than the one intending it.

It is easy to think of scenarios in which it is publicly known that a person had the intention to kill innocent people but did not (succeed to) do so. This

person would not be a terrorist. However, when it comes to the act of communicating ideological aims, the public knowledge of the intention to communicate these aims is already a sufficient condition to turn this intention into a realized intention. In the case of the thought experiment, it is thinkable that the police investigates the stabbing of the [innocent] person and publishes evidence that the perpetrator intended to communicate certain ideological aims with his action. With its publication, this intention immediately turns into a realized intention. Hence, this intention turns into a realized intention (consequence) of the attack as soon as these findings are published and reported by the media. Although not instantly successful, the perpetrator's intention of communicating an ideology becomes successful as soon as one discovers it.

This mechanism of discovery still works months or even years after the original action. Take, for example, the Oktoberfest attack from 1980 in Germany (Chaussy, 1985; Ravndal, 2015, pp. 22–23). Originally, the attack, in which the student Gundolf Koehler killed 12 persons with a pipe bomb, was portrayed as politically unmotivated crime. Yet, years after the attack the discovery of new evidence that directly connected Koehler's attack to right-wing extremist networks "turned" the attack into a terrorist attack. Specifically, this new evidence turned Koehler's (until then unsuccessful) intention to communicate his right-wing ideology with the attack into a realized intention (Chaussy, 1985).

Thus, scenarios in which a person only intends to communicate ideological aims by committing an act of violence against the [innocent] should, indeed, count as terrorism, if this intention is publicly known and, thereby,

automatically realized. However, if such an intention is never discovered, then the action stays in some sort of quantum state and could potentially turn into an act of terrorism as soon the intention is to be discovered. If not, it is impossible to know if such an action is an act of terrorism.

Thirdly, let us assume cases in which a terrorist succeeds in their intention to communicate their crime as well as their ideology but fails in their intention to make an audience *believe* in their ideology. A suitable example of such a case is the 2011 Oslo bombing that was planned and executed by the Norwegian right-wing extremist Anders Behring Breivik. On July 22, 2011, Breivik killed eight people and left at least 209 persons injured with an IED attack in Oslo (Appleton, 2014; Berntzen & Sandberg, 2014; Harris, 2011; Mala & Goodman, 2011). Only 90 minutes later, he gained access to a Youth camp of the Norwegian party Arbeidernes Ungdomsfylking (AU) on the Norwegian holiday island Utøya and executed 69 people, most of them adolescents, in a one hour lasting shooting rampage. (Appleton, 2014; Berntzen & Sandberg, 2014; Harris, 2011).

As the investigators described shortly after arresting Breivik, he could be characterized as a lone operator influenced by far-right, radical Christian, and islamophobic ideologies (Daily Mail, 2012; Erlanger & Shane, 2011; Taylor, 2011). This characterization of Anders Behring Breivik's political mindset was validated by Breivik himself, who had sent a 1518 pages long ego-document to 1,003 addresses via email shortly before the attacks (Breivik, 2011). In this document, Breivik described in detail that he perceives himself as "Commander (...) and one of the several leaders" (Breivik, 2011) of a fictional movement that he calls the Pauperes

commilitones Christi Templique Salomonici (PCCTS) Justiciar Templers. Furthermore, Breivik claimed that his attacks, as well as future attacks executed by this organization, should be seen as political acts of Christian resistance against what he calls the islamization of Europe through “Cultural Marxism” (Breivik, 2011).

Breivik clearly intended with the attack to make the Norwegian Government and society believe that his right-wing ideology of PCCTS would be the last bastion against the “islamization” of the country. Furthermore, he wanted to induce the belief that the movement of PCCTS is able to strike at any time until its demands are fulfilled. However, shortly after Breivik’s manifesto was reviewed by the authorities, it was publicly reported that Breivik’s PCCTS movement was not more than a fantasy of the terrorist. Rather than being part of an organized terrorist group, Breivik was a lone operator. While being outraged and shocked by the extent of violence during the attack, the Norwegian government and society did not give in to Breivik’s demands and did not fear further attacks from PCCTS. Thus, Breivik’s intention to make the Norwegian public to *believe* his ideology was an intention only.

However, although Breivik did not manage to cause the Norwegian public to believe in his ideology, it would seem counter-intuitive to exclude his attack from the definition of terrorism. A reason for that may be the hypothesis that it is not clear whether terrorism as a strategy to change policies or to infuse ideologies into society is an effective strategy in general. In fact, researchers like Max Abrahms, Richard English or Eric Gould doubt that the strategy of terrorism could be seen as a successful

means of political agendering at all (Abrahms, 2006; English, 2016; Gould & Klor, 2010). Although most certainly intended by terrorists, governments or societies do not seem to believe that right-wing extremism or Islamist extremism are powerful or convincing enough to cause them to change their policies or to abolish their way of life in favor of the terrorist's ideology. Yet, terrorist attacks cause moral outrage, panic, and sometimes even military interventions. Thus, it can be argued that the characteristic of making an audience believe a certain ideology is certainly intended by the perpetrator of a terrorist attack but does not have to be a realized intention of the attack to call it an act of terrorism. If one would demand this characteristic to be a necessary condition for terrorism, then one would equate the term terrorism with *terrorism as a successful strategy to influence politics and society*.

#### B) As unintended outcome

The above-described examples are cases in which the perpetrators of attacks indeed had the intention to communicate their ideological goals. Yet, there are cases thinkable in which ideological aims were unintentionally communicated during an attack. Here, especially those cases are interesting in which the audience of an attack misunderstood this attack to be ideologically motivated. In these cases, the characteristic of communicating ideological aims is an unintended consequence of said action. One recent example of such a case is the Munich shooting (2016) in Germany.

On July 22, 2016, the German-Iranian high school student David Ali Sonboly killed ten persons and wounded another 36 during a shooting spree

close to the Olympia shopping mall in Munich. After the attack, Sonboly committed suicide (Callimachi et al., 2016). Investigators later found out that Sonboly committed the attack specifically to revenge bullying in school.<sup>19</sup> Yet, during the attack, both the German police and the media reported that the shooting was a suspected terrorist attack. In addition to that, several individuals related to ISIL publicly applauded the attack and suggested that Sonboly should be seen as a combatant of the group. Additionally, Sonboly's heritage and several eyewitnesses report that Sonboly shouted "Allahu Akbar" during the attack (later discarded as untrue) mischaracterized the attack as an Islamist terrorist attack with the intention to communicate the apocalyptic ideology of ISIL (Callimachi & Eddy, 2016). Thus, in addition to the successful intentions of committing an act of violence against [innocent] people to spread fear, Sonboly's attack had the unintended consequence of communicating an Islamist ideology.

During the aftermath of the attack, more accurate details about Sonboly's motivation surfaced and the classification of the attack as an act of terrorism was discarded by the investigators. However, parts of the German society refused to abolish the narrative of Islamist terrorism with regard to this attack for weeks. Fueled by other attacks in the area that, in fact, were acts of Islamist terrorism, this narrative continued to spread. In this case, some people might argue that the characteristic of communicating an ideology only has to be present as an unintended consequence to call an attack an act

---

<sup>19</sup> Note that during the time of writing this thesis, German security officials published evidence that Sonboly's attack might have been motivated by right-wing extremist ideologies (Bernstein, 2017).

of terrorism. After all, it has to be acknowledged that groups like ISIL implicitly profited from the attack regardless of its perpetrator's intentions.

Yet, it seems counterintuitive to accept the position that attacks like the Munich shootings should be called acts of Islamist terrorism solely based on its consequences. Accepting this position would mean that every single act of violence should be defined as an act of terrorism if false or insufficient information about the perpetrator's intention is available. Such an approach is not only too inclusive to define terrorism but also leads to dangerous consequences: It would shift the definitory power over what should count as terrorism to the strongest public narrative. If, for example, the public and the media implicitly agree to interpret a certain attack as an act of terrorism, for example, because of the perpetrator's heritage, this narrative defines the act as terrorism regardless of the intention of the perpetrator. This not only leads to (further) political instrumentalization of the term terrorism but also helps groups like ISIL to redefine and reframe violent acts around the world as acts of Islamist terrorism. Thus, the communication of ideological aims as an unintended outcome is not, and ought not to be, sufficient to call an act of violence against the [innocent] an act of terrorism.

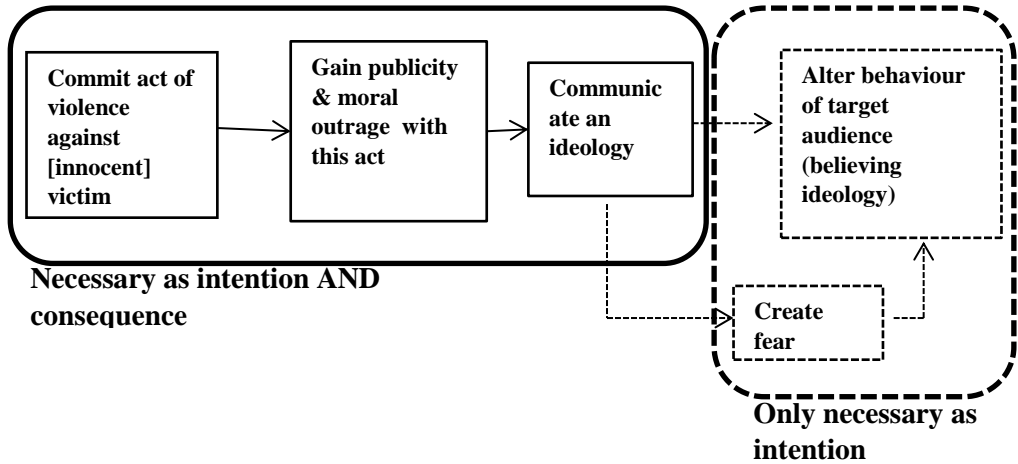
To sum up, it has been shown that the intention to communicate an ideological message to an audience and cause the audience to believe it is a necessary condition for an attack to count as an act of terrorism. Furthermore, this intention to communicate has to be public. Accordingly, the intention to cause the audience to know what the message is has to be realized if the attack is to count as a terrorist attack. However, it is not



necessary that the audience believe the message to be true for the attack to count as an act of terrorism.

## 5. Conclusion

This chapter has shown that popular border cases arising from the definition of terrorism can be successfully analyzed by deploying some basic action theory. Problems in defining terrorism were identified and possible solutions to these problems were offered by distinguishing between the intended, realized and unintended elements of terrorism. This chapter identified a set of individually necessary and jointly sufficient conditions of an action to count as an act of terrorism. This set consists of the three main characteristics of terrorism that were characterized in each case as either an intended (but unrealized) consequence of an action, an intentionally realized consequence or an unintentionally realized consequence of an action. On the basis of this analysis, one can construct an ideal type of an act of terrorism that includes all three characteristics and their respective sub-categories either as intentions only or as realized intentions.



*Fig. 1: Necessary elements in an act of terrorism*

This figure shows that an analysis of the most common characteristics and their respective sub-categories of terrorism allows to further specify what should be considered an act of terrorism. According to the results of this analysis, *terrorism is a deliberate, public act of violence against [innocent] victims that aims at spreading fear and has the publicly known intention to communicate an ideology.*

Here the action of violence is intended and realized; the act is intended to be publically communicated and is publically communicated causing moral outrage. Moreover, the act is intended via its publicity to create fear but might not in fact do so; and the act is intended to communicate an ideology and does communicate the ideology, yet this ideology is not necessarily believed.

Of course, this action-sensitive approach to the definition of terrorism does not come without a certain vagueness. Therefore, there are some borderline

cases that cannot be included or excluded beyond any doubt from this definition. For example, a dilemma evolves out of a publicly *unknown* intention to communicate an ideology that forces a terrorist act into a quantum state between crime and terrorism. However, the discovery of these additional challenges to the definition of terrorism should be seen as additional, valuable outcomes of this analysis. Specifically, one border-line case that was discussed in this first chapter will be of particular interest for the present thesis. The question of whether an outrageous attempt of terrorism with novel weaponry such as CBRN has the power to spread enough fear and moral outrage to count as a successful case of terrorism leads to questions concerning the impact of powerful weapon technologies in the hands of terrorists. In the next chapters, I will argue that some weapons do not have to produce any casualties or destruction to spread fear and damage institutions.

## **2. Concepts and frameworks of WMD and CBRN**

### **1. Introduction**

The concept of WMD is part of numerous national laws and is the core of the most important treaties of the United Nations (Organisation for the Prohibition of Chemical Weapons, 1992; United Nation Office of Disarmament Affairs, 1975). Yet, the definition of what should be considered a WMD is far from established and subject to controversial debates. Academics, policymakers, and legislators have been introducing a variety of partly conflicting conceptualizations of WMD into scientific debates, public discourse, and legislations over the last eight decades. Hence, it is unsurprising that this concept and its changing definition have been subject to politicization. Especially in light of the so-called “War Against Terror,” WMD became the synonym of a worst-case terrorist attack scenario that ought to be prevented by any means (Pillar, 2006). However, terrorism and other asymmetrical conflicts, in particular, pose serious challenges to the concept of WMD – serious enough to think about alternatives to this term in case of counter-terrorism discussions.

This chapter presents the history of the terms WMD and CBRN as well as numerous issues with and alternative approaches to the concept of WMD. It will be argued that a static concept that includes or excludes certain weapon types purely on the basis of their physical impact in an attack deals with problematic threshold issues. For example, casualty numbers that are used

to measure impact are difficult to compare in symmetrical and asymmetrical conflicts. In this chapter, I discuss concepts of terrorist weaponry that are focused on a more complex account of the impact of each weapon type used by terrorists. Specifically, the impact of a weapon type will be assessed by means of analyzing its hard (physical) and soft (psychological, economic, political) damage. Furthermore, the time that is necessary to create a high impact with the one-off use of the weapon, as well as uncertainties with regard to the consequences of the use of said weapon, will be part of the impact assessment.

However, in order to assess the dangers involved in and the severity of specific weapons in the hand of terrorists, it is not sufficient to focus only on the impact of a possible attack with this weapon. For example, even without an elaborate analysis, it is clear that nuclear weapons would easily achieve the highest score in terms of impact. However, the impact of a certain weapon technology does not say much about the terrorist threat posed by this weapon if this technology is simply not available to terrorist groups. Hence, a basic assessment of the resources and other restricting factors that guide the weapon choices of terrorists needs to be part of this chapter as well. This assessment might show a trend that is diametrically opposed to the impact of specific weapon technologies. It includes, for example, factors like availability, required expertise, operational space needed as well as tactical advantage and ideological considerations.

## 2. The (never-ending) history of WMD and CBRN

The notion of weapons of mass destruction has its origins in the middle of the twentieth century. One of the first recorded uses of the term WMD dates back to 1937 when the Archbishop of Canterbury warned against “all the new weapons of mass destruction” during his Christmas address (Carus, 2012, pp. 6–8). The archbishop never specified what kind of weapons he referred to in his address. Yet, researchers have been arguing that the term and the address, in general, was designed as a response to the bombing campaigns against civilians in Spain and Asia during that year (Carus, 2012, pp. 6–8). However, as Seth Carus argues, the Archbishop was also actively concerned with novel weapon systems like chemical warfare and could very well have referred to chemical or even biological weapons with the term weapons of mass destruction (Carus, 2012, p. 7).

The first politically relevant and precise notion of WMD was delivered roughly eight years after the Christmas address of the Archbishop of Canterbury. On 15 November 1945, the political leaders of the United States, Canada, and the United Kingdom issued a joint declaration calling for the regulation of atomic energy. In this declaration, the authors called amongst others “[f]or the elimination from national armaments of atomic weapons and of all other major weapons adaptable to mass destruction” (opp. cit. Carus, 2012, p. 8). An even more precise notion of WMD was defined only three years later by the United Nations Commission on Conventional Arms Control (CCA). The CCA issued an official definition of WMD and characterized this concept as chemical, biological, radiological, and nuclear (CBRN) weapons. Furthermore, the CCA opened

up this definition towards potential, novel weapon systems “which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons mentioned above” (opp. cit. Carus, 2012, pp. 9–10).

Another important part of the history of WMD and CBRN is the strategic use of the term WMD for political ends. As Michelle Bentley shows in a convincing argument, WMD has been defined and interpreted in different ways by different political actors in order to further political agendas (See Bentley, 2012, 2014). For example, the U.S. government and specifically the Department of Defense (DOD) appeared to favor a definition of WMD that exclusively refers to CBRN devices that are *capable of mass destruction*. Note that this definition would potentially exclude low-yield nuclear devices. As Bentley argues and Carus suggests, this slightly different – and ambiguous – definition had political advantages for the USA (Bentley, 2012, pp. 392–393; Carus, 2012, p. 31). Amongst others, it would enable the U.S. military to deploy low-yield nuclear weapons in space or the deep sea, although the UN Space Treaty and the Sea Bed Treaty prohibited the deployment of WMDs in space or the deep sea. Because of these changing definitions of WMD that admittedly only differed in nuances from the CBRN-based understanding of WMD, Bentley argues that WMD should be understood as a non-essentialist term rather than as a static definition.

Furthermore, Carus managed to identify six different understandings of WMD in national and international discourses, of which most are based on (some) CBRN technologies (Carus, 2012, p. 36). The most controversial interpretations of WMD in this list (such as weapons of mass effect) will be discussed below.

### 3. Abandoning WMD altogether?

Researchers have identified several different problems with the concept of WMD that range from conceptual issues to implementation issues in intelligence and law enforcement practice. In particular, Christian Enemark has been stressing the problems of the term “WMD”. In a pivotal article for this discussion, Enemark states:

“The WMD label exaggerates the destructiveness of chemical weapons, misrepresents the problem of biological weapons, and diverts attention from the overriding importance of dealing with nuclear weapons” (Enemark, 2011, p. 382).

This heterogeneity of weapon types summarized under the umbrella term of WMD certainly poses challenges to the concept of WMD. These challenges are even more pressing when dealing with improvised CBRN weaponry. As past incidents of use of chemical agents showed, attacks using chemical or even radiological weapons do not inflict mass casualties comparable to those casualty numbers expected for the deployment of, for example, a nuclear weapon or a weaponized biological agent (For cases see Danzig et al., 2011; The Times of Israel, 2015). In fact, researchers have argued that, for example, improvised radiological weapons do not produce more physical impact than IEDs or other conventional weapons (House, 2016, p. 73).

Moreover, even each of the four major weapon types summarized under the term WMD seems too broad to account for terrorist weapon technologies. For example, the use of salmonella bacteria to terrorize innocent people



would certainly count as improvised biological warfare but does not create the devastating consequences that a weaponized Marburg virus may be capable of. The salmonella campaign of the Rajneesh cult in 1984 is a case in point here (Early et al., 2017, p. 59). Thus, it seems inaccurate to refer to all CBRN weapons as “weapons of mass destruction”. The extent of destructiveness between these four categories, but also within each of these categories, is too diverse to group all of these weapons under the term WMD.

However, contrary to Enemark’s position, one could think of at least three different arguments against the radical abandonment of WMD.

First of all, it is simply impossible (and undesirable ) to remove the concept of WMD from international law and diplomacy. Seth Carus shows in a detailed analysis that the term of weapons of mass destruction is an essential concept in many of the most relevant international treaties including the Chemical Weapons Convention (CWC), Biological Weapons Convention (BWC), the Nuclear Non-proliferation Treaty, the Strategic Arms Reduction Treaty (START), the Space Treaty, and the Seabed Treaty (Carus, 2012, pp. 6–34). Abandoning the term WMD would mean to, potentially, having to jeopardize or even renegotiate these treaties.<sup>20</sup>

---

<sup>20</sup> Enemark argues against this by stating that WMD is a redundant term in international treaties that could be simply replaced by chemical, biological, or nuclear weapons. However, as Bentley has shown, the term WMD is more than a summarizing term of NBC, but a political tool. Because of this historically grown relevance of the term, it might, in fact, not be as easy to replace it in international treaties as Enemark suggests (See Bentley, 2012; Enemark, 2011, 2012).

Secondly, Bentley points out in a well-crafted argument that the term WMD is a non-essentialist concept that is being re-defined and used by political actors in order to further political agendas. This active role of WMD as a strategic tool in politics makes it almost impossible to abandon it from policymaking (See Bentley, 2012).

Lastly, it should be noted that military-grade biological, chemical, and nuclear weapons that are stockpiled and deployed by nation-states have common characteristics that could make the WMD concept useful for military strategists: For example, all three weapon categories require decontamination and extensive protective gear and all three weapon categories include strictly anti-personnel capabilities that outperform the blast radius of conventional weapons.

Yet despite the arguments in favor of keeping WMD as a concept in general, one still has to account for Enemark's criticism of diversity of impact within this concept. One possible solution would be to adopt the strongest definition of WMD as presented in Carus's article that only classifies those CBRN weapons as WMD that are, in fact, mass destructive (Carus, 2012, p. 36). Obviously, this classification almost immediately poses a threshold level problem: what should be considered mass destruction in this regard? One way of arguing would be to favor a *potential* mass destructiveness of certain CBRN weapons: while a nuclear warhead, the Novichock virus or a weaponized Marburg virus could potentially kill thousands of people in a one-off use, Salmonella bacteria or a dirty bomb are not capable of doing so. Obviously, this interpretation of WMD is not flawless as it allows certain strategic and politically motivated exclusions or inclusions to the WMD

category, as seen above. However, in light of Enemark's strong case against the concept on the one and good reasons to keep WMD on the other side, the definition of WMD as military-grade CBRN weapons that have been in national military arsenals at some point and that are actually capable of mass destruction seems to be the least problematic choice and will be used in the next section of this chapter.

#### 4. WMD and terrorism

It is important to note that, despite massive amounts of WMD/CBRN-related research and threat assessments in terrorism studies<sup>21</sup>, WMDs defined as military-grade CBRN weapons with mass destructive effects are almost absent in the arsenal of the most relevant terrorist groups. According to the Global Terrorism Database (GTD), the most comprehensive collection of terrorist incidents, only 0.233 percent of all recorded terrorist attacks were committed with CBRN weapon technologies. The majority of these cases were targeted poisonings and the use of CS or tear gas ((START), 2016). Based on an empirical assessment of terrorist attacks against the United States of America, the authors of another study note that “[b]etween 1970 and 2010, there were 751 terror attacks using conventional explosives and only 85 attacks using CBRN weapons” (Early et al., 2017, p. 58). Moreover, the authors of this study have included very low-impact CBRN incidents such as attempted poisonings.

---

<sup>21</sup> A brief selection of published research includes (G. Ackerman & Jacome, 2018; G A Ackerman & Pereira, 2014; Gary A Ackerman & Pinson, 2014; Asal et al., 2012; Bentley, 2012, 2014; Binder & Ackerman, 2019; Carus, 2012, 2017; Caves Jr & Carus, 2014; Enemark, 2011, 2012; House, 2016; Hummel, 2016; Ivanova & Sandler, 2007; Palmer, 2004; Parachini, 2003; Pichtel, 2011).

Furthermore, the concept of WMD, as defined above, does not encompass all mass destructive terrorist events or all terrorist weapons of mass destruction. Indeed, many of the past terrorist attacks that produced exceptionally large amounts of fatalities were executed with weapons that would not qualify as WMD as defined above. The attack on September 11, 2001, in New York City is just one (prominent) example of such weapons (See discussion in Bentley, 2012, p. 397). Furthermore, it has been shown in different studies that the most deadly terrorist attacks have been committed with conventional weapons such as IEDs or firearms. For instance, the authors of the recent studies on WMD terrorism in the USA that was mentioned above note in this regard:

*In addition to their higher attack frequency, conventional attacks using explosives cause higher damage, on average (...) Since 1970, 216 people have died from terrorist bombings in the USA while seven individuals have died from CBRN attacks. On average, 0.28 people die per bombing campaign, while 0.08 people die per CBRN attack (Early et al., 2017, p. 59).*

In addition to this observation, a quantitative data analysis of the incidents listed in the GTD calculated both the total numbers of fatalities as well as the fatalities per attack for different weapon types used by terrorist groups (See LaFree et al., 2014). Based on this calculation, vehicle-based attacks seem to be the deadliest terrorist weapons, followed by melee weapons and firearms. According to this study, chemical weapons come in fourth and are the deadliest weapons that are commonly considered WMDs – with a total fatality number of 629. In comparison, explosive devices have a slightly

lower rate of fatalities per attack but are responsible for a total amount of 99,379 deaths (LaFree et al., 2014, p. 139).

Because of the absence of WMDs in terrorist incidents, one could argue that this weapon category should not have priority and should not be discussed to such an extent in terrorism research. However, next to the low probability that a terrorist group, in fact, gets their hands on a WMD, law enforcement and security agencies have been using the term WMD with regard to terrorism to stress the danger of certain non-CBRN weapons with particularly high impact. In these instances, the notion of mass destruction has arguably lowered threshold levels when referring to crimes or terrorism in comparison to the above-formulated definition of WMDs as military-grade CBRN weapons. Even a death toll in the lower hundreds caused by an improvised device could count as a WMD event in the eyes of practitioners and policymakers:

In the USA, this approach to redefine WMD for terrorism was even turned into national legislation. In the aftermath of the Oklahoma City bombing in 1998, the perpetrator of the attack, Timothy McVeigh, was sentenced to death in accordance with a by then only one-year-old reform of the US criminal code (For discussion, see Madeira, 2012). According to these changes, the use of a WMD can be punished with the death sentence and WMD in this regard does not only refer to CBRN devices, but also to other “destructive devices include[ing] bombs, grenades, mines, or any gun with a barrel larger than one-half inch” (opp. cit. Carus, 2012, p. 29). In this reform, the term WMD does not only refer to CBRN weapons, but could better be characterized as CBRNE (chemical, biological, radiological,

nuclear, and explosive). Next to Timothy McVeigh, also the shoe bomber Richard Reid as well as the perpetrators of the Boston Marathon bombing were prosecuted for using WMDs – despite the fact that all these attacks involved conventional IEDs.

The interpretation of WMDs as CBRNE is one of the most prominent proposals to cope with the challenges of the concept of WMD with regard to terrorism. Next to practical and legislative advantages, the interpretation of WMD as CBRNE in terrorist incidents also appears to be a solution to the problem that the above-defined interpretation of WMD as military-grade CBRN may be both too narrow and factually irrelevant to account for most mass-casualty terrorist attacks. By adding explosive weapons, that were used in 52.65 percent of all terrorist attacks listed in the GTD ((START), 2016), the concept of WMD rapidly becomes a synonym for the most worrisome and most destructive weapons in terrorism – as the term traditionally promised.

Despite these obvious advantages, the treatment of WMD as CBRNE extrapolates some of the problems Enemark is raising in his article. For example, the problem that WMD includes too diverse weapon types that cannot be summarized in a single category becomes even more severe with regard to the CBRNE interpretation. The addition of explosive weapons to the definition of weapons of mass destruction would further broaden the concept and would, for example, refer to the nuclear bomb and to small IEDs that contain little more than pyrotechnical substances alike. Furthermore, if one would interpret explosive weapons as not only referring to IEDs but also to RPGs, mortars, grenades, and small artillery, then the

category of WMD would include almost all known weapon types with the exception of small firearms and melee weapons. This interpretation of WMD seems to be too broad to be an efficacious category for both symmetrical and asymmetrical conflicts. Efficacious in this regard does not only mean that the CBRNE interpretation of WMD seems too diverse from a theoretical perspective. It also poses serious challenges for the practitioners and institutions that work with this definition. First of all, the CBRNE definition fundamentally conflicts with the definition of WMD used in international law and numerous UN regulations and treaties.

Furthermore, since the label CBRNE presents itself as a single category of (advanced) weaponry, law enforcement, and intelligence practitioners could be tempted to allocate a special branch of their work to this category. However, since the weapons summarized under this label are highly diverse, some of them need completely different resources and analysis than others. For example, counter-measures against nuclear terrorism ought to focus on global non-proliferation efforts and state-funded terrorism, while IED counter-measures are (amongst others) focused on restricting access to certain household chemicals. The CBRNE label could be falsely suggesting that the threats evolving out of these different weapon types should be treated within the same department or group of analysts.

Finally, the CBRNE definition of WMD is still focused on physical impact as a defining criterion. However, as will be shown below, the impact of a weapon in the hands of terrorists should not only be characterized by focusing on its capability to produce mass physical destruction. Several authors pointed out that the impact of a terrorist weapon consists of multiple

different categories including, but not limited to, physical destructiveness (See e.g. Bunker, 2000; Dunn et al., 2008). Selected approaches to give alternative concepts to classify especially impactful terrorist weapons will be discussed in the following chapter.

## 5. Alternative concepts for terrorist weapons of mass destruction

The issues associated with mass casualty terrorist events and the definition of WMD caused several researchers, practitioners, and policymakers to rethink the conceptualization of terrorist weaponry.

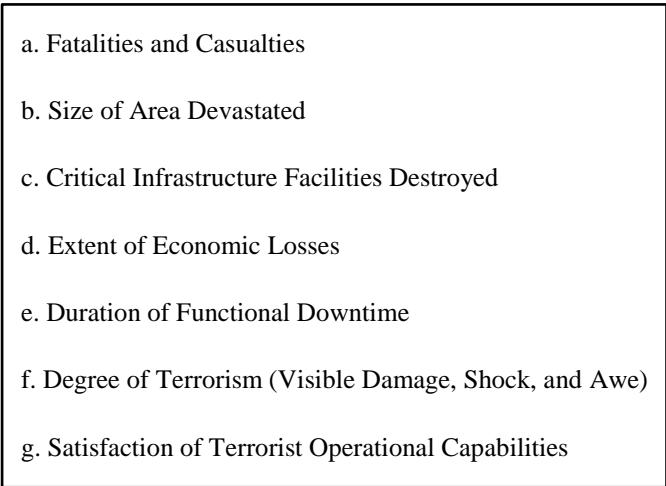
One possible solution to the problem of defining WMD was proposed by Robert J. Bunker, who presented his concept of Weapons of Mass Disruption (WMD<sup>2</sup>) in a publication in 2000 (See Bunker, 2000). In his article, Bunker points out that certain novel weapon types (including CBRN weapons like non-lethal viruses) cannot be classified as causing mass destruction. Bunker argues that these weapons target relationships and bonds on a massive scale (mass effect) in society rather than physical objects and persons (Bunker, 2000, pp. 41–43). Therefore, these weapons might have an enormously disruptive effect despite not inflicting mass casualties or large-scale physical destruction.

Clearly, Bunker's novel concept of WMD<sup>2</sup> could be used to solve the problem that some WMDs such as radiological dispersal devices (RDDs) do not seem to be mass destructive, but rather mass disruptive in societies. However, in solving this problem, Bunker creates yet another category of



weapons that is arguably as vague as WMD. The concept of WMD<sup>2</sup> does not seem have clear borders and threshold values with regard to effect size and extent of disruption. Thus, Bunker's solution to the problems of WMD creates even more problems with regard to vagueness and fuzzy borders between weapon categories. Furthermore, many of Bunker's examples of WMD<sup>2</sup> weapons (i.e., radio frequency weapons, genetic alteration weapons, liquid metal embrittlement) seem even more detached from the reality of terrorist weapon choices than the traditional WMD weapon category.

Perhaps the most promising candidate concept in relation to mitigating the problems of WMD with regard to terrorism is the concept of Weapons of Mass Effect (WME). Initially proposed by William Yengst in 2008, the concept of WME is aimed at accounting for all those (terrorist) weapons that cannot be considered strictly mass destructive in the traditional sense, but that create a mass effect (See Yengst in Dunn et al., 2008). Yengst defines mass effect as an interplay of seven different criteria:

- 
- a. Fatalities and Casualties
  - b. Size of Area Devastated
  - c. Critical Infrastructure Facilities Destroyed
  - d. Extent of Economic Losses
  - e. Duration of Functional Downtime
  - f. Degree of Terrorism (Visible Damage, Shock, and Awe)
  - g. Satisfaction of Terrorist Operational Capabilities

*Fig. 2: Yengst's criteria for mass effect (Dunn et al., 2008, p. [2-5] 4-5)*

According to Yengst, these criteria can be used as a rating system for terrorist weapons: only if a particular weapon reaches a certain score with each of these criteria and surpasses a certain threshold (in Yengst's analysis 41 points), then one could reasonably call this weapon a weapon of mass effect. Examples of these WMEs in Yengst's analysis are explosive attacks against critical infrastructure, the use of kinetic energy against office buildings (e.g., with an aircraft) or the contamination of drinking water supplies. With his approach to a dynamic rating system, Yengst effectively circumvented the demarcation problems resulting from static concepts such as WMD. Thereby, he solves problems such as the lacking identification of mass destruction and the high diversity of weapon types within the concept of WMD.

However, Yengst's proposal of WME does not abolish or replace the concept of WMD but rather offers an additional category of terrorist weapons for all those unconventional weapon types that are not regarded WMDs in the traditional sense. While the dynamic nature of Yengst's approach does not run into the same problems as Bunker's WMD<sup>2</sup> proposal, it does not explicitly solve the problems with the concept of WMDs, since only a few of Yengst's WME examples challenge the concept of WMD. Furthermore, Yengst's concept of WME allows for a large degree of subjectivity concerning the presumed effect of a weapon or an attack. For example, a workshop report from 2010 that used Yengst's concept portrayed the 9/11 attacks, the PFLP aircraft hijackings in the 1970s as well as the attempted assassination of Margaret Thatcher with an IED as WME attacks.

To sum up, while Yengst's approach to introduce a rating system to measure the effect (or impact) of terrorist weapons appears to be a suitable candidate to resolve a number of the problems with the concept of WMD in relation to terrorism, his introduction of the static WME concept for high-scoring weapons re-introduces some of these problems. By including or excluding certain weapon types to this concept according to varying criteria, researchers that use WME are yet again facing the problems that have been discussed above with regard to WMD. Hence, and based on Yengst's proposal, the following section will propose to expand Yengst's idea of a rating system to measure the impact of terrorist weapons. However, contrary to Yengst's approach, this new proposal does not introduce yet another concept of high-impact weapons but rather treats each and every (potential) terrorist weapon individually and based on its score in the rating system.

## 6. The terrorist weapon rating system

As seen in the last section, some researchers and practitioners have made attempts to overcome the problems arising from the traditional interpretations of WMD and CBRN. However, it also has been shown that these attempts either run into new problems or fail to resolve the original problems. However, the score-based approach of WME that was introduced by Yengst seemed to be the most promising attempt to cope with the problems that the term "WMD" poses with regard to terrorism. Hence, elements of Yengst's methodology will form the basis for my own proposal. In the following section, a dynamic rating system to identify the most dangerous terrorist weapons will be introduced.

Obviously, the term “dangerous” in this context is vague and unhelpful, at least at first glance. However, on my account dangerous will be cashed in terms of the broader concept of risk. Thus, a dangerous terrorist weapon is a weapon that poses the greatest risk to society.

As several researchers already pointed out, risk is a two-dimensional term that refers both to the harmful impact as well as the probability of that impact (See e.g. J. J. F. Forest, 2012). Thus, in the cases of terrorist weapons the risk would be calculated by recourse to, firstly, the factors restricting the terrorist’s decision to use a weapon and, secondly, the possible impact (or effect) that this weapon would have if used by terrorists.

As already seen above, Yengst’s criteria for defining WMEs are primarily aimed at one dimension of the risk that a terrorist weapon poses, namely the impact (or effect) of the weapon. However, to properly analyze this risk, both dimensions, impact and probability, are needed. Hence, the rating system in this section will not only include some of the criteria Yengst uses to assess the impact of a certain weapon but will also identify factors on the probability axis – in particular, factors that restrict the weapon choices of terrorists.

Assessing the likelihood with which a weapon might be used by terrorists is a highly complex endeavor. Terrorist groups and lone operators are agents with a wide variety of motives (both rational and irrational) who are also interested in disguising their decision-making and in deceiving researchers and investigators. Thus, a quantitative and standardized estimation of the probabilities of the use of certain weapons by terrorists is, in general,

challenging. However, researchers like Gary Ackerman, Adam Dolnik, Brian Jackson, and others have identified and discussed several criteria that might influence the decision making of a terrorist group to use a specific weapon for an attack (G. Ackerman, 2014; Cragin, 2007; Dolnik, 2007; Jackson & Frelinger, 2008). Based on these criteria, it might be possible to give an indication as to how likely it is that a terrorist group might be successful in acquiring and using a certain weapon for an attack.

First of all, however, it is necessary to further refine the criteria to be used in assessing the impact or effect of a certain weapon in the hands of terrorists. One can, at least, identify four major criteria that contribute to the impact of a certain weapon:

a. Hard damage

First of all, the most visible impact that a weapon can produce is physical damage. This damage includes destruction of, and physical damage to, buildings or other structures as well as the physical harming or killing of persons and animals. However, while damage to buildings and persons can be easily characterized as physical damage, that might not be as easy with other forms of damage, such as the damage created by a cyber-attack. Since no kinetic force is used to conduct these attacks, but rather digital means such as software, it might be difficult to call the damage inflicted by a cyber-attack hard damage. However, I argue that, depending on the chain of consequences caused by a cyber-attack, one should characterize its damage as hard damage even if the direct damage caused by the attack might not be physical. This argument holds especially for those cyber-attacks directed at

critical infrastructure. In most of these cases, the software is not the weapon itself but rather the means to turn the critical infrastructure into some sort of second-degree weapon that, via being destroyed or damaged, does physical harm to persons or damage to buildings.

#### b. Soft damage

Traditionally, the harm or damage resulting from an attack is categorized as follows: loss of civilian life, injury to civilians, and damage to civilian structures (ICRC, 2016, p. 32).<sup>22</sup> As seen above, all three of these types of harm constitute hard damage. Yet, international organizations such as the ICRC stress that this traditional view of harm is too narrow to account for specific harms that are not of a physical nature, but can still have devastating destructive effects on civilian life. With regard to these latter harms, the ICRC counts (amongst others) (1) mental harm as well as (2) economic loss and displacement, as potentially having such a destructive effect (ICRC, 2016, pp. 35–37 and 41–43).

(1) Mental harm as one possible source of damage in the aftermath of an attack is, according to the ICRC, implicitly mentioned in international humanitarian law since it forbids “(...)acts or threats of violence the primary purpose of which is to spread terror among the civilian population” (opp. cit. ICRC, 2016, p. 33). In this quote, “terror” refers to severe mental harm in the form of horror, psychological trauma, and post-traumatic stress. The importance of mental harm in international humanitarian law was stressed by the International Criminal Tribunal for Rwanda (ICTR) which included

---

<sup>22</sup> As defined in the codification of the principle of proportionality in Article 51(5)(b) of Protocol I of 8 June 1977 additional to the Geneva Conventions (AP I).

both “serious bodily or mental harm” (opp. cit. ICRC, 2016, p. 34) in the definition of genocide.

However, other psychological effects in the aftermath of a terrorist attack are relevant – even if such effects would not be considered disproportionate harm under international humanitarian law. The two most important examples of such psychological reactions to an attack are anxiety and moral outrage.<sup>23</sup>

A terrorist attack with an advanced weapon technology or CBRN device has the potential to inflict widespread anxiety in society (G. Ackerman & Jacome, 2018, p. 24; Gary A Ackerman & Pinson, 2014; Gross, Canetti, & Vashdi, 2016; Palmer, 2004). For example, public fear of possible contamination caused by improvised radiological or chemical weapons would be instances in which weapons inflict a massive degree of anxiety (Khripunov, 2006; Palmer, 2004; Wessely, 2005).

As briefly described in chapter 1 of this thesis, moral outrage can be understood as the anger and horror at the violation of a moral standard or at the (feared) loss of what we deeply care about. Hence, the complex emotion of moral outrage does not only include anxiety and horror, but primary anger and disgust that can manifest in demonstrations, public condemnations of attacks or calls for justice on a collective level (Johansen et al., 2018). Arguably, those attacks performed with unconventional and

---

<sup>23</sup> Please note that there is a large variety of emotions and mental harm involved in the aftermath of a terrorist attack including fear, anger, stress as well as aggression and violence. As examples for mental harm, I chose anxiety and moral outrage as well as post-traumatic stress, political militancy, distrust since they are the most relevant ones for this thesis.

globally ostracized weapons (such as chemical or biological agents) have the potential to cause a larger degree of moral outrage than, for example, an attack with a knife or gun.

While a certain degree of anxiety and moral outrage seems, at first glance, a proportionate reaction to an attack, and is in many cases only a temporary condition with minor influence on the impact of an attack, both anxiety and moral outrage can, depending on the nature of the attack, result in moral injury, political militancy, and the erosion of trust in society and government (See for discussions Gross et al., 2016, 2017; Miller, in press).

As Seumas Miller argues, an event that includes the “removal or threatened removal of what one cares deeply about” (Miller, in press, p. 9)<sup>24</sup> has the potential to cause moral injury in a person who witnesses said event. One manifestation of such a moral injury would be the occurrence of a post-traumatic stress disorder (PTSD) that is commonly defined as “(i) severe distress and functional impairments (ii) resulting from traumatic events” (opp. cit. Miller, in press, p. 2).

Another manifestation of moral injury in the aftermath of a terrorist attack is the erosion of trust, the call for (disproportionate) retaliation, and political militancy as Michael L Gross, Ryan Shandler and other researchers show in their studies. Specifically, it is shown that responses to cyber-terrorism with, at least, some kinetic impact such as fatalities include the tendency to call for drastic political measures in response to the attack including retaliation (Shandler et al., 2021). In another study, Gross shows that the public reacts

---

<sup>24</sup> In our case a terrorist attack that takes or threatens the life and health of our loved ones.



with political militancy that includes calls for “internet surveillance, government regulation, and military retaliation” (Gross et al., 2016, p. 4) in response to terrorism and, more specifically, cyber-terrorism. It is essential to note that Gross and his colleagues found out that the massive physical impact of an attack alone does not necessarily cause a high degree of political militancy, but that the *perception* of the threat influences the degree of political militancy as well (Gross et al., 2016).

Another manifestation of such a political radicalization as an effect of moral injury could be the erosion of trust in security institutions. For example, a nuclear device in the hands of terrorists could seriously compromise the national security of a country. More specifically, a successful attack with an impactful weapon might harm the reputation of intelligence institutions, law enforcement, and the military since it may result in the public ceasing to trust them and their ability to keep society safe (Meyer, 2004, p. 231; Van Der Does et al., 2019, p. 11).<sup>25</sup>

(2) Economic loss and (at least temporary) displacement could add to the impact of a terrorist attack. Particularly, those attacks that involve weapon technologies capable of causing contamination of a certain area potentially cause significant economic damage (Lemyre et al., 2005) by means of rendering a certain area (e.g., a business or shopping buildings or streets) unusable for a long period of time. It is noteworthy that not only a de facto-contamination of a certain area would cause economic damage, but

---

<sup>25</sup> Please note that several empirical studies found that the aftermath of a terrorist attack can also have the potential to temporarily increase trust in the Government and in other members of society in general. This effect is known as the rally effect. However, recent studies showed that this effect is only a short term effect in the immediate aftermath of an attack. (Dinesen & Jæger, 2013; Geys & Qari, 2017; Van Der Does et al., 2019).

also the public fear of contamination in the aftermath of, for example, a radiological attack that was, in fact, not capable of causing any health-damaging contamination (See Khripunov, 2006).

Closely related to damage to domestic politics and economy is the potential for terrorists to instigate or escalate *international* conflicts with certain weapons. A chemical attack by a Syrian terrorist group in the European Union, for instance, could easily further internationalize and escalate the Syrian civil war – not least because the nature of the attack can be used as a symbol of transporting the horrors of this civil war to Europe.<sup>26</sup>

#### c. Length of the attack

Not only the damage caused by an attack with a certain weapon but also the attack itself can tell a lot about the impact of said weapon. One important factor is the length of the attack in terms of the duration of use of this weapon during an attack. For example, a knife is a weapon that demands multiple uses over a long duration to create significant physical damage (i.e., to harm many people). In contrast, an IED is able to create large scale damage in a one-off use. Other than in case of a knife attack, police forces responding to an IED attack do not have any chance to interrupt or stop the attack as it happens. Hence, a weapon that creates significant damage in a very short time can be characterized as especially impactful.

---

<sup>26</sup> A more detailed analysis of this particular point can be found in chapter 3.

#### d. Uncertainty of consequences

Contrary to Yengst's approach, it may be very hard (if not impossible) to properly anticipate the damage a certain weapon will do in terms of physical, economic, and psychological damage. However, arguably the impact of a certain weapon should be considered especially high if one is unable to anticipate the consequences resulting from the use of it. This uncertainty associated with a particular weapon extrapolates its psychological damage by means of spreading large-scale fear in public. For example, the severity of the consequences from the use of pathogens as terrorist weapons is a matter of controversy among experts, yet the public believes the effects of biological weapons to be catastrophic (James & Oroszi, 2015; Palmer, 2004, pp. 6–7; Sullivan & Bongar, 2007). Again, the town of Salisbury was extensively contaminated with the most deadly chemical agent ever produced (Novichock), yet only three people were wounded as a result of this attack (Faulconbridge & Holden, 2018). However, the uncertainty concerning the effects of terrorists using biological weapons makes these weapons especially effective in terms of causing psychological and other forms of soft damage. With regard to counter-measures against these weapons, security agencies often refer to the precautionary principle as a guiding approach (General discussion concerning this principle in Grunwald, 2008; Roeser et al., 2012).

However, the uncertainty attached to these weapons is a problem not only for the counter-terrorism authorities but also for the individual who uses them. First of all, as is the case for the authorities, the perpetrator faces a high degree of uncertainty with regard to the extent of the impact a certain,

advanced weapon would have. For example, the release of a fatal virus in a shopping center might have a tremendous impact, yet the fragile nature of viruses as well as environmental conditions and other factors might diminish said impact dramatically. Secondly, the perpetrator of such an attack faces uncertainty with regard to her own security when using certain weapon types. For example, in the example above the perpetrator might very well fall victim to her own weapon during the attack against the shopping mall. This dual uncertainty makes it almost impossible to use said weapons in a controlled and discriminate manner. This uncontrollability makes these weapons even more dangerous and, hence, increases their potential impact.

So far, these four criteria only give information about what could happen *if* terrorists would acquire and use a certain weapon technology. However, to properly analyze the risk certain weapon types are posing, it is also necessary to consider the factors that increase or decrease the probability that terrorists might acquire and use a certain weapon. In addition to the criterion of high impact of a weapon, researchers have shown that terrorists might also consider the following criteria in choosing their weapons:

a. Availability

The probability that a certain weapon will be used by terrorists can be seen as high if the materials that are necessary to assemble said weapon are openly available or can be acquired with little restrictions. Furthermore, the financial means that are necessary to acquire and assemble a particular weapon are part of the decision-making process of a terrorist group in their

choice of weapons. The more affordable a weapon is, the more likely it will be acquired by small cells and lone operators (G. Ackerman, 2014, pp. 14, 76–82, 90, fig. 4.1. Cragin, 2007, table 2.1. Cragin et al., 2004, pp. 48–57; Dolnik, 2007, p. 19; J. F. Forest, 2006, pp. 1–13; J. J. F. Forest, 2008, pp. 269–282; Jackson, 2001, pp. 198–201).

#### b. Required expertise

Expertise plays a crucial role in the acquisition and use of weapons by terrorists. Some weapon types require extensive and specialized expertise to be used successfully, while others do not require deep knowledge of any kind. Here, the pre-existing expertise as well as the knowledge resources (i.e., personnel, network, safe spaces for testing) of a terrorist group deeply influence what kind of weapon will be chosen for an attack (G. Ackerman, 2014, pp. 14, 83, 87–88; Cragin, 2007, table 2.1. J. F. Forest, 2006, pp. 1–13; J. J. F. Forest, 2008, pp. 269–282). Expertise plays a crucial role in the acquisition and use of weapons by terrorists. Some weapon types require extensive and specialized expertise to be used successfully, while others do not require deep knowledge of any kind. Here, the pre-existing expertise as well as the knowledge resources (i.e., personnel, network, safe spaces for testing) of a terrorist group deeply influence what kind of weapon will be chosen for an attack (G. Ackerman, 2014, pp. 14, 83, 87–88; Cragin, 2007, table 2.1. J. F. Forest, 2006, pp. 1–13; J. J. F. Forest, 2008, pp. 269–282).

One particularly important factor determining the expertise that is needed to successfully use a certain weapon is the sophistication of the delivery

system for such a weapon.<sup>27</sup> A weapon with a specialized, complex delivery system might create a large impact, but might require a large amount of resources and considerable specialized expertise. The history of delivery systems for CBRN weaponry illustrates the variety of weapon delivery systems and their influence on the impact of those weapons.

For example, delivery systems for nuclear weapons range from intercontinental ballistic missiles (ICBM) to tactical nuclear weapons (TNWs). Due to their short range and low yield, TNWs have a compact design. For instance, the W54 warhead has a yield range from 10 tons to 1 kiloton and fits into a portable transport container (H-912 transport container) that can be carried by soldiers. W54 warheads are also the basis of the M-29 Davy Crockett recoilless gun that only weighs 23 kg (Pichtel, 2011, pp. 140–150).

Other weapon types that have not been used by nation states on a large scale have less standardized delivery systems. For example, states that owned a biological weapons program experimented with different delivery systems to disperse these agents among enemy forces. Since biological warfare agents are effectively only dispersible as aerosols, the two major methods of delivery in most historical programs were dispersion through spray mechanisms and filling missiles, mortars or bombs with pathogens. One example of such a delivery system is the SPD Mk I bomb of the US military that was considered to be one of the most suitable candidates to deliver biological agents like *Bacillus Anthracis* in the 1940s (Sidell et al., 1997, p. 44). Additionally, Iraqi military scientists used R-400 bombs for the

---

<sup>27</sup> The author expresses his gratitude to Michael L Gross for raising this point.

possible delivery of *Bacillus Anthracis* and *Botulinal* toxins in 1990 (Carus, 2017, p. 31).

In direct comparison to biological warfare agents, chemical weapons possess a quite extensive history of military use and, thus, have been produced and stockpiled in standardized delivery systems worldwide. One example of such a delivery system is the M139 sarin bomblet that was developed as a chemical cluster munition by the US Chemical Corpse. Chemical warheads containing multiple of these bomblets could be attached to weapons like the MGR-3 Little John artillery rockets (52 bomblets) or short-range missiles like the MGM-29 Sergeant (330 bomblets) (Sidell et al., 1997, p. 59). In contemporary conflicts such as in the ongoing civil war in Syria, agents like sarin, chlorine or mustard agents are typically being delivered via artillery shells as well as with aerial bombs (OPCW, 2016).

Nearly all of the above discussed weapon delivery systems were designed and used by nation states and, hence, are not available on the free market or attainable through theft. Moreover, getting access to these technologies would require large resources and using them would demand a high degree of expertise. Hence, to use agents like radiological materials, pathogens or toxins in an attack, terrorists often have to rely on improvised delivery systems that include simple spray mechanisms used for agricultural purposes or IEDs. With the help of an IED, radiological materials can be dispersed or containers with toxic gases could be opened remotely. Chapter 3 of this thesis will give some insights into possible delivery systems for selected radiological and toxic agents.

### c. Operational space needed

Some weapon technologies need extensive space and specialized facilities if they are to be used in an attack. For example, the construction of an improvised nuclear device (IND) requires, at least, a laboratory with specialized equipment and facilities to store raw materials, precursors, and other materials. In a similar fashion, the handling of pathogens such as *Yersinia Pestis* demands laboratory conditions with suitable safety standards to avoid accidental infection. Yet, a simple IED might be manufactured in an apartment in an urban area without risking detection.

The operational space that is needed to manufacture a certain weapon type influences the weapon choices of terrorists in, at least, two ways: first of all, a large operational space such as an industrial complex, a laboratory or a remote facility requires very considerable financial resources. Secondly, a large operational space increases the risk of detection by security agencies. Potential terrorists would have to sign documents and create cover stories in order to get access to a laboratory facility. These procedures make them and their plot vulnerable to be exposed and interrupted (G A Ackerman & Pereira, 2014; Bunker, 2000; Cragin et al., 2004; Dunn et al., 2008; Flade, 2016; Lakoff, 2007).

### d. Tactical, strategical, and ideological advantage

Last but not least, the use of a particular weapon has to have a clear tactical, strategic or ideological advantage over other weapons. Some terrorist groups have a strategy of toppling a regime by targeting specific persons and institutions, while others prefer to spread fear with mass-casualty attacks.



Hence, the strategy and, consequently, the preferred tactics of a group determine the weapon choice of a terrorist group as well (G. Ackerman, 2014, pp. 13, 72, 99; Cragin, 2007, table 2.1. Dolnik, 2007, pp. 13–21; Jackson & Frelinger, 2008, p. 15).

However, not only tactics and strategy but also the underlining ideology of the group plays a crucial role here (G. Ackerman, 2014, pp. 12, 73, 83; Cragin, 2007, p. 44; Dolnik, 2007, p. 70f; Drake, 1998). For example, a Marxist-Leninist terrorist group that mainly targets political figureheads might not be as interested in indiscriminate biological agents as an apocalyptic religious group that attempts to kill all “infidels”.

It is important to note that all of these weapon choice criteria cannot be understood as general rules for terrorist decision-making. Rather, they should be seen as indicators for weapon choices that are highly dependent on specific ideologies, organizational structures and capabilities of terrorist groups (G. Ackerman, 2014; Cragin, 2007; Dolnik, 2007; Jackson & Frelinger, 2008; Koehler-Derrick & Milton, 2017). For example, the weapon choice pattern of ISIL-inspired lone operators in Western Europe might be completely different from the weapon choice pattern of the FARC in Colombia. Hence, to accurately assess the risk that a particular weapon poses, one has to specify this risk by means of attaching it to a certain terrorist branch (e.g., Islamist cells or right-wing lone operators) and a region (e.g., Western Europe).

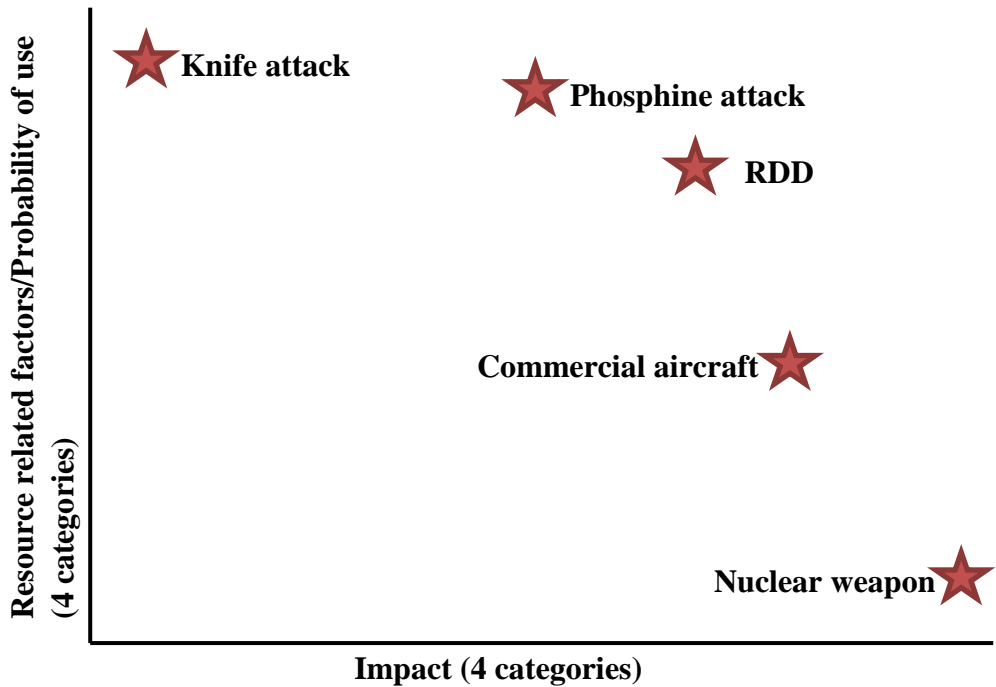
Furthermore, the assessment of the impact that a certain weapon might have cannot necessarily be generalized. To properly assess the impact of a

weapon, it is important not only to avoid general weapon categorizations, such as CBRN or CBRNE, one should also avoid generalizations of weapon types such as “chemical weapon” or “explosive”. Rather, one should attempt to focus on the nature and amounts of ingredients that a particular weapon consists of to arrive at a specific scenario that can be coupled with the specified weapon choice patterns of a particular group in a particular region. For example, one could assess the impact of a medium-sized improvised chemical device consisting of phosphine and estimate whether the choice patterns of a small terrorist cell in a Western democracy would be in favor of this weapon.<sup>28</sup>

On the basis of assessments and risk categorizations like this one, it is possible to compare different terrorist weapons with each other and single out those that might be both highly impactful and within reach of certain groups in specific regions. For Western Europe, one could summarize and compare these risk categorizations of different weapons in a rating graph like the one shown below. In this graph, the above-mentioned assessment of phosphine can be directly compared with the assessments of other weapon technologies and, thereby, high-risk weapon technologies can be identified. This graph can be extended to create a detailed and dynamic rating system of weapon technologies.

---

<sup>28</sup> Please note that a detailed discussion of this specific assessment can be found in the following chapter.



*Fig 3: Graph to display the risk assessment of terrorist weaponry*

Yet, to what degree is this rating-based approach superior to the above discussed CBRNE interpretation of WMD that is (at least to some degree) currently being used in counter-terrorism practice? First of all, from a conceptual perspective, the rating approach has the advantage of giving a more detailed overview of the risk that a certain weapon type poses in the hands of a given terrorist group. Not only physical impact and casualty numbers but also soft damage and the handling of the weapon technology as well as its availability and ease of use are included in this overview. Secondly, the rating approach does not include or exclude a fixed set of

weapon types. Therefore, this approach can be used to determine the risk of a wide variety of weapons that might be used by terrorists in the future. Thirdly, the approach to use a rating system for these weapons with regard to terrorism does not conflict with the existing definition of WMD in international legislation. After all, a nuclear weapon can be both a WMD according to international law and the most impactful (yet least available) terrorist weapon on the scale.

Finally, from the point of view of practitioners and counter-terrorism institutions, the more detailed account of the presumed impact of a certain weapon in the hands of terrorists could be used to allocate resources more efficiently on particular weapon types that pose the greatest risk. For as we have seen above (and will see in the next chapters), the counter-measures against the acquisition of an off-the-shelf nuclear weapon might be radically different from the counter-measures necessary to prevent an attack with the above-described improvised phosphine device or a crude RDD. While the first one requires international efforts of non-proliferation and the enforcement of international treaties, the latter one involves counter-measures such as educating and cooperating with hardware store employees or companies that produce pesticides in Western democracies on a local level. Hence, the introduced weapon rating system enables counter-terrorism institutions to group certain weapon types together dynamically and allocate specific groups of counter-measures necessary to prevent attacks using said weapons.

## 7. Conclusion

This chapter has shown that the categorization of weapon technologies using concepts like WMD runs into severe problems when applied to the phenomenon of terrorism. Hence, it was proposed to abolish the static approach that lists weapon categories with regard to the terrorist threat and, instead, to introduce a dynamic rating system to assess the risk that specific weapons pose in the hands of particular terrorist groups. This approach is less vulnerable to problems identified with the static approach but still manages to provide researchers and policymakers with a clear assessment of the most dangerous terrorist weapons. Yet, since the risk assessment, and especially the assessment of the probability of the terrorist use of a weapon (choice criteria), should not be interpreted as generalizable or quantifiable, the presented rating system ought to be treated as a first (but promising) indication of the dangers posed by particular weapons in the hands of particular groups in particular regions.

However, for this thesis, this chapter provides a useful framework to identify and assess the most dangerous weapon technologies with regard to terrorist cells and lone operators in Western democracies. In the upcoming chapters, three substances are identified that score especially high on both the “impact” axis and the “probability of use” axis. As will be shown, especially the high scores of these substances on criteria like soft damage and availability demand a specific group of counter-measures on behalf of terrorism institutions. In order to contain the threat posed by weapons with these values, security institutions have to form partnerships with businesses, researchers, and citizens.

### **3. Threat assessment of selected common-use toxins – Ricin, phosphine, americium**

#### **1. Introduction**

In the last chapter, a terrorist weapon rating system was introduced to measure both the impact of a certain weapon technology in the hands of terrorists as well as the probability with which it might be used by terrorists to perform attacks. This rating system provides both researchers and practitioners in the field of counter-terrorism with a first, solid assessment of the dangers of particular weapon types. Furthermore, this assessment can help in the design of counter-measures against certain groups of weapon technologies that exhibit similar features and scores in the rating system. For as will be shown in this chapter, weapon types with similar scores and features on the rating system often require similar counter-measures on the part of security agencies in order to prevent their acquisition and use by terrorist groups.

To demonstrate this characteristic of the terrorist weapon rating system as well as its other advantages, this chapter assesses the impact and probability of use of three different substances. It will be argued that all three of these substances pose an extreme risk to Western democracies of a high-impact attack by terrorist groups or lone wolves. As will be shown, all three of these substances present good examples of the most dangerous terrorist

weapon technologies since they are an excellent compromise between high-impact weapons and weapons that are easy to access and use. The substances in question are ricin, phosphine, and americium. As already mentioned above, the assessment will also show that the description of these three substances in the framework of the terrorist weapon rating system shows that cooperation and partnerships between security institutions with corporations and citizens are necessary in order to prevent the successful acquisition and use of ricin, phosphine, and americium by terrorists.

Yet, before analyzing these three substances in terms of the terrorist weapon rating system, a brief description of the nature and chemistry of each substance needs to be provided:

a. Ricin

Ricin is a toxic glycoprotein that was identified and initially described in 1889. It is a naturally occurring toxin that can be found in and extracted from the seeds of the plant *Ricinus communis* (Sidell et al., 1997, Chapter 32). These seeds are commonly called castor beans. Ricin is extracted and used in powdered form and is one of the most powerful organic poisons. If organisms are exposed to ricin as an aerosol, it exhibits an LD<sub>50</sub> value of 2.7 to 3 µg/kg and an LD<sub>50</sub> of 30 µg/kg with gastro-intestinal exposure (Pichtel, 2011, pp. 126–128).<sup>29</sup>

---

<sup>29</sup> The LD<sub>50</sub> value refers to the lethal dose of a substance and describes how many µg (or mg) per kg body weight of the substance is necessary to kill 50 percent of the exposed population.

## b. Phosphine

Phosphine is a colorless, toxic gas compound with the formula  $\text{PH}_3$ . It is heavier than air and exhibits  $\text{LC}_{50}$  values<sup>30</sup> of 20 ppm in rats if exposed to the gas for one hour. Phosphine kills organisms by seriously disturbing the transport and use of oxygen in the body. Hence, it is considered a so-called pulmonary or choking agent (National Center for Biotechnology Information, 2019). Phosphine can be produced on an industrial scale by acid-catalyzing white phosphorous or by reacting white phosphorus with sodium or potassium hydroxide. For this thesis, however, especially the preparation of phosphine on a small scale is interesting. For example, phosphine can be produced by mixing metal phosphides (such as aluminum phosphide or calcium phosphide) with water (Bogle et al., 2006; Gurjar et al., 2011; Parakrama 'gura 'gurusinghe, 2014). This simple production method is deployed in order to use phosphine as a rodenticide. The use of metal phosphide tablets with water allows it to produce phosphine on-site and in specific areas only (e.g. mole tunnels) (Bogle et al., 2006; Gurjar et al., 2011).

## c. Americium

Americium is a highly radioactive element with the atomic number 93. For this thesis, especially the isotope Americium-241 ( $^{241}\text{Am}$ ) is of interest.  $^{241}\text{Am}$  has a half-life of 432.2 years and exhibits a radioactivity of 126.8 Gigabecquerels per gram (GBq/g) (Motzkus et al., 2012, pp. 16–17; U.S. Agency for Toxic Substances and Disease Registry, 2004). Like all other

---

<sup>30</sup> The  $\text{LC}_{50}$  value refers to the lethal concentration of a substance and is bound to a specific duration of exposure.



Americium isotopes,  $^{241}\text{Am}$  belongs to the group of  $\alpha$ - and  $\gamma$ -emitters. Although there are only very few hazards to be expected from the  $\alpha$ -particles alone, the ingestion of  $^{241}\text{Am}$  through air, food, water or if in contact with the skin has various negative health effects. One of the most prevalent commercial applications of  $^{241}\text{Am}$  is the use of it in ionizing smoke detectors. The amount of  $^{241}\text{Am}$  in current smoke detectors of this type does not exceed one microcurie (or  $0.29\text{ }\mu\text{g}$  based on the mass of  $^{241}\text{Am}$ ) (Satterfield, 2011, p. 20; U.S. Agency for Toxic Substances and Disease Registry, 2004).

## 2. Impact

### 2.1. Ricin

#### a. Hard damage

As already mentioned briefly above, ricin belongs to the strongest organic toxins and can harm and kill organisms in different ways. For example, the inhalation of powdered, purified ricin has extremely damaging effects on organisms. Only  $2.7$  to  $3\text{ }\mu\text{g}$  of ricin is sufficient to kill an organism with the weight of one kg (Pichtel, 2011, p. 126; Sidell et al., 1997, Chapter 32). Hence, the exposure to  $167\mu\text{g}$  or  $0.2\text{ mg}$  of ricin via inhalation has a lethal effect on human beings with a probability of 50 percent. That is less than the weight of an average grain of sand. Symptoms from inhaling ricin include weakness, fever, and pulmonary edema. This can result in respiratory distress and death within 72 hours. In the case of aerosol exposure through

ricin, patients usually die from hypoxemia as a result of massive pulmonary edema and alveolar flooding (Pichtel, 2011, p. 127; Sidell et al., 1997, Chapter 32).

Due to the high risks of aerosolized ricin particles to human health, terrorists and other criminals are likely to choose this type of exposure in order to commit an attack with the agent. Especially agricultural spray mechanisms and modified IEDs have to be mentioned as possible delivery systems of ricin. Furthermore, terrorists might use ricin-coated bullets as delivery system or might attempt to disperse the toxin via air ventilation systems.<sup>31</sup>

However, despite its concerning LD<sub>50</sub> values, it is not clear in the literature what extent of hard damage would be the result of a large-scale ricin attack (See e.g. Pichtel, 2011, pp. 126–128). Note that the agent is a strictly antipersonnel weapon. Hence, architecture and other structures are not affected by an attack with ricin alone. However, the use of ricin in a modified IED might cause physical damage to structures via the IED. It is very difficult to give an estimate about possible casualty numbers from a large-scale ricin attack since there are (fortunately) no historical cases of a large-scale attack with aerosolized ricin available. Furthermore, powdered ricin is very sensitive to a variety of environmental factors. For example, strong winds, rain, or air filtration systems in buildings could strongly diminish the impact of a ricin attack. Hence, despite its relatively high toxicity, one would need almost eight metric tons of this agent to use it in a large-scale attack in an urban area. Other biological agents such as

---

<sup>31</sup> Please note that the author refrains from giving detailed instructions into the necessary steps to use spray mechanisms and IEDs as delivery systems for ricin.

botulinum toxins<sup>32</sup> show much higher lethality under the same conditions (Carus, 2001, p. 13).

b. Soft damage

While not much is known about the possible hard damage (i.e., casualty numbers) from a large-scale ricin attack, the soft damage from such an attack can be measured more reliably. In this regard, historical cases such as the Cologne ricin plot from 2018 can be of help.

Although (from the perpetrator's perspective) an unsuccessful attack, the Cologne ricin plot can still be used to assess the soft damage that a terrorist attack with ricin might cause to the public and institutions. First of all, it is important to note that German law enforcement arrived with special forces in category A and B HAZMAT suits<sup>33</sup> at H.'s apartment complex and evacuated the entire neighborhood after the arrest. Furthermore, toxin specialists arrived at the scene of the plot to research the sophistication and nature of the biological agent that was present in H's apartment (BBC, 2018). This entire process is most likely a standard procedure in case of a (presumed) biological threat and, hence, can be expected to happen every time German security institutions are confronted with suspicion of the preparation and use of a biological or chemical agent.

However, it is crucial to note that journalists and reporters were on the scene

---

<sup>32</sup> The LD<sub>50</sub> value of botulinum toxins is 3ng per kg body weight and, hence, almost 1,000 times more toxic than ricin. Yet it has to be noted that botulinum toxins are the most toxic substances on the planet (Carus, 2001).

<sup>33</sup> A general classification of HAZMAT suits and personnel protection equipment (PPE) can be found in Pichtel (2011, pp. 315–334).

of the investigation in Cologne to document this procedure for the German public. Consequently, German news outlets such as the EXPRESS newspaper provided the German public with images of H's neighborhood that showed a massive presence of special forces, police personnel in HAZMAT suits of the category B as well as toxin experts with HAZMAT suits of the category A (Baumanns, 2018).

Arguably, these photos in combination with reports about the toxicity and availability of ricin sparked a wave of outrage and fear in German society. The mere sight of investigators in HAZMAT suits, experts on the scene as well as the evacuation of the building was more than sufficient to create an image of an apocalyptic weapon that was almost deployed in the heart of one of Germany's biggest cities (Ward, 2014, p. 119). Hence, although never used in an attack, H's ricin device created a substantial amount of psychological damage in German society. The fear and the (mis-)interpretation of H's device as potential weapon of mass destruction that was widely visible in the reporting about the incident presents evidence for the high psychological impact of ricin as a weapon of terror (See for general argument in connection to CBRN weapons G. Ackerman & Jacome, 2018, p. 24).<sup>34</sup>

Furthermore, this high degree of psychological damage adds to the damage that the (attempted) use of ricin causes on a political level and to institutions. Due to the high levels of fear that occur in the aftermath of an attack or plot with ricin, public trust in the Government and, especially,

---

<sup>34</sup> In the aftermath of the Cologne ricin plot, other researchers like Petter Nesser came to the same conclusion as mentioned in interviews with German newspapers (Unger, 2018).

security institutions might erode. In particular, the mischaracterization of ricin devices as some sort of weapon of mass destruction can spark skepticism concerning the ability of a nation's security apparatus to keep its citizens safe from terrorist threats of an almost apocalyptic nature. Influenced by inaccurate and sensational reporting of these incidents and pop-cultural accounts about the WMD terrorism threat<sup>35</sup>, citizens might lose trust in law enforcement, intelligence institutions and the military. Furthermore, they might start to distrust their Government's current security policies.

c. Length of attack

Depending on the nature of the device that a terrorist uses to disperse ricin, an attack with this agent might only be a matter of very few seconds. For this thesis, it is worthwhile to focus on the dispersion of ricin with the help of a modified IED as well as the aerosolization of ricin through some sort of spray mechanism. An attack with an IED that is being used to release and distribute ricin powder in a certain area only takes the time that is necessary to push the detonator of the IED. Hence, the length of the attack can be characterized as less than two seconds. In comparison to the IED approach, the distribution of powdered ricin through spray mechanisms demands a longer time span. For example, if a perpetrator disperses the powder from a spray bottle in a building or in public transport, the attack would have to go on for, at least, several minutes in order to cause the desired effect. This reasonably long time span might be enough for potential victims to move away from the contaminated area or for police forces to stop the perpetrator

---

<sup>35</sup> For a detailed discussion, see the last chapter of this thesis.

during the attack. However, if a terrorist would use pre-installed systems such as air conditioning installations in large buildings to disperse the ricin powder, the length of the attack would shrink down to the few seconds that are needed to introduce the agent into the system.

d. Uncertainty of consequences

As already discussed in section a. of this chapter, it is uncertain what the physical impact of a large-scale terrorist attack with ricin would be. Just like other biological warfare agents, ricin is very sensitive to environmental factors (See for general discussion Enemark, 2011) and its toxicity only refers to ideal exposure to organisms in laboratory environments. Hence, it is unclear whether an attack with aerosolized ricin would cause a substantial amount of casualties and would contaminate the area around the scene of the attack. As past incidents with biological agents have shown, common estimates about the severity of a biological attack might drastically differ from the reality of an attack with pathogens and toxins. One example of such a vast gap between the expected impact of a biological agent and its actual physical impact is the case of *Bacillus anthracis*:

To assess the damage that a biological weapon would cause in an environment that can be interpreted as cutting edge with regard to emergency response services and healthcare infrastructure, one has to rely primarily on scenarios and estimates that were published by the World Health Organization (WHO) in the 1970s. In a WHO study on the possible effects of biological agents, the effect of different agents on the populations of a fictional Western city with 1 million inhabitants was assessed.

According to the study, the dispersal of circa 50 kg of anthrax spores in the city would put 180,000 inhabitants at risk of being infected (Carus, 2001, table 7). According to the WHO, 95,000 people would die from anthrax exposure in this scenario. *Bacillus anthracis* can be contracted via contact with wounds or sore skin, but also through food and especially through inhalation, which is the most dangerous form of exposure to the bacterium. Untreated or not properly diagnosed cases of inhaled spores of *B. Anthracis* are fatal in up to 95% of all cases. Symptoms occur one to seven days after exposure. Spores of *B. Anthracis* are known to be resistant against sunlight, heat, many disinfectant agents and the spores can survive in a vegetative state in the soil for a long time (Carus, 2001; Pichtel, 2011, pp. 114–119; Sidell et al., 1997).

Contrary to the WHO account, the only example of an actual bioterrorist attack with this pathogen presents a radically different image of the damage evolving out of the dispersal of anthrax spores in a major city. In September 2001, the microbiologist Bruce Edwards Ivins sent out two waves of letters containing both cutaneous and inhalational anthrax to news media outlets and to the offices of U.S. senators in Washington D.C, New York City, Trenton and Palm Beach (Whitby et al., 2015). As a result of this attack, 22 people that were exposed to the spores fell ill. Eleven of these anthrax victims inhaled the pathogen and five died from this exposure. In the aftermath of this attack, nearly 30,000 people received post-exposure prophylaxis to prevent further cases of illness. However, while the fact that five people fell victim to this bioterrorist attack is obviously a tragedy, the damage inflicted by *B. Anthracis* was not nearly as devastating as scenario-based threat assessments like the WHO assessment from 1970 presumed.

This contrast between the assessments and the actual case from 2001 shows vividly how uncertain the extent of the hard damage inflicted by a biological weapon such as *Bacillus anthracis* might be. Authors like Christian Enemark stressed in convincing arguments that biological weapons might be the most unpredictable weapon category since the success of their deployment depends on a large variety of environmental factors and circumstances that can either help or damage the success of an attack (See esp. Enemark, 2011).

This discrepancy with regard to the impact of biological agents such as *Bacillus anthracis* or ricin leads to a high amount of uncertainty in the assessment of these weapons. Consequently, this uncertainty adds to the impact of this weapon since neither emergency services nor security agencies can assess with certainty what the threat posed by a biological agent in the hand of a terrorist organization might look like. Hence, many analysts work on basis of the precautionary principle and prepare for worst-case scenarios that assume and warn against the most devastating possible consequences resulting from a biological attack (As seen in the analysis of the WHO estimations in Enemark, 2011; and for a critical comment in Wessely, 2005, p. 3). These assessments reinforce the public anxiety with regard to these kinds of attacks and, thereby, add to the psychological damage of biological terrorist attacks.

However, not only the emergency services and the security agencies have to deal with large amounts of uncertainty when it comes to the possibility of a ricin attack. Also, the perpetrator of such an attack faces uncertainties ranging from accidental self-contagion (Ward, 2014, p. 102) to a failed



attack due to inadequate environmental circumstances or ineffective dissemination. In this regard, the use of ricin in an attack might not be desirable for a terrorist since the extent of the hard impact of an attack with this agent might be too uncertain. However, it is important to note that, despite this uncertainty with regard to the hard impact of ricin, the *soft* damage inflicted by an attack with this agent can be assessed and expected with less uncertainty.

## 2.2. Phosphine

### a. Hard damage

There are no openly accessible assessments available to determine how many casualties a terrorist attack with a phosphine-based device would inflict. However, based on the  $LC_{50}$  factor of this substance and coupled with more general estimates and assessments with regard to the use of chemical weapons in general, a first impression of the hard damage caused by a phosphine attack can be presented.

First of all, it should be noted that phosphine exhibits dangerously low  $LC_{50}$  values in comparison to other toxic industrial chemicals (TICs) such as chlorine. A population of rats has to be exposed to 293ppm of chlorine for one hour in order to be killed by the gas with a probability of 50 percent. For phosphine, this value is only 20ppm. Hence, phosphine can be described as being more than ten times as toxic as chlorine. Note in this regard that chlorine is considered a chemical warfare agent by the OPCW, while phosphine is not. However, as already mentioned in connection to ricin,  $LD_{50}$  and  $LC_{50}$  values should always be seen as median estimates under

laboratory conditions. These values alone say very little about the actual physical effect of phosphine in a terrorist attack. To assess the hard damage caused by phosphine and chemical warfare agents in an operational environment, it is necessary to take a closer look at a historical example of their use against combatants and non-combatants. In contrast to biological and nuclear warfare agents, it is possible to find multiple instances of chemical attacks in historical and contemporary conflicts that can shed light on the damage this weapon category might inflict. One of those instances is the terrorist attack against the subway system of Tokyo in 1995 (Danzig et al., 2011). During this attack, members of the death cult Aum Shinrikyo opened several canisters of sarin in underground trains and, thereby, killed 12 people (Daly et al., 2005; Danzig et al., 2011). Given the lethality of sarin, this death toll seems surprisingly low.

This assumption is supported by the outcome of the report of the U.S. Office of Technology Assessment from 1993 that anticipated the damage caused by 300kg of sarin in a city like Washington DC. According to this scenario-based analysis, the damage inflicted by this chemical agent would not surpass more than 200 fatalities (U.S. Congress Office of Technology Assessment, 1993). With regard to the destructiveness of chemical weapons, the report concludes that this weapon category only manages to inflict mass casualties comparable to the casualties caused by nuclear or biological weapons if deployed in very large numbers.

The report goes even further by stating that chemical weapons might, in fact, be less effective than conventional explosives if enemy forces (or the target population) are prepared and possess adequate protective gear. This

assessment roughly aligns with anecdotal evidence from Syria where chemical weapon inspectors, as well as military personnel, argue that chemical attacks do not offer significant tactical advantages or produce excessive death tolls in direct comparison to conventional bombings.<sup>36</sup> However, other than conventional explosives, chemical warfare agents are not necessarily bound to a specific area (e.g., a fixed blast radius) but can be transported to other areas depending on wind directions and other environmental influences. Finally, most chemical agents including phosphine are heavier than air and, thus, are especially effective in the basement areas of buildings; areas where people might seek shelter during an attack.

b. Soft damage

There is no academic discussion available on the psychological and political impact of terrorist attacks using phosphine. However, in order to assess this soft damage, it is necessary to discuss the soft damage of chemical agents in the hands of terrorists in general. The role of fear and politics in chemical terrorism can be discussed by referring to already published analyses.

Next to the (arguably limited) hard damage inflicted by chemical agents such as phosphine, a terrorist attack with an improvised chemical device would primarily inflict widespread fear and panic among the affected population. This soft damage caused by chemical agents was particularly visible during the attack against the Tokyo subway in 1995 (Danzig et al., 2011, pp. 33–34; Parachini, 2001, p. 391). The dissemination of sarin in the

---

<sup>36</sup> Personal conversation between the author and a former OPCW chemical weapons inspector in 2018.

underground infrastructure of Tokyo did not only kill 12 people but caused mass panic among subway passengers. Coupled with inadequate information about the nature of the attack, this widespread anxiety caused over 5,000 people to seek medical attention due to actual or believed symptoms caused by sarin exposure (Smithson & Levy, 2000, report 35). One of the key details of this case was that neither the exposed subway passengers nor the first responders and the hospital personnel had any knowledge about the nature of the chemical agents that they were exposed to (G. Ackerman & Jacome, 2018, footnote 19; Smithson & Levy, 2000, report 35). The hospitals in the area quickly became overburdened with the number of new patients, of which the majority sought unnecessary medical help. Furthermore, the decontamination efforts and the clean-up operations in the subway systems added to this anxiety and caused people to avoid the area as well as produced fear-inducing imagery in media outlets worldwide.

With regard to this example, it is important to note that an attack with phosphine would not require any decontamination efforts that would surpass the ventilation of the area or building in which the attack happened. However, as happened in Tokyo in 1995, it is likely that neither the victims of the attack nor the first responders will have any knowledge about the specific agent that was used in the attack. Hence, it is thinkable that fire departments and counter-terrorism forces will arrive on the crime scene with personal protective equipment (PPE) that would be necessary for a chemical attack (in that case the most likely PPE would be HAZMAT suits of level B) (See for general classification Pichtel, 2011, pp. 315–334). As already shown in the case of ricin, the presence of responders with PPE would likely contribute to public anxiety and, hence, would add to the soft damage of the

attack.

Next to anxiety, a chemical attack in a Western democracy would cause political damage as well as damage to institutions. In the current global political environment in which a chemical attack would be directly or indirectly linked to the atrocities in the theatre of the Syrian civil war, the terrorist use of chemical agents would transport the message that the war in Syria is being further internationalized and is (at least indirectly) reaching Western democracies. Security institutions and governments would, potentially, lose public trust after such an attack, because it would be assumed that they are not able to shield their societies efficiently from the (direct or indirect) dangers evolving out of the conflict in Syria. In the special case of phosphine, this connection would be even more visible because ISIL used not only chlorine and sulfur mustard against combatants and civilians in Syria but also experimented with the use of phosphine as a chemical weapon in this region (G. Ackerman & Jacome, 2018, p. 29; Binder et al., 2018, p. 28; Quillen, 2016, p. 1025; Strack, 2017, p. 19).

c. Length of attack

Just like in the case of ricin, an attack with phosphine might require very few actions on part of the perpetrator and, thus, is difficult to interrupt by first responders or law enforcement officers. One likely way of using phosphine in an attack is to disseminating it by mixing some kind of metal phosphide tablets (such as calcium phosphide) with water directly on the scene of the attack (Bogle et al., 2006). It is important to note that such a production and dissemination of phosphine would only have a substantial

effect in enclosed spaces such as trams, buses, tunnels or elevators. Furthermore, the gas would be produced and released at a pace that would allow potential victims of the attack to leave the area before significant health effects occur. Finally, this style of attack would take at least a few minutes; minutes that would make it (at least in theory) possible to interrupt the perpetrator and stop the attack.

Another, more dangerous, way of disseminating phosphine would be to produce the gas before the attack, store it in containers and combine these containers with a small IED that opens them while detonating. In this attack, the length of the attack would shrink down to 2 or 3 seconds and, hence, would be almost impossible to interrupt once the perpetrator pressed the button to detonate the IED. However, it has to be noted that this style of dispersing phosphine would only cause significant effects in enclosed spaces and might not release phosphine in an ordered way that is necessary to kill or seriously harm potential victims beyond the blast radius of the IED. For it is likely that the detonation of the IED seriously interferes with the structural integrity of the enclosed area (e.g., it rips a hole in a bus) and, thereby, causes the released phosphine to disintegrate quickly.

#### d. Uncertainty of consequences

Finally, a chemical attack against an urban area would necessarily include multiple layers of uncertainty with regard to the consequences of such an attack. This uncertainty is particularly pressing in the case of phosphine since this agent has not been used as a warfare agent extensively. Hence, empirical data about the possible consequences of a phosphine attack is

lacking.

Yet, one major part of the uncertainties involved in a phosphine attack is the result of the difficulties of identifying the nature of the chemical agent shortly after the attack. The existence of a large variety of different chemical agents can cause first responders to prepare for worst-case scenarios rather than counter-measures directed at this specific agent: while some agents (like phosphine) are known to disappear within minutes or hours after their use, others, such as VX, are very persistent and render areas uninhabitable for weeks (Pichtel, 2011, pp. 48–52).

Furthermore, many chemical agents are nearly odorless (if in pure form) and might only cause symptoms hours after exposure. This makes it very difficult for first responders to clearly identify the nature of the attack (Pichtel, 2011, Chapter 2). Both first responders and the affected population are faced with uncertainty concerning the nature of the agent that they have been exposed to and concerning the severity of health-related consequences of this exposure. This uncertainty adds to anxiety and, in general, to the psychological impact of phosphine as a chemical weapon. The case of the Tokyo subway attack as well as the recent case of Salisbury are examples of the tremendous effects of uncertainty with regard to chemical weapons in general.<sup>37</sup>

---

<sup>37</sup> The case of the attempted assassination of the Russian dissident Sergei Skripal is very an interesting, “positive” example with regard to uncertainties involved in the assessment of consequences of chemical attacks. The chemical agent that was used for the attack, the Novichock agent, has been suspected to be the most deadly chemical agent in the world (Faulconbridge & Holden, 2018; Sidell et al., 1997, p. 75). However, the assassination with the agent failed. Furthermore, considering the toxicity and the amount of Novichock that

However, as already portrayed in the case of biological agents, chemical agents like phosphine might be very sensitive to environmental circumstances such as weather, wind and temperature. That does not only make it very difficult for first responders and security agencies to give reliable estimations of the effects a phosphine attack would have in a given urban area. It also leaves potential perpetrators with a large amount of uncertainty with regard to the success of their attack.

### 2.3. Americium

#### a. Hard damage

The physical damage caused by a terrorist attack with americium is considered to be very limited in research. One of the most detailed accounts of the expected hard impact caused by a radiological attack with americium is the master dissertation of Jessica Satterfield (Satterfield, 2011). In this dissertation, Satterfield discusses the possibility that terrorists might attempt to use  $^{241}\text{Am}$  from smoke detectors to construct an RDD.<sup>38</sup> With regard to this isotope, Satterfield states that “for [a potential terrorist]<sup>39</sup> to acquire enough americium to concern federal officials, he would have to purchase or steal at least 16 million smoke detectors” (Satterfield, 2011, p. 20). Note that Satterfield makes it explicit in her analysis that health threats to human

---

the citizens of the town Salisbury were exposed to, the tragic death of only one person seems very surprising (Schwartz, 2019).

<sup>38</sup> In this scenario, the RDD would consist of a small IED that is simply strapped to a considerable amount of americium in order to disperse the isotope during the detonation. Satterfield refrains from giving a detailed description of the process of extracting the americium in order to combine it with the IED.

<sup>39</sup> In her dissertation, Satterfield uses the case of Dhiren Barot as an example. See below for a more detailed description of this case.



beings caused by the radiological substance in question shall be the basis for concern to security officials. Within the boundaries of this definition, an attack with a realistic amount of  $^{241}\text{Am}$  sources seems, indeed, incapable of inflicting any casualties via radiation. If at all, the negative health effects of the  $^{241}\text{Am}$  source would not surpass the blast radius of the IED that it is combined with to form an RDD. By referring to historical cases of terrorist RDD plots, Satterfield states that “[a] plan to acquire 10,000 smoke detectors would have provided him [Dhiren Barot] with 0.01 curie of americium, which is far too little material to cause a health threat to one person, let alone 500” (Satterfield, 2011, p. 20).

In addition to Satterfield, other authors have argued as well that terrorist groups might refrain from using RDDs, including with sources like  $^{241}\text{Am}$ , “because of their lack of outright lethality and visceral violence as compared to the alternatives (...)” (G. Ackerman & Jacome, 2018, p. 26). However, as will be made clear in the next section of this chapter, the hard impact of an RDD does not need to inflict casualties or even have negative health effects via radiation to be a suitable terrorist weapon. Rather, the *measurability* of radiation is sufficient as hard impact to make  $^{241}\text{Am}$  based RDDs efficient (and, hence, dangerous) tools for terrorists.

A historical example can be used to support the claim that incidents with a realistic amount of  $^{241}\text{Am}$  sources involved show heightened radiation levels that are clearly surpassing normal values of background radiation. The 5th Report of the Standing Working Group on Safe Transport of Radioactive Materials in the European Union from 2006 includes an accident involving 900 ionizing smoke detectors in France in 1999 (European Commission,

2006). The authors of the report state that a truck transporting these smoke detectors caught fire close to the small town of Langres. Furthermore, they describe that “[t]he overall activity of the cargo was 3.96 MBq, i.e., 0.02 A2” (European Commission, 2006, p. 46). Six days after the fire department arrived at the site of the accident and contained the fire, an operational team of the Radiation Protection Agency measured the radiation levels at the site and the trailer. Here, the report states that

[a]t the fire location, alpha contamination equal to 10 times the background level was recorded over a 1 m<sup>2</sup> area. The result of the soil sampling showed a 3,700 Bq/kg activity. A lower activity was also detected down the highway, due to the spillage of water used by the firemen. The burnt chassis of the truck trailer (stored by a scrap merchant) showed spot contamination, and burnt debris were found with an activity of 12,000 Bq/kg (European Commission, 2006, pp. 46–47).

While it has to be stressed that these levels of radiation did not pose significant health risks to the firefighters or other human beings in the proximity of the accident, it is evident that the burning of 900 <sup>241</sup>Am smoke detectors is capable of creating radiation hotspots with activity up to 12,000Bq/kg. Even this fairly high level of activity is unlikely to cause negative health effects. Yet, it is clearly recognizable as a direct outcome of the accident and, hence, transforms this road accident into a radiological accident. The measurability of heightened radioactivity is the only hard impact that an <sup>241</sup>Am based RDD might be capable of producing. However, this limited hard impact is accompanied by a tremendous soft damage.

b. Soft damage

Unlike the physical damage inflicted by a  $^{241}\text{Am}$  based RDD, the soft damage of such a device would be severe. First of all, even an RDD that only disperses low radioactive particles and materials requires specialized personnel and units of fire departments to clean the area and, if necessary, decontaminate structures and persons. Hence, the ground zero of the attack would, in any case, be evacuated and emergency personnel in HAZMAT suits of the categories A or B would be present. As already discussed in the sections on ricin and phosphine, these efforts alone would be sufficient to inflict wide-spread anxiety and, hence, cause substantial psychological damage.

Yet an attack with a  $^{241}\text{Am}$  based RDD would have another, significant effect: although not hazardous on a large scale, the radiation released by such an RDD attack would spread tremendous fear not only among the citizens geographically affected by the attack but among the whole target society (For detailed discussion see Khripunov, 2006; Satterfield, 2011, p. 41). Since radiation is not detectable by the human sensory apparatus, people will fear for their health in widespread areas without being able to unambiguously assess the health risks for themselves and their families.

Furthermore, it has to be noted that Western societies like, for example, the Canadian society, do not seem well-informed with regard to the nature of a radiological attack. According to interviews performed in 2008, most Canadians are unable to tell details about radiological terrorism or to differentiate between radiological and nuclear attacks. One in 8 of the

respondents even misinterpreted radiological attacks as nuclear attacks (Etchegary et al., 2008, pp. 488–489). This misinterpretation, however, extrapolates the soft impact of a radiological attack dramatically by exaggerating the threat that society is exposed to. For example, if a family in Germany hears about a radiological attack in the inner city of Berlin on the radio, their minds might go directly to pop-cultural references to nuclear Armageddon or worst-case scenarios from the era of the Cold war. Only few people would interpret this news message as a minor incident that might not affect an area greater than a few hundred meters (For discussion concerning “Radiophobia” and Cold War, see Khripunov, 2006, pp. 277–280).

Due to the un-detectability of radiation, the society affected by a radiological attack is completely dependent on Governmental institutions in receiving information on possible health effects due to radiation in their area. However, in case of past nuclear accidents like the ones in Chernobyl (Ukraine) and Fukushima (Japan), it was publicly criticized that people were not sufficiently warned against the health effects of heightened radiation levels in their areas by their respective Governments (Dickstein & Vanunu, 2016, pp. 13–15).

In the case of Chernobyl, this lack of clear communication was even debated in Germany at the time. Hence, it is reasonable to assume that the mere existence of a radiological threat in a country could contribute to the erosion of trust in governmental institutions with regard to crisis communication. More fear and psychological stress in the target society would be the consequence (Khripunov, 2006, pp. 283–285 and 286–288). Even if there are no dramatically heightened levels measured in the

aftermath of an attack, the nature of the attack as a radiological attack could be sufficient to erode trust and spread panic.

A similar mechanism was visible in the aftermath of the meltdown of the reactor Fukushima II in Japan in 2011: In the weeks after the meltdown, sales of Geiger counters and Iodine tablets in Germany increased dramatically since parts of German society feared heightened radiation levels and health risks from the meltdown (Theobalt, 2011). Although the German government stressed multiple times that it would be impossible to be exposed to hazardous radiation levels coming from Fukushima in Germany, many people tried to measure radiation levels on their own without understanding how Geiger counters work or how to properly measure and interpret radiation levels (Frankfurter Rundschau, 2011). The result was widespread confusion (that stemmed from a misinterpretation of, for example, background radiation) and even more anxiety.

c. Length of attack

There are, in principle, two ways of manufacturing a weapon from a radiological source. First of all, radiological material can be dispersed with the help of an IED. This so-called RDD spreads radiation by means of radioactive debris and particles as the result of the detonation of the IED. The second possibility to use a radioactive isotope as a weapon would be to expose people to the unshielded isotope. This method is called a radiological exposure device (RED) and involves an unshielded radioactive source. This source is, for example, placed under the seat of a bus or a tram in order to expose a large number of persons to a substantial amount of

radiation. Obviously, this second possibility requires a long time span for the attack and, hence, can be detected, interrupted and stopped at any given moment.

In the description of  $^{241}\text{Am}$  as source of a radioactive weapon of terror, it is important to note that only the RDD weapon type is of relevance. As already shown in an earlier section of this chapter, the  $\alpha$  radiation that the isotope  $^{241}\text{Am}$  emits would not be sufficient to cause any health risks solely by being unshielded. Some authors even note in this regard that the  $\alpha$  rays emitted by this isotope can simply be stopped by a piece of paper. Hence, there would be no effect whatsoever if one would use  $^{241}\text{Am}$  as a source for a RED. That leaves a potential perpetrator with the use of  $^{241}\text{Am}$  as the radioactive source in an RDD. However, since RDDs are, in their essence, modified IEDs, an attack with such a device would not be interruptible or stoppable once the perpetrator ignites the device.

d. Uncertainty of consequences

As shown in an earlier section of this chapter, the presumed hard damage caused by an RDD with  $^{241}\text{Am}$  as radioactive source is unlikely to cause any physical damage or health risks that surpass the effect of the IED that is a necessary part of the RDD. Yet, the example of the accident in Langres (France) in 1999 shows that it might be difficult to predict how  $^{241}\text{Am}$  behaves if exposed to extreme heat or if dispersed by detonation. Hence, if first responders measure heightened radiation levels at ground zero of an IED attack, there is, at least theoretically, always a danger of encountering radiation hotspots with extremely high radiation levels in comparison to the

levels measured in the surroundings. Hence, when handling debris from a blast site with some sort of radioactive material involved, it is to be expected that first responders behave according to the precautionary principle to account for possible radiation hotspots and unexpected levels of radiation in the surroundings. Obviously, these precautionary measures call for visible safety equipment and, thereby, add to the soft impact of a  $^{241}\text{Am}$  based RDD. Furthermore, the lack of public knowledge about the nature of radiation as well as the above-described anxiety and distrust when it comes to radiological incidents will be only fueled by the uncertainties involved in assessing and measuring the effect of an RDD (Khripunov, 2006, pp. 283–285).

It has to be noted that in case of a radiological device that is based on  $^{241}\text{Am}$ , a possible perpetrator is not exposed to a large number of uncertainties since the use of  $^{241}\text{Am}$  in an RDD would not have the aim to cause any physical damage via radiation. Rather, the perpetrator aims to create an atmosphere of fear by performing an attack with measurable, heightened levels of radiation in the aftermath. While the extent of these levels is surely uncertain, the fact that there will be some measurable effect by detonating a substantial amount of  $^{241}\text{Am}$  is almost certain.

### 3. Probability of use

#### 3.1. Ricin

##### a. Availability

When discussing the availability of ricin to malicious agents, one has to distinguish between the already processed and pulverized agent and the seeds of *Ricinus communis* that contain ricin in its unprocessed form.

Ricin is considered a toxin warfare agent by the OPCW of the United Nations and, hence, part of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (CWC) (Organisation for the Prohibition of Chemical Weapons, 1992). According to this convention, the production and stockpiling of ricin is forbidden for both nation-states and non-state actors

<sup>40</sup>.

In addition to that, the European Union uses its Council Regulation (EC) No 428/2009 to make it explicit that, although considered a dual-use substance, ricin is part of the CWC. The regulation states that there is “(...) no National General Authorisation for intra-Community trade” of this substance. Furthermore, several nations introduced fierce restrictions on the production and use of ricin in accordance with the CWC. For example, in Germany, ricin is considered a forbidden weapon of war according to the *Kriegswaffenkontrollgesetz* (Regulation on the control of weapons of war)

---

<sup>40</sup> With regard to non-state actors, the CWC calls upon the signing nation states “to enforce that prohibition in respect of persons (natural or legal) within their jurisdiction.” (Organisation for the Prohibition of Chemical Weapons, 1992).



and is not to be produced or stored with very few exceptions. All these restrictions on international, European and national levels would make it exceptionally difficult for small terrorist cells or lone actors to acquire already processed ricin without raising flags with national or European security agencies. Yet, there is another, drastically more accessible, way of acquiring ricin that ought to be discussed in more detail.

All the strict regulations that were mentioned above do not apply to naturally occurring goods that contain ricin; i.e., castor beans. First of all, it has to be noted that the plant *Ricinus communis* is abundant in the Mediterranean region and the tropics. Hence, it is possible to harvest castor beans from naturally growing plants in these regions.

Furthermore, the possession and trade of castor beans are not subject to any regulations relevant to security on European or national levels. Hence, while the acquisition and possession of ricin are illegal, the acquisition and possession of *Ricinus communis* and its seeds are not. In fact, castor beans can be ordered online via numerous retailers for low fares. The reason for this unrestricted trade of castor beans is the use of *Ricinus communis* in recreational gardening as well as the widespread use of castor oil as a laxative, moisturizer and natural remedy. Thus, a potential terrorist that is interested in ricin might not attempt to acquire already processed ricin but rather castor beans. One example of this strategy is the case of the Cologne ricin plot in which the perpetrator ordered castor beans online in order to extract ricin from the seeds.<sup>41</sup>

---

<sup>41</sup> A detailed discussion of this case can be found in chapter 7 of this thesis.

## b. Required expertise

However, in order to extract ricin from the seeds of *Ricinus communis* and to successfully weaponize this agent, some specialized expertise is needed. First of all, it has to be noted that, in order to successfully disperse ricin in the most effective way in terms of hard *and* soft damage, an IED is needed. Hence, a potential perpetrator of a ricin attack needs sufficient knowledge to construct a simple IED from unrestricted or loosely restricted materials. In this regard, peroxide-based explosives, as well as ammonium nitrate (AN)-based IEDs, seem suitable candidates. Past incidents like the 7/7 bombings in London as well as the Oslo bombings in 2011 show that small terrorist cells and lone operators are able to assemble and successfully use IEDs with only little training or, in the case of Anders Behring Breivik, only with online manuals and trial and error testing. Thus, the construction of a simple IED seems within reach of terrorists in liberal democracies even without any in-depth knowledge and only on the basis of online manuals and self-acquired tacit knowledge.<sup>42</sup>

Since it is particularly difficult to acquire already processed, pulverized ricin, a potential terrorist would have to manufacture it by extracting it from castor beans. For this manufacturing process, a basic understanding of biology and chemistry is necessary. However, this knowledge does not have to go very deep if the terrorist is provided with a manual on how to extract ricin from castor beans. It is important to note that open source information websites such as Wikipedia already provide basic insights into the process

---

<sup>42</sup> For an in-depth analysis of the explicit and tacit knowledge that is necessary to manufacture IEDs with different explosives, see the unpublished master thesis of Feltes (2015).

of purifying ricin from its natural source. Chapters 8 and 10 of this thesis will discuss the details and issues with this abundance of information on the internet. Furthermore, an abundance of videos and documents such as the *Poisoner's Handbook* or the *Mujahideen Poisons Handbook* written by an author in the Jihadi community are available online and include ricin purification manuals. As Anne Stenersen pointed out, these documents provide the reader with simple manuals that do not demand a laboratory environment for purification processes (Stenersen, 2009, p. 53). Yet, Stenersen questions the quality of these manuals and shows, based on the findings of a Spanish laboratory experiment, that the process of ricin purification in the manuals will not deliver pure ricin, but a substance that consisted of only up to 0.33 percent ricin (Pita Pita et al., 2004; Stenersen, 2009, p. 53). Such a substance would clearly not be a mass casualty weapon but would still include the soft damage that any ricin-based device would be capable of inflicting.

A more recent source of detailed ricin purification manuals is the manifesto “2083. A European Declaration of Independence” by Anders Behring Breivik (Breivik, 2011). In his manifesto, Breivik describes two different, very simple ways of extracting ricin from castor beans and uses less than ten steps for each manual. These step by step manuals read like a cooking recipe and could easily be replicated by individuals without any prior knowledge in chemistry or biology.<sup>43</sup> Furthermore, Breivik provides online links to images and further information concerning the steps of ricin purification and he

---

<sup>43</sup> Please note that the author refrains from giving a detailed account of the actual process of ricin preparation. For a discussion concerning the issues with publishing “dual-use” and “dangerous knowledge” in this dissertation, please see chapter 6, chapter 8 and chapter 10.

describes the safety measures that are necessary for the process. He stresses that utmost care and attention has to be given in order not to get self-contaminated with ricin while preparing it. It has to be noted that especially the safe handling of ricin (and other toxic substances) during the process of manufacturing a weapon demands some degree of tacit knowledge that only can be gained in communication and experience-based learning with other knowledgeable individuals. In the case of the Cologne ricin case, the perpetrator apparently received some advice from knowledgeable ISIL affiliates via the messaging service Telegram (Flade, 2018, p. 3). The acquisition of ricin-related tacit knowledge simply via trial and error is, due to the toxicity of the agent, extremely dangerous for the manufacturer.

To sum up, little prior knowledge is needed to prepare a simple weapon with ricin. The internet and other terrorists, such as Breivik, provide the necessary manuals for ricin purification and describe the process in accessible steps. However, although the purification of ricin might be simple, the dangers of self-contamination are not to be underestimated.

#### c. Operational space

The preparation of an attack with ricin requires a safe operational space. This space allows it to plan the attack as well as purify the castor beans and manufacture the ricin device without enabling detection by security institutions. First of all, it has to be noted that the process of manufacturing a small IED demands, at least, an operational space that ensures both a sufficient degree of privacy as well as enough room to allow for the different steps in the production of explosives. Hence, a potential terrorist

would need, at least, a private apartment for the process of manufacturing, for example, peroxide-based explosives or a whole building in order to manufacture an ammonium nitrate-based explosive of a reasonable size (See case studies in Feltes, 2015).

Furthermore, it is important to note that, if a terrorist has to acquire the necessary tacit knowledge to manufacture an IED via trial and error, then a larger and more remotely located operational space is needed. One example of such a strategy is Anders Behring Breivik's farm outside of Oslo, where he was able to perform detonation tests of small amounts of ammonium nitrate mixed with fuel oil (ANFO) and ANALFO/ANALNM<sup>44</sup> and, thereby, gained the tacit knowledge necessary to successfully construct and detonate the IED for his attack.<sup>45</sup>

As both Stenersen describes and the Cologne ricin plot shows, the extraction process of ricin as propagated in online manuals does not demand a laboratory environment. According to the manuals, ricin could be purified even within a very constrained operational space such as a garage or a kitchen of an apartment (Stenersen, 2009, p. 53). For example, Sief Allah H, the perpetrator of the Cologne ricin plot, only had two small apartments as operational space to prepare his ricin device. Apart from undertaking preparations to manufacture a peroxide-based IED, H. succeeded in processing around 84.3 milligrams of powdered ricin in this environment (Flade, 2018, p. 3). Presumably and based on the existing manuals, he did

---

<sup>44</sup> ANALFO stands for ammonium nitrate fuel oil and ANALNM stands for ammonium nitrate nitromethane.

<sup>45</sup> A more detailed analysis of the tacit knowledge and operational space necessary for IED manufacturing can be found in the unpublished thesis of Feltes (2015).

not need more than big buckets or a bathtub as a vessel and small instruments like coffee grinders for this purifying process. However, it has to be noted that the process of pulverizing ricin in a small operational space like an apartment presents a serious health risk to the perpetrator as well as to other inhabitants of the building. While the perpetrator might succeed in undertaking the necessary precautionary measures, his or her neighbors might be exposed to ricin powder spreading from the perpetrator's apartment. The consequence of this exposure might be fatalities in the building and, hence, a high risk of exposure and arrest.

In summation, it has been shown that it is possible to manufacture simple ricin-based IEDs in very small operational spaces such as apartments. However, the necessary tacit knowledge in IED manufacturing and the health risks of ricin exposure in the manufacturing process might demand larger operational spaces such as farms or buildings in remote areas. Moreover, manufacturing in remote areas might minimize the risk of arrest.

#### d. Tactical and ideological advantage

In order to answer the question of whether ricin would offer any tactical advantage to, or would be ideologically permitted by, a terrorist group, it is necessary to take a look at the track record of terrorism-related incidents involving ricin. A description of these events can help to give a first overview of what kind of terrorist groups might gain a tactical and ideological advantage from using the agent in an attack. For whether or not a certain weapon offers a tactical advantage to a terrorist group, depends on the strategic and tactical objectives as well as the ideology of said group.

First of all, it has to be noted that ricin is among the most popular biological agents in terms of acquisition and (attempted) use by terrorist groups and other non-state violent actors (VNSA). According to the Profiles of Incidents Involving CBRN Use by Non-state Actors (POICN) Database of the START consortium that lists over 517 cases of incidents involving CBRN materials (Binder & Ackerman, 2019), ricin has been used in 6.9% (36 cases) of all listed cases involving CBRN agents (Binder & Quigley, 2019). In the database, ricin is by far the most used agent among all known biological agents in past CBRN-related incidents involving VNSA. The largest group of perpetrators in terms of ideologies in this sample is individuals and cells with an Islamist background. Hence, Islamist terrorist groups and inspired lone operators seem to be one of the most prevalent groups of VNSA that could gain a tactical and ideological advantage from the use of ricin. This result corresponds with multiple studies that have shown that Islamist terrorist groups such as al Qaeda and ISIL have been interested in the acquisition of biological agents (G. Ackerman, 2009; G. A. Ackerman & Pereira, 2014; G. Ackerman & Jacome, 2018; Carus, 2001, 2017; Dukic, 2017; House, 2016; Hummel, 2016).

For example, the Cologne ricin plot can show in what form the use of ricin could offer a tactical advantage to Islamist cells and why the Islamist ideology could be seen as lenient towards the use of biological agents. As a lone operator that swore allegiance to ISIL, Saif Allah H. attempted to commit an attack that was both simple enough to be prepared without a large number of resources and expertise but with a high impact in comparison to other lone actor tactics such as knife attacks. An attack with a simple ricin-based IED would certainly be (and arguably was) a show of

strength for ISIL and would have created (and, again, arguably did create) widespread anxiety. Arguably, the public outrage following the construction of a "layman's WMD" or a "bio-bomb" as the German news coverage put it, was the most important tactical advantage to H. and his affiliates. Hence, in this plot, ricin seemed to be the weapon of choice since its stigma as a biological weapon and the connected soft impact would benefit ISIL's tactical objectives in Germany in an innovative – and for lone operators achievable – way (For general debate about lone operators and CBRN capabilities, see Gary A Ackerman & Pinson, 2014).

However, one other key element in this regard is the Islamist ideology. For if a certain weapon or attack target does not correspond with the ideological foundation of a certain terrorist group, this weapon or target would not offer any advantage to said group (For a discussion on ideology and target selection see Drake, 1998). For example, the first generation of the RAF was not primarily interested in acquiring indiscriminate weaponry since their specific Marxist-Leninist ideology did not allow to target random civilians indiscriminately. However, ISIL as a religious extremist group that could, arguably, be characterized as an apocalyptic cult does not seem to have the same ideological restrictions (de Graaff, 2016). Rather, every individual who does not share the group's specific interpretation of Islamic religion is a legitimate and potential target. Furthermore, many of ISIL's followers regard the fight of the group as the battle before Judgement Day (For a general discussion, see de Graaff, 2012). This ideology allows for a wide range of weapon technologies including highly indiscriminate biological weapons and toxins such as ricin.



Another group of VSNA that might gain a tactical and ideological advantage from the use of ricin as a weapon is the group of lone operators and small cells with a right-wing extremist background. While the POICN database only contains a few entries of attempted use or acquisition of ricin by right-wing extremists, a recent study has argued in a convincing manner that especially lone operators with this ideology might be interested in CBRN weapons including toxins (Koehler & Popella, 2018).

One recent example of such a motivation to, at least in theory, acquire biological toxins like ricin is the manifesto 2083 by Anders Behring Breivik. As already discussed above, Breivik describes ricin as a possible weapon agent for the fictional patriotic movement that he called the *Pauperes commilitones Christi Templique Salomonici* (PCCTS) Justiciar Templers. In his manifesto, he claims to be “one of several commanders” (Breivik, 2011, p. not specified) of this group. According to Breivik, the PCCTS should be seen as some kind of Christian resistance against what he called the “Islamization of Europe” through “cultural marxism”. In his manifesto, Breivik describes the use of poisoned bullets against soft targets as one tactic in the struggle of the PCCTS. He writes:

For those Justiciar Knights who feels it would be simply too risky or unrealistic to successfully manufacture explosives of the appropriate or required quanta there are other just as efficient methods of shock attacks that are available to us. Shock attacks or more precisely armed assaults, involving assault rifles or pistols, on concentrations of category A and B traitors, should be combined with the application of poison bullets. (...) The purpose of using chemical or biological rounds

is to inflict [sic] fatal poisoning should the target fail to die from external or internal bleeding from the projectile itself. A relatively simple procedure and manufacturing technique converts your projectile weapon into a chemical or biological weapon (Breivik, 2011, p. not specified)<sup>46</sup>.

Breivik proposes to use ricin-coated bullets for what he calls “shock attacks” that spread anxiety and disruption via the use of biological weapons and toxins. Furthermore, instead of advocating to use ricin in combination with an IED, he proposes to use it as a complementary weapon agent in a firearms attack in order to increase the soft damage caused by this attack.

Another detail in Breivik’s proposal on how to use ricin as a weapon agent is that he explicitly recommends attacks using this toxin for those terrorists that do not have the expertise or the operational space to successfully manufacture an IED. Hence, in Breivik’s perspective, the purification of ricin does not require the same degree of expertise and operational space that the construction of an IED would demand. Thus, his proposal to use ricin in an attack specifically addresses lone operators and small cells without extensive resources.

Breivik’s manifesto can be used as an insightful example of the tactical advantages that ricin offers to right-wing extremist lone operators and small cells. However, at first glance, the spectrum of right-wing extremist ideologies seems less permissive when it comes to the use of highly

---

<sup>46</sup> The author refrains from specifying page numbers in Breivik’s manifesto. A detailed discussion about this strategy of treating “dangerous knowledge” such as the manifesto can be found in chapters 8 and 10 of this thesis.

indiscriminate weaponry in comparison to, for example, Islamist ideologies. Yet, Koehler and Popella have shown that lone operators with this ideological background exhibit tactics that target [innocent] civilians just as indiscriminately as Islamist terrorists (Koehler & Popella, 2018). Furthermore, Breivik offers attempts to justify the use of highly indiscriminate weaponry such as CBRN in his manifesto. In his chapter “The use of chemical and/or biological weapons is going too far?” he, for instance, writes:

If you have moral quarrels remember that the multiculturalists are slowly exterminating us indirectly by allowing Islamic demographic warfare in combination with their refusal to ensure sustainable indigenous fertility rates. (...)It is your duty to use any and all means necessary to prevent the mass extermination of our cultures, identities and the ongoing genocide of the free peoples of Europe (Breivik, 2011).

Notably, Breivik uses a similar attempt to justify the use of highly indiscriminate weapons and tactics that Osama Bin Laden used in his frequently quoted declaration from 1998. In this declaration, he stressed that the use of WMDs against al Qaeda’s enemies would be in accordance with the group’s ideology and should, in fact, be seen as “a religious duty” (opp. cit. G A Ackerman & Pereira, 2014, p. 27).

To sum up, both Islamist and right-wing extremist lone operators and small cells of both ideologies have shown interest in using ricin in attacks and, hence, perceive the agent as both an enrichment to their tactics and in line with their ideological foundations.

## 3.2. Phosphine

### a. Availability

Unlike castor beans, phosphine-producing agents such as aluminum phosphide or calcium phosphide are subject to restrictions in most Western democracies including the United States of America and the European Union. In the USA, the purchase and use of phosphine and phosphine-producing substances as pesticides is limited to certified personnel of specialized companies in the field of pest control. For example, the Environmental Protection Agency (EPA) classifies aluminum phosphide-based pesticides as so-called “Restricted Use Pesticides (RUP)” due to an inhalation hazard for humans.<sup>47</sup> Furthermore, the Department of Homeland Security considers phosphine as a “chemical of interest (COI)” according to the Chemical Facility Anti-Terrorism Standards (Department of Homeland Security, 2019). In accordance with these standards, every US facility that possesses phosphine in quantities that surpass a certain threshold quantity has to report their possessions of this chemical to the Cybersecurity and Infrastructure Security Agency (CISA).

On the European level, phosphine and phosphine-producing chemicals are regulated as well. Phosphine is labeled as a dangerous substance in accordance with the Classification, Labelling and Packaging (CLP) Regulation. Amongst others, the label applied to phosphine according to the CLP regulation is GHS06 “Acute Toxicity”<sup>48</sup>. Additionally, according to the

---

<sup>47</sup> See EPA, 40 CFR 152.175 - Pesticides classified for restricted use.

<sup>48</sup> See (EC) No 1272/2008.

risk management performed by EU-based companies in connection to the REACH legislation process of the European Chemical Agency (ECHA), phosphine is a gas that is explosive if heated and under pressure (ECHA, 2019).

More specifically, the European Union is calling upon its member states in several regulations and directives to regulate the sale and use of pesticides and to restrict the use of certain pesticides to professional users only<sup>49</sup>. For example, in case of aluminum phosphide as pesticide, the European Union recommends that its member states take necessary measures to restrict the use of this substance: “Authorisations [on state level] are subject to the following conditions: (1) Products shall only be sold to and used by specifically trained professionals.”<sup>50</sup>

Clearly, the European Union is urging its member states to implement the necessary legislation in order to restrict the use of phosphine-producing products such as aluminum phosphide and calcium phosphide. However, on a national level, these restrictions might differ between the member states and leave loopholes open that might be used by malicious agents to acquire these substances. For example, in Germany, the use of phosphine-producing agents is regulated by the *Verordnung zum Schutz vor Gefahrstoffen* (GefStoffV) as well as by the *Verordnung über Verbote und Beschränkungen des Inverkehrbringens und über die Abgabe bestimmter Stoffe, Gemische und Erzeugnisse nach dem Chemikaliengesetz* (ChemVerbotsV). Specifically, the GefStoffV identifies phosphine-

---

<sup>49</sup> See here especially Directive 2009/128/EC, art. 5 and 6 and more general in Regulation (EC) No 1107/2009.

<sup>50</sup> Regulation (EU) No 1034/2013, annex.

producing agents as chemicals that are only allowed to be sold to and used by individuals that possess a permission by a Governmental agency or with a certificate of good use (*Begasungsschein*). However, in the same article, the GefStoffV also specifies that private consumers do not need any permission or certificate if they intend to use a substance that includes not more than 15 grams of phosphine “on an occasional basis”<sup>51</sup>. Hence, in Germany, it is currently possible to purchase certain amounts of phosphine-producing substances without any restrictions..

Yet, although individual consumers are allowed to purchase, for example, small amounts of calcium phosphide without getting official permission to do so, the retail stores that sell these products have to take certain precautionary measures in accordance with the ChemVerbotsV. For example, retail employees, who are licensed to sell calcium phosphide products, have to verify that the customer in question is at least 18 years old. Furthermore, the customer has to convince the certified vendor that he or she will use the product according to its intended use as a pesticide for small-scale pest control operations on an occasional basis. Lastly, the vendor has to educate the customers about necessary protection measures, possible health hazards, and the appropriate waste management of the product. In addition to that, the relevant stores have to keep records of every purchase by documenting the details of the purchase and customer information such as full name and address in a notebook (*Giftbuch*).<sup>52</sup>

To sum up, in countries like Germany, it seems possible for a potential

---

<sup>51</sup> In the German original: “gelegentliche Tätigkeiten” GefStoffV, Annex I, number 4.2 (2).

<sup>52</sup> Phone interview and email contact with an executive of a relevant German agriculture supply company on 27 August, 2019. The interview partner preferred to stay anonymous.

terrorist to buy small amounts of calcium phosphide pellets. However, he or she might need several IDs or other convincing ways to show different names and addresses to be stored in the *Giftbuch* in order to avoid attracting the interest of security institutions.<sup>53</sup>

b. Required expertise

A very low level of expertise is required in order to manufacture a simple phosphine dispersing device. A potential perpetrator of a phosphine attack would only need to have a basic understanding of how to efficiently store gases such as phosphine in canisters since the production of phosphine from calcium phosphide pellets is described in the product description of the pellets. In addition to the pellets, only H<sub>2</sub>O is needed to produce phosphine. Hence, a potential terrorist does not need prior knowledge to manufacture phosphine, but has to have a suitable delivery system to disperse the agent. In this regard, terrorists might choose spray mechanisms in large open areas or canisters filled with phosphine in small enclosed areas. The latter one might be opened with the help of a small IED in order to avoid harming the attacker.<sup>54</sup> Here, it is important to note that especially affiliates of ISIL with ties to the civil war in Syria might possess tacit knowledge to appropriately store and release toxic gases such as phosphine since ISIL repeatedly experimented with and used phosphine-based devices in Syria. Key individuals of the ISIL predecessor al Qaeda in Iraq (AQI) established training curricula for chemical warfare as early as 2002 and other experts,

---

<sup>53</sup> A detailed discussion about the *Giftbuch* and the relevant mechanisms of detection can be found in chapter 7 of this dissertation.

<sup>54</sup> One example of such a delivery system is the al Qaeda-attack with chlorine canisters in Iraq that was described earlier.

such as Suleiman Daoud Al-Afari, probably distributed valuable explicit and tacit knowledge amongst ISIL affiliates in Syria and Iraq before being captured by US Special forces in 2016 (Strack, 2017, p. 21). Hence, a knowledge transfer concerning ways to store and handle toxic gases to operatives in the West is a real possibility and might already happen (Nesser et al., 2016). A precedent for such a transfer was detected in Australia in 2017, where two ISIL affiliates received instructions on chemical device manufacturing from an ISIL individual in Syria via the internet (Strack, 2017, p. 22).

However, not only among Islamist groups but also in the right-wing terrorist environment, there is knowledge transfer with respect to the manufacture and handling of toxic gases. For example, Anders Behring Breivik describes the use of hydrogen cyanide-based pesticides as a chemical weapon and writes that “[t]he product [certain pesticide] is currently only produced by one Austrian company, but it is easily obtainable. The “acid gas” vaporizes as soon as the hermetically sealed containers are opened.” (Breivik, 2011, p. not specified). In this passage, Breivik stresses the ease of use of this product; an argument that can be extended to phosphine-producing pesticides such as calcium phosphide pellets.

Depending on the way the potential terrorist aims to disperse the gas in a disclosed area, he or she additionally might need some expertise in order to manufacture a simple IED that breaks the canisters and, thereby, releases and possibly ignites the phosphine. The expertise that is needed to build such an IED was already discussed in section 3.1 b. of this chapter as well as in the unpublished master thesis of the author (Feltes, 2015).



### c. Operational space

The operational space to prepare a small phosphine-based device would not surpass the operational space that is needed to manufacture an IED or a ricin-based device, as described in section 3.1. c of this chapter. However, since some phosphine products might exhibit a strong odor that resembles the odor of fish or garlic, a potential terrorist risks exposure while handling this agent in an urban environment such as an apartment unit. Furthermore, the debris produced by the unpacking of large amounts of small bags of calcium phosphide pellets could attract the attention of neighbors and security institutions. Additionally, in a small apartment without ventilation, the terrorist might expose herself and other people in the building to harmful amounts of phosphine by accident. Larger operational spaces such as farms or garages in a rural environment would allow a safe preparation of the agent without detection.

### d. Tactical and ideological advantage

Due to its high degree of soft damage, both Islamist groups and right-wing lone operators seem to regard phosphine, or the use of chemical agents in general, as a tactical advantage.

As already discussed in some detail, both al Qaeda and ISIL have shown interest in the production and use of chemical warfare agents as weapons of terror. For example, with al-Zarqawi's training curriculum in Herat and another al Qaeda-led chemical weapons facility in Khurmul in the early 2000s, the group clearly exhibited the intent to manufacture and use chemical agents as weapons (Strack, 2017, p. 19). Furthermore, in 2006,

AQI allegedly committed several vehicle-borne attacks using chlorine by detonating vehicle-borne IEDs together with chlorine canisters in the Anbar province in Iraq (Strack, 2017, pp. 19–20).

As AQI's successor, ISIL has been showing interest in chemical weapons as well. The group experimented not only with chlorine and mustard agents but also with phosphine in the theatre of the Syrian civil war (Binder et al., 2018). However, it is highly debated whether the use of chemical weapons offered any tactical *military* advantage to ISIL in the region. Rather, researchers like Binder and Quigley stress that these agents have been considered tools of fear and terror in a region in which civilians are all too familiar with the threat of chemical attacks (Binder et al., 2018, p. 29).

However, Binder and Quigley also stress that the lack of propaganda of chemical weapons on ISIL's side may hint to a lack of interest or, at least, to the absence of a coordinated CW program by ISIL that is backed by its leadership (Binder et al., 2018, pp. 29–30). Yet, one could extend their argument about the soft damage of these weapons in the region and suggest that ISIL might use crude chemical devices in the West in order to transport the global outrage and fear of chemical weapons in the context of the civil war in Syria to Western liberal democracies. This psychological and political dimension of even a small chemical attack with the easily obtainable phosphine would certainly advance ISIL's strategical and tactical objectives in the West. As an apocalyptic group, the use of chemical and other CBRN agents would also not conflict with, but rather be seen as encouraged by, ISIL's ideology.

Next to Islamist groups, also lone operators in the right-wing spectrum, such as Anders Behring Breivik, showed a general interest in the use of chemical agents. Without specifically mentioning phosphine, Breivik described possibilities to use chemicals such as hydrogen cyanide in attacks against [innocent] civilians in his manifesto (Breivik, 2011, p. not specified). Furthermore, his chapter “The use of chemical and/or biological weapons is going too far?” clearly expresses the possibilities to use chemical agents in attacks without conflicting with his particular right-wing ideology.

### 3.3. Americium

#### a. Availability

Americium, or more specifically  $^{241}\text{Am}$ , is available for private consumers as a radioactive source in ionizing smoke detectors. Due to the small amount of  $^{241}\text{Am}$  in these detectors and because of the fast detection mechanism of these smoke detectors in comparison to optical smoke detectors,  $^{241}\text{Am}$  based smoke detectors are available in the USA without any restrictions. According to the U.S. Nuclear Regulatory Commission (NRC), “[c]ompanies that make ionization smoke detectors must have a license. However, people who purchase the smoke detectors for their homes do not need a license” (Environmental Protection Agency, 2019). Hence, with sufficient financial resources, a potential terrorist would be able to buy hundreds or thousands of these detectors in order to extract the  $^{241}\text{Am}$ . Obviously, purchasing hundreds of ionizing smoke detectors could raise suspicion, but this could be avoided by spreading individual purchases over time and space (different municipalities and states).

In most European states, the trade and possession of ionizing smoke detectors is regulated and restricted to specific vendors and consumers. The basis for these regulations is the European Council Directive 2013/59/Euratom that calls upon the European member states to perform risk assessments for ionizing consumer products such as ionizing smoke detectors. According to the directive, “Member States shall prohibit the sale or the making available to the public of consumer products if their intended use is not justified (...)”<sup>55</sup> or exceed the maximum activity threshold for ionizing consumer products that were set by the European Council. Hence, the European Union shifts the burden of prohibiting or allowing the sale and use of ionizing smoke detectors to its member states, albeit within the boundaries of the above-mentioned threshold values.

A similar approach is visible in the recommendations of the International Atomic Energy Agency (IAEA) concerning ionizing smoke detectors. The IAEA calls upon nation-states to achieve an “international consensus on harmonization of sale to the public” (IAEA, 2016, p. 51) of ionizing smoke detectors and other consumer products that include an ionizing radioactive source. Specifically, the IAEA argues that “[t]o this end, regulatory bodies should establish contacts with their counterparts in other States [sic] to agree on the procedures and criteria for undertaking safety assessments and for exempting from regulatory control the sale of radiation generators and consumer products to the public” (IAEA, 2016, p. 51).

Within the European Union, the achievement of such a consensus that is based on national safety assessments seems achievable since many member

---

<sup>55</sup> European Council Directive 2013/59/Euratom.

states already followed the recommendations of the IAEA and the European Council. For example, in Germany, the sale and use of ionizing smoke detectors are strictly regulated and restricted to professional applications such as on ships or in areas with specific explosion and fire hazards. The sale, possession and use of ionizing smoke detectors are regulated by the *Gesetz zum Schutz vor der schädlichen Wirkung ionisierender Strahlung* (StrlSchG) in Germany. In the *StrlSchG*, it is stated that every person or company who sells or installs ionizing consumer products such as smoke detectors with  $^{241}\text{Am}$  as an ionizing source requires permission to do so by the Federal Office for Radiation Protection (*Bundesamt für Strahlenschutz* (BfS)).<sup>56</sup>

To sum up, it seems very much within the capabilities of small terrorist cells and lone operators to successfully acquire a sufficient amount of  $^{241}\text{Am}$  in order to construct a small RDD with measurable radiation levels in the USA. However, national restrictions and EU safety directives might make it very difficult for the same actors to acquire this substance in most European member states.

#### b. Required expertise

Just as the physical effect of a  $^{241}\text{Am}$  based RDD, also the expertise that is needed in order to construct such a device cannot be determined with certainty. However, first of all, it has to be noted that the process of obtaining and removing the  $^{241}\text{Am}$  source from a smoke detector would not require any in-depth knowledge but would most probably consume a large

---

<sup>56</sup> StrlSchG art. 16, no.

amount of time considering the number of smoke detectors that are needed for a sufficient quantity of  $^{241}\text{Am}$  sources (Satterfield, 2011, p. 20). However, according to Satterfield, once removed from their shielding, the  $^{241}\text{Am}$  sources would have to be modified “into a form suitable for an RDD” (Satterfield, 2011, p. 20). Here, a prior understanding of the properties of  $^{241}\text{Am}$ , and ionizing sources in general, is necessary.

Several terrorist groups and lone operators have shown interest in the preparation and use of RDDs in general<sup>57</sup> and, hence, provide instructions on how to manufacture these devices. One of the most popular manuals with a special treatment of  $^{241}\text{Am}$  as a radioactive source of an RDD is the online document written by Dhiren Barot and his associates (See for discussion Satterfield, 2011).

Barot, an Indian al Qaeda affiliate, was, along with six co-conspirators, arrested by the British Metropolitan police in 2006. Amongst others, Barot and his associates pleaded guilty of preparing a terrorist attack with explosives and a “radioactive dirty bomb” (BBC, 2006). One detail about Barot’s arrest and trial is especially interesting for this section. According to the Metropolitan police, Barot and his group published a set of weapon manufacturing manuals that were most likely based on the tacit knowledge that Barot and others acquired in al Qaeda training camps. In these manuals, Barot described ionizing smoke detectors as a viable source for  $^{241}\text{Am}$  based RDDs (Ranstorp & Normark, 2009, p. 128). Barot suggested collecting the  $^{241}\text{Am}$  sources of around 10,000 smoke detectors and combining them with a simple IED in order to create an RDD (Satterfield, 2011, pp. 19–20).

---

<sup>57</sup> See for discussion section c. of this chapter.

However, according to Jessica Satterfield, Barot remains unspecific in his manual with regard to the details of modifying and processing the  $^{241}\text{Am}$  in a way that would be suitable for such an RDD (Satterfield, 2011, p. 20). Another example of an RDD manufacturing manual (albeit not specifically focused on  $^{241}\text{Am}$ ) is the document “Radioactive Pollution” that was uploaded to al Qaeda internet forums in 2006. With regard to this document, Anne Stenersen notes that “[d]etails on how to manufacture the RDD are not provided, the author simply suggests the user take the radioactive material and ‘put around it the explosives you have available.’ ”(Stenersen in Ranstorp & Normark, 2009, p. 57).

A similar level of sophistication in RDD manuals can be found in manuals with ties to right-wing extremism. For example, Anders Behring Breivik describes the nature and effect of RDDs in his manifesto. In the chapter “Radiological Dispersal Devices, RDDs; creating, deploying and detonating radiological bombs in Western European capitals”, Breivik offers a list of nine suitable radiological sources that includes  $^{241}\text{Am}$ . With regard to this specific isotope, Breivik notes that it is “widely used in smoke detectors” (Breivik, 2011, p. not specified). However, while Breivik goes into some detail on how to combine the radioactive material with a dispersive mechanism (in his case an IED or incendiary device), he fails to give instructions on how to prepare and modify the radioactive material in order to disperse it. However, the detailed account on how to disperse radioactive sources through shrapnel and other RDD-related recommendations make Breivik’s manifesto a particularly dangerous RDD manual on the Internet.

c. Operational space

The operational space that is necessary in order to construct a  $^{241}\text{Am}$  based RDD is comparable to the operational space that is needed for the preparation of a ricin-based IED. Next to the space to manufacture the IED that will be used as one of the two key components of the RDD, a potential perpetrator needs some space in order to store and modify large amounts of ionizing smoke detectors. However, as Satterfield mentioned, the sheer amount of smoke detectors that are needed to acquire a substantial amount of  $^{241}\text{Am}$  would pose a considerable risk of detection and arrest in an urban environment. Hence, in order to prepare the RDD, a safe house in a rural area would be advantageous as a potential perpetrator would be forced to handle substantial amounts of products and debris. Furthermore, although the radiation of  $^{241}\text{Am}$  sources from around 10,000 smoke detectors would not be sufficient to expose neighbors to hazardous radiation levels, measurable radiation hotspots due to the RDD manufacturing process might trigger detection in an urban area. Hence, a farm or a similar compound in a rural area would probably be the operational space of choice for a terrorist aiming to manufacture a radiological dispersal device.

d. Tactical and ideological advantage

In order to determine what kind of tactical advantages the use of a  $^{241}\text{Am}$  based RDD would bring and whether the use of such a device would be in line with the ideology of a certain terrorist group, it is necessary to give a short overview of past terrorist intentions to acquire and use RDDs.

Based on the manuals and attempts to acquire information and material in



order to build RDDs by al Qaeda affiliates, it can be argued that several individuals in connection to the network perceive this weapon as a tactical advantage for their agenda. In their own documents, these individuals stress the soft impact of RDDs. For example, in the document “Nuclear Pollution”, the author advises to

“(…) put the bomb in a city crowded with large markets and commercial shops (…) so that the government will close that area and everything around it because of the power of the material and the area of its dispersal. By this, you cause a large economic crisis to this country.” (op. cit. Ranstorp & Normark, 2009, p. 57).

However, as researchers like Stenersen have pointed out, despite efforts like Barot’s plot, most al Qaeda operatives seem to treat the use of RDD with a remarkable amount of disinterest in the relevant online forums and beyond (Stenersen in Ranstorp & Normark, 2009, p. 57). However, the manuals show that al Qaeda affiliates recognize the serious soft damage that the use of even a small RDD would inflict. In particular, small cells that are not capable of organizing a massive attack with advanced weaponry might see a tactical advantage in <sup>241</sup>Am in order to spread radiation-associated panic. The use of such devices would be covered by Osama Bin Laden’s fatwa from 1998, in which he specifically advocated and praised the use of CBRN weapons in Jihad. Documents containing fatwas with the same encouragements were found on laptops of arrested ISIL affiliates (G A Ackerman & Pereira, 2014).

Another group with a (partly) Islamist ideology has to be mentioned in

connection to RDDs; namely, the rebel groups involved in the conflict between Russia and the Chechen resistance movement in Chechnya. During this conflict, the resistance group leader Shamil Basayev expressed a strong interest in the use of RDDs and other radiological devices as weapons of terror. For example, in 1995, Chechen rebels with Basayev as commander buried a 13-kilogram box of the radiological element cesium 137 ((Cs)-137) in a park in Moscow to demonstrate the group's ability to perform radiological attacks in Russia (Bale, 2004). Basayev and his associates made this radiological threat in the hope that the fear of an actual RDD alone might offer them a tactical advantage in their struggle against Russian authorities.

Lastly, also right-wing extremist lone operators have displayed a strong interest in the use of RDDs to further their tactical agenda. One example in this regard is, again, Anders Behring Breivik. In his manifesto, Breivik describes the use and function of an RDD as follows:

Since a dirty bomb is unlikely to cause many deaths, many do not consider this to be a weapon of mass destruction. Its purpose would be to create psychological, not physical, harm through mass panic, and terror. For this reason dirty bombs are sometimes called "weapons of mass disruption". Additionally, containment and decontamination of thousands of victims, as well as decontamination of the affected area will require considerable time and expense, rendering areas partly unusable and causing devastating economic damage (Breivik, 2011, p. not specified).

With regard to his own, fictional, terrorist group PCCTS, he specifies the tactical use of RDDs by elaborating:

The PCCTS, Knights Templar intend to include radiological weapons in our arsenal as they are quite easy to create and relatively easy to acquire for those individuals with basic knowledge. However, we do not intend to detonate radiological weapons before the capitulation deadline given to the criminal multiculturalist regimes of Western Europe which is; Jan 1st, 2020. Preparations to acquire enough caesium and other radiological components should however begin immediately so that we are well positioned to effectuate attacks after the deadline. Our radiological attacks (RDDs) will cause minimal to no civilian casualties but will create devastating ideological, physiological and economical damage on the targeted cultural Marxist/multiculturalist regime (Breivik, 2011, p. not specified).

It is clearly visible from these two passages that Breivik perceives the use of RDDs as a massive tactical advantage for right-wing extremist lone operators and small cells. In particular, the large amount of soft damage inflicted by this weapon type seems to be in line with Breivik's agenda to target the so-called "cultural Marxist/multiculturalist regime" ideologically. In Breivik's view, the use of RDDs and, more specifically, the use of <sup>241</sup>Am based RDDs offers a massive tactical advantage and is ideologically justified. Yet, considering Breivik's great enthusiasm about RDDs, it is remarkable to note that he apparently never undertook efforts to acquire radioactive materials in order to construct such a device. One explanation

for this might be his fear of being exposed to lethal doses of radiation while constructing an RDD; a risk that he warns against at length but interprets as worth taking for other PCCTS operatives:

Let there be no doubt; the cost and complexity of using protective systems needed to protect the handler from radiation is not realistic. Our goal is therefore to use protective systems (hazmat suits, improvised and relatively inexpensive lead containers) that allow the builder/transporter of the bomb to survive long enough in order to successfully deploy and detonate it (Breivik, 2011, p. not specified).

#### 4. Conclusion

In conclusion, this chapter has shown that all three discussed substances (ricin, phosphine, and americium) create a reasonable high impact if used in a terrorist attack. This impact stems mostly from the soft damage created by the use of these substances. Furthermore, it has been shown that all three substances can be acquired without restrictions or with few restrictions and require only limited amounts of expertise and operational space to be prepared for an attack. Furthermore, this chapter stressed the importance of these weapons for the tactical agendas of, especially, small cells and lone operators with an ideological background in Islamist or violent right-wing extremism. Lastly, it was argued with selected examples that none of these substances were considered by these terrorist groups to be unacceptable weapons for ideological reasons.

Hence, ricin, phosphine, and americium-based improvised devices score reasonably high on both the Impact and the Probability of Use axes of the terrorist weapons rating system. That makes all three high-risk substances that Western democracies, in particular, need to protect themselves against by recourse to multi-layered counter-measures on the part not only of security institutions but also other stakeholders. As will be shown in the next chapters of this thesis, such a multi-layered web of counter-measures is capable of reducing both the scores of these substances on the Impact axis and the Probability of Use axis in the rating system. However, not only security institutions but also manufacturers, vendors, researchers, the press, and the public have to be involved in counter-measures against the terrorist use of ricin, phosphine, and americium.



# **Part II:**

## **Responsibilities and stakeholders**

## **4. The concept of collective moral responsibility**

### **1. Introduction**

A terrorist attack with a complex weapon system is rarely committed by a lone actor but involves the actions of multiple actors that are working towards a collective end (e.g., the detonation of a weapon). Terrorism with toxic substances as weapons can, hence, be characterized as a joint action (based on the account of joint action in Miller, 1995, 2001) of members of a group of agents; in this case, terrorists. Roughly speaking, a joint action is an action comprised of a set of individual actions each of which is directed to the same end (a collective end). Thus, two men lifting a crate onto a truck is a joint action; each lifts his side of the box and in doing so each has as an end to bring it about that the crate is relocated from the ground onto the truck. However, some joint actions, such as a large number of workers building (say) the Great Wall of China, are far more complex and take place over a far longer period of time.

What of those combating terrorists seeking to detonate a chemical, biological or radiological weapon? Due to the complex nature of these weapon technologies, the counter-measures against these weapons also have to be designed as joint actions of multiple members of various groups of agents having as their collective end to prevent and prepare for terrorist attacks involving the use of chemical, biological or radiological weapons.



However, whenever different agents cooperate in order to realize a collective end, questions of responsibility arise – not only with regard to causal responsibility but especially concerning *moral* responsibility. Here, it is necessary to take a step back and investigate the following questions: Who is (morally) responsible for the consequences that result from an action performed by members of a group of agents? Can a group itself be held responsible for a specific action? Or is it only the members of a group that are the bearers of responsibility for a joint action to which they contribute as well as, potentially, the outcome of that joint action? These questions refer to a prevalent issue in philosophy, namely the issue of collective moral responsibility.

The following chapter introduces the philosophical problem of collective responsibility and provides an overview of proposed solutions to this issue. In particular, this chapter investigates collectivist and individualist accounts with regard to collective moral responsibility. For the discussion of collective moral responsibilities involved in the prevention and preparation for chemical, biological, or radiological attacks, this chapter favors a multi-layered, individualist account of collective moral responsibility.

## 2. Can groups be held morally responsible?

In the history of philosophical thought spanning thousands of years, the discussion concerning issues of collective responsibility is rather young. While scholars debated issues and forms of individual responsibility since the beginning of philosophy itself, the question of whether a group of

persons can be causally and/or morally responsible for an action only found its way into the philosophical discourse in the early 20<sup>th</sup> century.

One of the first academics to investigate collective responsibility was Max Weber, who rejected the notion of collective responsibility and argued that a group, as opposed to its members, is not capable of forming own intentions and, hence, cannot perform actions rather only its members can act. Consequently, as Weber argues, groups cannot be held morally responsible, rather responsibility can only be attributed to their individual members (Mäkelä, 2013; Smiley, 2017). Other influential scholars in this field, like H. D. Lewis, rejected the idea that responsibility could be attributed to a group per se on similar grounds (Mäkelä, 2013). Both Weber and Lewis, but also other scholars like Karl Jaspers, rejected the possibility that a group as such can be held morally responsible for a specific action by arguing that a group cannot fulfill the requirements for moral agency (Jaspers, 1946).

According to the notion of moral agency, a moral agent can be morally praised or blamed for its actions. While some agents, such as cows or other animals, are not moral agents, human beings usually are. Various philosophers introduced different sets of defining conditions for moral agency. Some of these sets of conditions have found their way into recent discussions of joint actions (Mäkelä, 2013; Miller, 2006; Pettit, 2007). For example, Peter French characterizes a moral agent as someone who a) acts intentionally, b) is capable of making rational decisions, c) is responsive to (moral) criticism and events. Seumas Miller presents a similar list by claiming that an agent can be held morally responsible for an action if the agents intentionally and freely performed said action, the action is morally

significant, and the agent could foresee or at least know about the consequences of the action (Miller, 2006) (See also Pettit, 2007).<sup>58</sup>

Critics of collectivist accounts of collective moral responsibility such as Weber, Lewis, and Jaspers usually argue that groups per se do not fulfill one or more of these requirements of moral agency. Hence, they cannot be considered moral agents and, subsequently, cannot be praised or blamed for their actions (supposing they actually perform actions) or the consequences of their actions; nor can they be praised or blamed for the actions of their members or the consequences of these actions. Indeed, Weber and Lewis argued that a group as such is not capable of forming intentions and, hence, is not capable of performing an action; so it is not even an agent, let alone a moral agent (Lewis, 1948; Smiley, 2017; Weber, 1914).

However, while Weber and Lewis rejected the collectivist notion of collective responsibility, the growing societal complexities of the 20<sup>th</sup> century provided more and more examples of situations where a group or other collective entity seems to bear more moral responsibility for a particular action than the individuals who comprise the group or other collective entity in question (See e.g. Arendt, 1987). Institutions and corporations are only a few examples of collective entities that increasingly seemed to act as single entities rather than simply as an aggregation of the actions of their members. To many scholars, it seemed unfair to entirely blame, for example, each and every worker in a company for a horrendous accident that happens in said company, especially if it was not apparent if

---

<sup>58</sup> Pettit calls these conditions value relevance, value judgement, and value sensitivity (Pettit, 2007).

any particular individual agent can be held responsible at all for what happened. These exceptional cases in which no individual agent fulfills the requirements for moral responsibility, but seemingly the group does, is called the problem of many hands – a severe challenge to Weber’s and Lewis’s arguments (See for discussion van de Poel et al., 2015). Hence, philosophers and sociologists investigated the group as a potential bearer of collective moral responsibility more closely in the late 20<sup>th</sup> century and found a potential solution to the issues at hand: the collectivist account of collective moral responsibility.

### 3. The group as moral agent. Collectivist theories of collective moral responsibility

The reductionist account of collective moral responsibility that reduces the moral responsibility of collective entities to the aggregated responsibilities of the individual members of those entities clashed with the fact that moral responsibility, and certainly legal responsibility, was attributed to institutions, corporations, and other highly structured groups. Hence, some philosophers, including Peter French and Margaret Gilbert, favored another interpretation of collective moral responsibility that can be called the collectivist account of collective moral responsibility, according to which moral responsibility can, in fact, be attributed to collective entities as such.<sup>59</sup>

---

<sup>59</sup> The following description of these three collectivist accounts is based on the original works of the philosophers in question but also based on the discussions of their accounts in Miller (2001), Miller and Mäkelä (2005), and Sand (2018, chapter 6).

### 3.1. French's account

Peter A. French may be the most influential defender of a collectivist account of collective moral responsibility. In his book *Collective and Corporate Responsibility* (French, 1987) as well as in his article *The Corporation as a Moral Person* (French, 1979), he formulates a proposal to solve the above-described problems with the distribution of responsibility in groups by arguing that some collective entities comprised of individual human beings (e.g., corporations or institutions) are moral agents and, hence, can bear moral responsibility. Here it is important to note that, according to French, this responsibility of the group as a moral agent is independent of (possible) individual moral responsibilities of the individuals that are part of said group.

However, to assign moral responsibility to a group, French has to show that some (well structured) groups are, in fact, capable of forming a moral agent. Here French uses an account of agency that was introduced by Donald Davidson (French, 1979; Sand, 2018, p. 218). According to this account, a person classifies as an agent if this person performs a specific act intentionally. However, this agent becomes a moral agent in the sense of being morally responsible for said action if the agent is able to answer for her actions, i.e., is able to give reasons for her acting in a certain way. This answerability-approach to moral responsibility was initially introduced by Elizabeth Anscombe (French, 1979; Sand, 2018, p. 217).

In his paper on the corporation as a moral person, French argues specifically that corporations, institutions and other well-organized groups with

structured decision-making mechanisms ought to be called “full-fledged moral persons” (French, 1979, p. 207) according to the criteria discussed above. Here it is important to note that French does not only ascribe *legal* personhood to these kinds of groups but goes further by arguing that these groups are agents that are also capable of answering for their morally relevant actions (French, 1979; Sand, 2018, p. 216). Hence, French concludes that collective moral responsibility (understood in this collectivist sense) can be assigned to the corporation (or other well-structured groups) directly since this group is a moral agent.

### 3.2. Gilbert’s account

In her article *Who’s to Blame? Collective Moral Responsibility and Its Implications for Group members* (Gilbert, 2006), Margaret Gilbert defends an account of collective moral responsibility that, similar to French’s account, includes the argument that one can describe certain groups as moral persons in some way.

In the article, Gilbert argues that certain collectives (well-structured groups like institutions or corporations) can be seen as bearers of moral responsibility since they fulfill the conditions for being what Gilbert calls blameworthy “plural subjects” (Gilbert, 2006, pp. 98–102). In the first part of her article, Gilbert argues that a well-structured group can develop both joint commitments towards a (morally relevant) cause and is also able to form collective intentions and act upon these intentions. Furthermore, Gilbert shows that these groups are able to have collective beliefs and collective knowledge (Gilbert, 2006, pp. 104–108). Lastly, she argues that

the ‘doings’ of groups such as institutions and NGOs also satisfy the requirement of being freely performed actions.<sup>60</sup> Gilbert concludes that certain groups can be characterized as plural subjects that are blameworthy (or possess answerability) – blameworthiness being a necessary condition for moral responsibility (Gilbert, 2006, pp. 96–98).

An important element in Gilbert’s argument is the conditions for membership in a group (or plural subject). In the second part of her article, Gilbert argues that in order to be a member of a plural subject, an individual does not have to be an active part of the morally significant collective action in question. Hence, being born into a certain group is a sufficient condition for being part of the plural subject that this group constitutes and, hence, for taking part in the joint commitment of the group (Gilbert, 2006, pp. 109–114; Miller & Mäkelä, 2005, p. 640). However, Gilbert also emphasizes that individual members who did not partake in a morally significant action of the plural subject cannot be blameworthy for the group’s action. Gilbert offers this argument to distinguish between collective and individual moral responsibility within the same plural subject (Gilbert, 2006, p. 109).

---

<sup>60</sup> In a similar fashion to French and Gilbert, Philip Pettit argues in his article *Responsibility Incorporated* (Pettit, 2007) that certain, well-organized groups qualify to be moral agents and, thereby, bearers of moral responsibility. According to Pettit, certain well-structured groups (like institutions) are capable of displaying a decision making process involving with their own reasoning of their own, i.e., these reason-based decisions are not merely being an mere aggregation of individual, reasoned decision making processes of the group’s members (Miller & Mäkelä, 2005, p. 646; Pettit, 2007). In order to support this claim, Pettit introduces several thought experiments of which the so-called discursive dilemma is the most well-known.

#### 4. The individualist account of collective moral responsibility

Several authors identified problems with the collectivist view that moral responsibility could be assigned to groups per se (Mäkelä, 2013; Miller, 2006; Miller & Mäkelä, 2005; Sand, 2018). For example, with regard to Gilbert's notion of plural subjects, Miller and Mäkelä note that this notion is either referring to a somewhat mysterious group agent or is simply reducible to individual agents and their respective individual responsibilities (Miller & Mäkelä, 2005). There is also the problem of proliferation of moral agents in every club, business company, school, police force, council, bureaucracy. Can these entities really be agents with a mind and a moral sense? Then there is the problem of explaining the relationship between these collectivist 'minds' and the minds (intentions, beliefs, etc.) of their human members. These issues with the collectivist accounts of collective moral responsibility led researchers like Seumas Miller and Pekka Mäkelä to reject this interpretation of collective moral responsibility and to propose own accounts of this phenomenon. For the present discussion, especially Miller's view that is expressed in his article *Collective Moral Responsibility: An Individualist Account* (Miller, 2006) is relevant. On this account, if it works, recourse to mysterious collective minds is unnecessary.

In his article, Miller defends an account of collective moral responsibility that rejects the notion favored by French and Gilbert that collectives and groups can be characterized as moral agents and, hence, bearers of moral responsibility. Accordingly, any linguistic expressions such as "BP is morally responsible for the oil disaster" are simply shorthand ways of ascribing moral responsibility to the relevant BP managers. However,



Miller also explicitly dismisses Lewis's and Jasper's reductionist view of collective moral responsibility, according to which collective responsibility is nothing more than an aggregation of the individual responsibilities of the persons that constitute a certain collective or group (Miller, 2006, p. 176). Instead, Miller defends an account of collective moral responsibility that is based on his analysis of joint actions. On Miller's account, collective responsibility is joint responsibility. Each participant in a joint action performs his or her individual action interdependently with the actions of the others, and in doing so each participant has the same end as the others, i.e., there is a collective end in Miller's parlance (Miller, 2006, pp. 177–178).

In the first part of his article, Miller distinguishes between different types of responsibility and separates issues of individual responsibility from issues of collective responsibility as well as mere causal responsibility from moral responsibility. Miller also introduces the concept of institutional responsibility that refers to specific duties and obligations that are constitutive of specific institutional roles. Here it is important to note that institutional responsibility and moral responsibility might conflict in certain situations and should be seen as two different kinds of (individual and collective) responsibility (Miller, 2006, p. 178). Miller's view is essentially that collective responsibility is a "species" of joint responsibility.

In detail, Miller describes the "action" of a group as a joint endeavor in which each and every member of the group performs an individual action that contributes to what Miller calls the collective end of the group. This collective end is the joint goal of all group members and is to be achieved in

performing the joint action. In aiming at this collective end, every agent involved in the joint action performs his or her action in order to realize this end and in the belief that the other agents involved are also performing their individual contributory actions. Hence, a joint action can be described as a set of interdependent, individual actions that are performed to realize a collective end. Based on this account of joint action, collective responsibility is a responsibility that is shared between the agents involved in the joint action in question: every single agent is individually responsible for their contributory, individual action to realize the collective end, but in virtue of aiming at this collective and performing these individual actions in the belief that the other agents will do the same, every agent involved in the joint action is jointly responsible for realizing the collective end— in addition to being individually responsible for their contributory action.

With regard to this individualist account of responsibility, it is essential to note that, to be jointly responsible for a specific (joint) action, an agent involved in the joint action does not have to perform a contributory action that is *causally necessary* for realizing the collective end. Here Miller uses the example of multiple persons stabbing a man to death (Miller, 2006, pp. 179–181). Each of the persons stabs this man only one time, and none of the stabs are sufficient to kill the man. However, the sum of the stabs kills the man eventually. Hence, no member of the group performs an action or even set of actions that is causally necessary or sufficient for the death of the person. However, each makes a causal contribution to the person's death and does so having the person's death as a shared end.

Moreover, killing is obviously a morally significant action. Thus the members of the group are jointly morally responsible for his death. Furthermore, on Miller's account, while being jointly (i.e., collectively) morally responsible for killing the man in question, each and every member of the group is also individually morally responsible (not only for his or her acts of stabbing) but also for the death of said man since each and every one made a causal contribution, performed their individual actions in interdependence with the actions of the others, and did so in order to fulfill the collective end of stabbing the man to death. Miller also notes that in the case of large-scale joint actions each contributor might not be *fully* morally responsible for the realization of the collective end.<sup>61</sup>

With this proposed, individualist account of collective moral responsibility as joint responsibility, Miller manages to assign collective moral responsibility to the members of groups without running into the problems that other individualist accounts in terms of aggregation face, while simultaneously avoiding the difficulties besetting collectivist interpretations.

## 5. Multi-layered collective moral responsibility and joint mechanisms in institutions, corporations, and other complex groups

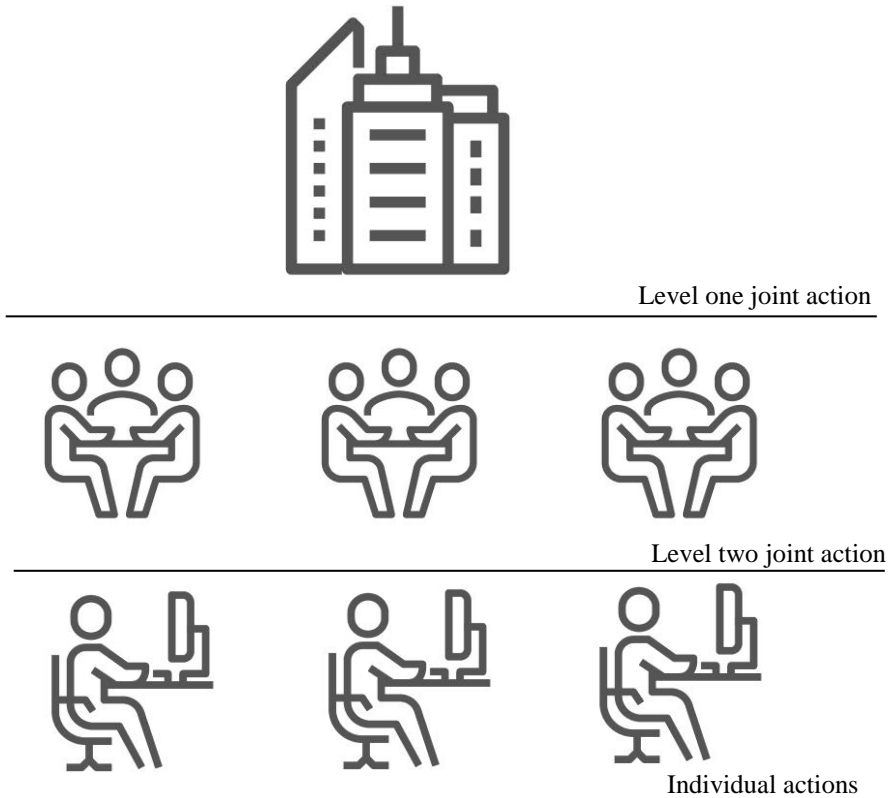
So far, we have only seen the advantages of Miller's individualist account of collective moral responsibility with regard to rather simple actions

---

<sup>61</sup> In connection to this argument, Miller also notes that there might be persons who merely assist to fulfil the collective end (e.g. by selling the stabbers the knives) and, hence, bear diminished moral responsibility for the death of the man on an individual level while still being jointly responsible for his death (Miller, 2006, pp. 179–183).

performed by small, non-hierarchical groups. However, as French and Gilbert have shown, a lot of the issues with collective moral responsibility occur in complex, hierarchical groups of individuals such as corporations, institutions, NGOs or governments.

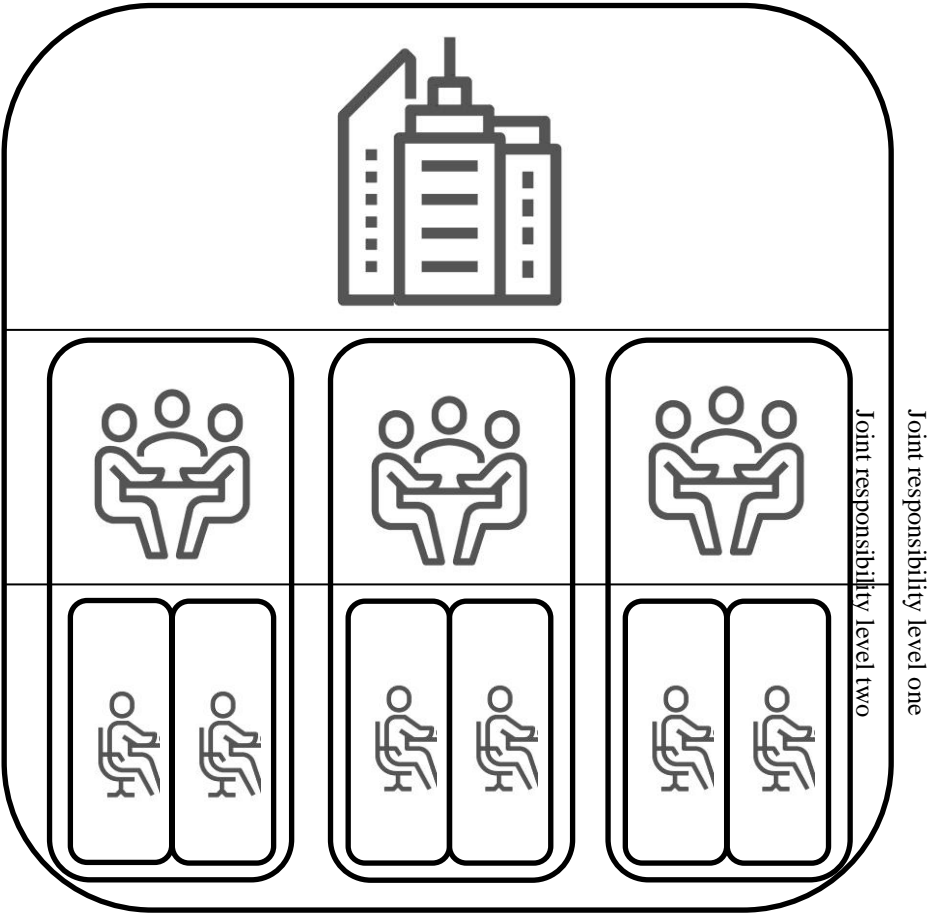
With regard to joint actions performed in more complex, hierarchical groups, Miller shows that joint actions can consist of multiple levels of individual actions and he introduces the concept of joint mechanisms to accommodate institutional procedures of various kinds, such as voting. First of all, Miller notes that a joint action might consist of multiple levels of individual and joint actions in order to realize a collective end. Specifically, it is easily imaginable that, for example, in order to prevent a terrorist attack (collective end), a security institution performs a joint action that itself consists of three joint actions of employees of three departments of said institution. Hence, each employee performs an individual action in order to contribute to the joint action of his or her department. This joint action, in turn, is (jointly with the actions of the two other departments) a single action in the joint action of the security institution to prevent the attack. In connection with these multiple layers of joint actions, Miller speaks of level one and level two joint actions. These multi-layered joint actions can be visualized as follows:



*Fig. 4: Multi-layered joint action*

In this diagram, there are six individual actions, three single level two actions (each of which is a joint action comprised of two individual actions), and one level one joint action (comprised of three single actions, each of which is a level two joint action). Crucially, at bottom, the level one joint action ultimately consists in the six individual actions, albeit the collective end of the level one joint action is different from the collective ends of the level two joint actions (which also consist of the six individual actions). In accordance with this model of multi-layered joint actions, collective moral responsibility (understood as a species of joint responsibility) can be applied in a multi-layered manner. Miller shows that it is, at least in principle,

possible to assign joint moral responsibility for the realization of the collective end on level one to the individuals performing the individual actions contributing to the level two joint actions. Hence, each employee of the security institution is jointly morally (and in this case, institutionally) responsible for realizing the collective end of the institution, i.e., preventing a terrorist attack. This multi-layered collective moral responsibility manifests as follows:



*Fig 5: Multi-layered joint (moral and institutional) responsibility*

It is important to note that each contributing individual agent in this structure may not be fully morally responsible for the level one collective end; each may only be partially morally responsible or, in the case of hierarchical structures, may have diminished moral responsibility.

In addition to such multi-layered joint actions, Miller also introduces the notion of joint institutional mechanisms to accommodate procedures such as voting, which are not simply joint actions or multi-layered structures of joint actions. According to Miller, a joint mechanism is to be distinguished from a joint action in that whereas joint mechanisms have individual actions as an input and these actions are directed to a collective end, joint mechanisms (but not mere joint actions) also deliver a result of these actions by virtue in part of the mechanism itself and this result may not be a collective end (Miller, 2006, p. 185).

One example of a joint institutional mechanism that Miller provides in his paper is the process of deciding to raise taxes in a parliamentary cabinet (Miller, 2006, p. 186). In this example, the individual actions of casting a vote whether or not to raise taxes by each cabinet member are the input of the institutional mechanism and the decision to raise taxes (or not) is the output. The joint institutional mechanism itself is the conventions and terms of voting in the Cabinet. Hence, each and every Cabinet member who provides input (individual action) into the joint mechanism can be seen as jointly institutionally responsible for the outcome of the vote – even if said outcome is not what the individual Cabinet member voted for.

However, Miller goes even further than this and argues that each and every Cabinet member who casts a vote is not only jointly institutionally but also jointly morally responsible for the outcome regardless if the outcome of the vote resembles the individual vote of the member. By virtue of accepting the joint institutional mechanism of voting in the Cabinet (that entails the obligation to accept what the majority of Cabinet members voted for), each and every member is jointly morally responsible for raising the taxes or not. Of course, one might be able to exclude oneself from this joint moral responsibility by rejecting the joint institutional mechanism altogether, e.g., by resigning from the Cabinet.<sup>62</sup>

However, while joint mechanisms *within* institutions (such as counter-terrorism agencies) help to close moral responsibility gaps by virtue of formulating clear (collective) institutional responsibilities for the members of these institutions, joint actions in which these institutions cooperate with other groups of agents (such as corporations, research institutions and different groups of citizens) pose additional problems. Yet, these cooperative, joint actions that involve multiple groups of stakeholders are needed to prevent a terrorist attack using toxins as weapons successfully. In order to identify the different layers of (joint) moral responsibilities involved, the concept of the web of prevention is needed and, therefore, is the subject of the next chapter of this dissertation. The web of prevention will be discussed together with the identification of the most relevant

---

<sup>62</sup> With his account of institutional mechanisms, Miller evidently found a way to solve Pettit's discursive dilemma and, therefore, shows that even decision making processes in very well structured and organised groups can be explained without using a collectivist interpretation of collective responsibility.



stakeholders involved in preventing and preparing for terrorist attacks using toxic substances as weapons.

## **5. Critical stakeholders in the fight against attacks using common-use toxins**

### **1. Introduction**

Due to the danger that the three selected substances, as well as other toxic substances, pose, security institutions, as well as other relevant groups of stakeholders, introduced a variety of measures to combat their illegal use by terrorists (and others). In order to identify the most relevant measures and stakeholders that are (or ought to be) involved in the fight against this branch of terrorism, this chapter will introduce the theoretical concept of the web of prevention. It will be shown that the fight against the use of toxins by terrorists can be described as a multi-faceted web of measures that are jointly performed by a set of stakeholders. In the second part of this chapter, the most relevant groups of stakeholders in the fight against the terrorist use of toxic and radiological substances are identified.

Specifically, it will be shown that, in addition to security institutions, manufacturers and vendors of products that contain ricin, phosphine, or americium ought to be part of the web of prevention. Furthermore, the press, researchers, internet users, and citizens will be identified as relevant groups of stakeholders in this web. For reasons of brevity, the counter-terrorism infrastructure of Germany was chosen as an example of the critical institutional component of the web of prevention. However, Germany's

security architecture – in which the Joint Counterterrorism Centre (GTAZ) is the counter-terrorism hub - roughly resembles the institutional architecture of other liberal democracies, including the USA (with its Fusion Centers), the UK (with its JTAC), the Netherlands (NCTV) or Belgium (CUTA) (Van Der Veer et al., 2019).

## 2. The web of prevention and CBRN terrorism

The concept of the so-called “web of prevention” is based on the notion of collective action and joint responsibility and was initially introduced in the domain of biosecurity. The concept was originally mentioned in an initiative of the International Committee of the Red Cross (ICRC) on biotechnology and security in 2002 (Rappert & McLeish, 2012, p. 4; Selgelid & Rappert, 2013, p. 277). Yet, similar concepts, such as the web of deterrence, date back to debates of non-proliferation and biosecurity during the Cold War (Rappert & McLeish, 2012, pp. 3–4).

In the context of biosecurity, the concept of the web of prevention describes an “integrative and comprehensive approach” (Whitby et al., 2015, Chapter 7) to prevent the malicious use of biotechnology for weapon purposes. The web includes a variety of different stakeholders such as national security institutions, international organizations as well as research institutions. These groups of stakeholders are jointly responsible for implementing measures such as export controls, disease detection and prevention, effective threat intelligence, international and national prohibitions, oversight of research, and biosecurity education (Bezuidenhout, 2012, p. 20; Selgelid &

Rappert, 2013, p. 277; Whitby et al., 2015, fig. 7.2). In promoting a multi-faceted web of measures to prevent the malicious use of novel innovations in biotechnology, the concept of the web of prevention quickly gained significant relevance in the academic debate on dual-use research and development.<sup>63</sup> In this debate, the roles and responsibilities of research institutions and individual scientists within the web of prevention are stressed. As, for example, Seumas Miller has shown, the notion of the web of prevention can be seen as an application of the concept of joint actions and collective moral responsibility (See Miller, 2018). All stakeholder groups within the web of prevention in question are jointly responsible for the common goal of preventing the production and use of biological weapons. Yet, each stakeholder group performs individual actions and has individual responsibilities in order to fulfill that common goal (Miller & Feltes, 2018, pp. 65–71). However, each of these “individual” or, better, single institutional actions are themselves joint actions comprised of the individual actions of the members of the institution in question (see discussion above).

Yet, the concept of the web of prevention has not been exclusively used in this specific context. Security researchers outside of the dual-use debate referred to this concept and stressed the importance of an extensive set of stakeholders taking a multi-faceted web of counter-measures against terrorist threats. For example, James Revill proposes a “web of IED prevention” in order to combat the threat of terrorist attacks using improvised explosive devices (Revill, 2016, p. 93). By parity of reasoning, I

---

<sup>63</sup> For a discussion of the dual-use debate, see section 3.2 of this chapter.

propose to deploy the concept of the web of prevention in order to analyze and improve the measures against the terrorist use of ricin, phosphine, and americium. This specific web of prevention ought to include, at least, three groups of counter-measures: (1) measures to deny terrorists access to these substances, (2) measures to prevent the distribution of expertise that can be used to manufacture weapons with these substances, and (3) measures that are aimed at resilience and recovery in the aftermath of an attack with these substances. Furthermore, and in accordance with the original idea of the concept, the web of prevention against terrorist attacks using common use toxins includes a variety of stakeholders. Each of these stakeholder groups possesses certain moral obligations in the fight against terrorist attacks using common use toxins and all groups (and, therefore, ultimately, the members of these groups) are jointly responsible for preventing and preparing for such attacks.

### 3. Essential stakeholders in the web of prevention against terrorist attacks using common use toxins

#### 3.1 The government<sup>64</sup>

The institutional counter-terrorism architecture in Germany includes a large variety of agencies and actors. In order to improve the communication and cooperation between these actors, a Joint Counter-Terrorism Centre (*Gemeinsames Terrorismusabwehrzentrum* (GTAZ)) was established in

---

<sup>64</sup> A short version of this section was published on the website [counterterrorismethics.com](http://counterterrorismethics.com) by the author and Paul Burke (Burke & Feltes, 2017).

2004 that provides a mechanism for the cooperation of 40 different agencies involved in German national security with regard to international Islamist terrorism (Bundesamt fuer Verfassungsschutz, 2017). Similar centers were also established to deal with domestic terrorism (e.g., *the Gemeinsame Extremismus- und Terrorismusabwehrzentrum* (GETZ)). The GTAZ is not an independent institution; rather, it acts as a platform to facilitate direct communication between a range of actors in the German counter-terrorism apparatus. These actors include the following:

#### The Federal Police (*Bundespolizei*)

As a crucial part of Germany's executive power, the Police are deeply involved in counter-terrorism activities as a matter of necessity. Alongside the regular Police forces, this institution also commands two very specialized counter-terrorism units: the *Grenzschutzgruppe 9 der Bundespolizei* (GSG9) and the BFE+ (Bundespolizei, 2017a; Pabst, 2015). The GSG9 unit was established by the German Federal Border Guard (*Bundesgrenzschutz*) in 1972 as a direct reaction to the attack during the Olympic Games in Munich, and it specialized in responding to hostage situations and terrorist attacks. In 2005 the GSG9 was transferred from the command of the Federal Border Guard to the Federal Police. The BFE+ was founded in 2015 and it was designed to complement the work of GSG9. The members of the BFE+ undergo a special training regime to respond to large-scale terrorist incidents and suicide bombings such as the attacks in Brussels and Paris (Bundespolizei, 2017a, 2017b; Pabst, 2015).

### The Federal Criminal Police Office (*Bundeskriminalamt* (BKA))

The BKA is, amongst other things, responsible for coordinating police investigations in all states of the Federal Republic of Germany, and it has a dedicated section, Division ST (or “State Security” (*Staatsschutz*)), which combats domestic and international terrorism.

### The Criminal Police Offices of the Federal States (*Landeskriminalämter* (LKA))

The LKAs of Germany’s 16 Federal states report to the State Ministers of the Interior and are concerned with severe criminal and terrorist activities in the respective states. The LKAs are involved in the investigation of those criminal offenses and groups that spread across the borders of major cities and also across regions. Like the BKA, each LKA also has a section specialized in politically motivated crimes including terrorism.

### Federal Domestic Intelligence Service (*Bundesamt für Verfassungsschutz* (BfV))

As the primary Intelligence agency for interior matters in Germany, the BfV focuses on security risks and threats within Germany. It collects Intelligence on domestic and international terrorist threats as well as economic and political espionage, and religious extremism (Bundesamt für Verfassungsschutz, 2017c). Another important task of the BfV is the reporting on, and education of, domestic German society and government about radicalization, extremism, and terrorism. In doing so, one of the main functions of the BfV is to coordinate the Intelligence gathered, and the

associated work conducted by the 16 state-level, domestic Intelligence services of the Federal Republic of Germany (Bundesamt für Verfassungsschutz, 2017c, 2017a).

The 16 State Domestic Intelligence Services (*Landesämter für Verfassungsschutz* (LfV))

The LfVs of Germany's 16 Federal states gather Intelligence and inform the public, as well as the state Governments (especially the State Minister of the Interior), about terrorist groups and plots, and about political and religious extremism in general. Additionally, each LfV reports to the BfV, and shares Intelligence with it. As with the BfV, the LfVs do not have any executive power.

Federal Intelligence Service (*Bundesnachrichtendienst* (BND))

Just like the BfV and the LfVs, the BND gathers Intelligence concerning possible terrorist activities, threats to German national security, areas of conflict, and espionage. In contrast to the domestic Intelligence services, however, the BND focuses on international and global issues and operates outside of the German borders. One of the core themes of the BND is the fight against global Islamist terrorism in terms of acquiring information about the activities of transnational and global Islamist networks (Bundesnachrichtendienst, 2017).



### Military Counter-Intelligence Agency and the Military (*Militärischer Abschirmdienst (MAD) und Bundeswehr*)

The MAD is part of the German Armed Forces (*Bundeswehr*) and ensures the security of German troops, whether in Germany and abroad. The work of the MAD focuses on military espionage and communication security during operations, but the agency also gathers intelligence concerning extremism and terrorist threats within or against the *Bundeswehr*. In contrast to the BND, the work of the MAD is bound to those regions in which the *Bundeswehr* is currently present and active (Militärischer Abschirmdienst (MAD), 2017).

Although not part of the G7, the *Bundeswehr* is also a vital part of the German counter-terrorism architecture. Since the German Constitution prohibits the *Bundeswehr* from being deployed within the borders of Germany (unless in a state of national emergency<sup>65</sup>), its main contribution in CT is restricted to the support of NATO troops and other coalition forces, in regions which are subjected to the activities of international terrorist networks such as Al Qaeda and ISIL (Auswärtiges Amt, 2017; Bundeswehr, 2017).

### Central Office of the German Customs Investigation Service (*Zollkriminalamt (ZKA)*)

The ZKA investigates all criminal activities that impact on Germany's border security. The ZKA is involved in a wide range of activities, including

---

<sup>65</sup> § 87a IV *Grundgesetz* (GG).

counter-narcotics work, anti-money laundering (AML), counter-espionage and the fight against the proliferation of chemical, biological, radiological, and nuclear agents (CBRN). The ZKA also cooperates with and coordinates the work of the regional Customs Investigation Offices in Germany (BUND.DE, 2017).

Federal Office for Migration and Refugees (*Bundesamt für Migration und Flüchtlinge* (BAMF))

The BAMF coordinates the work on migration and refugees in the Federal Republic of Germany. Along with responsibilities such as organizing refugee housing, monitoring refugee movements, and analyzing the varying causes of migration, Group 23 of Section 2 of the BAMF is also concerned with the security issues related to migration. In this area, Department 235 works on the issues of preventing radicalization, and also on national security matters related to migration and refugee matters (Bundesamt für Migration und Flüchtlinge, 2017).

Federal Public Prosecutor General (*Generalbundesanwalt* (GBA))

The Federal Public Prosecutor General represents the Government in the Federal Court of Justice in Karlsruhe. In addition to this general responsibility, the Federal Public Prosecutor General possesses jurisdiction over cases of terrorism, or severe crimes against the constitution or Government, in Germany.

With the GTAZ as a central platform, these 40 institutions are able to communicate on an equal level without rigorous bureaucratic constraints

and can share relevant information and Intelligence concerning Islamist terrorism in Germany. Together with this equitable communications framework, the GTAZ also provides two intelligence analysis units as well as eight other working groups to the strategic communications process described above. The two analysis units of the GTAZ are the Intelligence Information and Analysis Unit (*Nachrichtendienstliche Informations- und Analysestelle* (NIAS)) and the Police Information and Analysis Unit (*Nachrichtendienstliche Informations- und Analysestelle* (PIAS)). The NIAS consists of representatives of the BfV, the LfVs, the MAD, and the BND, while the members of PIAS represent the BKA, the LKAs, the GBA, and the Federal Police (Bundesamt fuer Verfassungsschutz, 2017).

Independent of their membership in one of these analysis units, the members of the GTAZ are also part of eight working groups that are concerned with a range of support activities, including the following: daily briefings; threat assessment; operational information exchange; Islamist terrorism-related cases; individuals from the Islamist-terrorist spectrum; de-radicalization; transnational aspects; accompanying measures concerning the legal residence status of individuals. In addition, members of the NIAS form an Intelligence Board within the GTAZ (Bundesamt fuer Verfassungsschutz, 2017). Finally, the BfV, the BKA, the BND, the MAD and the Federal Public Prosecutor General all work together in the Joint Internet Centre (*Gemeinsames Internetzentrum* (GIZ)) that is based outside of the GTAZ but is also exclusively concerned with issues of Islamist extremism and thus cooperates closely with the GTAZ (Bundesamt für Verfassungsschutz, 2017b).

### 3.2 Companies, citizens, and other relevant stakeholders

Next to the architecture of governmental security institutions in a liberal democracy, other groups of actors have to be mentioned with regard to counter-terrorism measures against attacks using common use toxins. These groups are not institutional parts of a country's security infrastructure but have the potential to contribute valuable insights and put in place measures in the fight against terrorist groups using toxins. In fact, many of the groups that will be discussed below, and other actors that will not be discussed in this section, are already partaking in general counter-terrorism measures in many Western liberal democracies in some capacity. Yet, in this section, the role of a set of selected groups with regard to those counter-terrorism measures aimed at terrorist attacks using common use toxins will be central.

#### Manufacturers

One essential group of actors that is relevant to countering terrorism using toxins as weapons is the group of companies and private endeavors that manufacture toxic substances. Manufacturers of toxic and radiological substances such as phosphine and americium-based devices can be of great value to security institutions since these companies both have in-depth knowledge about these substances and function as distribution centers of these products and relevant information to vendors and other professional customers. Furthermore, the manufacturers of toxic substances are able to actively influence further innovations in the field of substances like phosphine or with regard to products such as ionizing smoke detectors. That

offers security agencies the chance to cooperate with manufacturers in order to incorporate security considerations into the design process of products.

### Vendors

The group of companies and private organizations that sell toxic substances, or products that contain those substances, is also highly relevant to counter-terrorism efforts. Vendors and their online shops or physical stores are the primary sources for the acquisition of toxic substances such as ricin, phosphine, or americium. Hardware stores, gardening suppliers, and farmer's supply markets offer products that contain these substances or, at least, precursors of these substances. Hence, employees of vendors of toxic substances might be in direct contact with potential terrorists. This unique role of vendors is, for obvious reasons, of interest to security institutions. Functional cooperation between vendors and these institutions could possibly deny terrorists access to a large variety of dangerous substances and, thereby, contribute to the prevention of attacks.

### The press

As already discussed in this thesis at length, publicity is a critical component of terrorist actions. Hence, publishing companies and, in particular, the news media ought to be part of a functioning web of prevention aimed at the terrorist threat. In particular, the soft damage (i.e., anxiety, political damage, etc.) inflicted by a terrorist attack requires publicity and media reporting of the death and destruction caused by the terrorist attack if news of the latter is to reach the target audience. Multiple researchers have discussed at length the role of the press in terrorism

(Ayish, 2014; Mythen & Walklate, 2006; Weimann, 2008).

As one of the critical characteristics of attacks using all three substances (ricin, phosphine, and americium) is the enormous extent of soft damage that they are able to inflict, the corresponding web of prevention necessarily has to include media outlets. For only if the press is aware of its capacity to either strengthen or diminish the soft damage caused by a toxin attack, can the impact of these attacks be contained. Note that the role of the press in the web of prevention is predominantly focused on diminishing the impact of an attack *after* it has happened. Chapters 6 as well as the last section of this thesis will further explore this role and the ethical implications of this role.

#### Internet Users and social media companies

As citizens of a society, we can occupy a variety of roles that are relevant to combatting CBRN terrorism. For example, some citizens might work in a hardware store and, thereby, occupy the roles of vendors in the web of prevention against terrorism using toxins. Another role that is relevant to the web of prevention is occupied by most citizens in a Western democracy; that is, the role of being an internet user. In 2017, roughly 87% percent of all European households had at least one internet connection (D. Schmid, 2018). Hence, and unlike the role of being a vendor or media representative, the role of the internet user is one occupied by the majority of individuals in society.

It was shown in chapter 3 of this thesis that the expertise to manufacture toxic and radiological weapons for terrorist purposes can be acquired via the

internet without a significant risk of detection or arrest. Hence, the “space” occupied by online activities is important in the preparation of a terrorist attack using toxic or radiological devices. This space, however, is particularly difficult for security institutions to police and monitor. In this regard, the joint efforts of all internet users and social media providers, guided by security officials, may be essential to detect and flag illegal online behavior efficiently. Chapter 10 of this thesis will outline such an approach.

The internet and social media also have a crucial role to play in post-incident communication and recovery following an attack. As Alastair Reed and Haroro Ingram have shown, social media and its users have the potential to assist emergency services, to inform the public, and to bring communities together in the aftermath of a terrorist attack (Reed & Ingram, 2019).

### Researchers

As the analysis in chapters 2 and 3 of this thesis showed, the fight against terrorist attacks using toxic and radiological weapons involves threat assessments and the identification of new threats. Academic researchers are needed to identify and assess these threats in a structured manner. Furthermore, these researchers can also provide security analysts with novel frameworks to analyze the impact of terrorist innovation. Important here is the ability to understand and even predict the largely non-quantifiable harms resulting from a terrorist attack, such as soft damage. Finally, academic researchers analyze current policies regarding, and measures taken to combat, terrorist attacks and, thus, are able to provide policymakers with

valuable advice on how to optimize current counter-terrorism infrastructures. Due to this critical role, academic researchers ought to be part of the web of prevention against terrorists using toxins.

There is a second dimension to the involvement of academic researchers and scientists in a web of prevention against terrorism. Researchers in the field of biological sciences, chemistry, and physics have access to information and materials that are of high interest to potential perpetrators of toxic or radiological attacks. Furthermore, new research outcomes and novel developments in these fields might (although intended to help society) be used by malicious users (such as terrorists) to design novel weapon types. This pivotal role of scientists in CBRN security and counter-terrorism is commonly known as the dilemma of dual-use research and development (Miller, 2018).

However, the moral obligations of scientists engaged in dual-use research will not be a focus of this thesis. First of all, the three substances that are discussed in the present analysis are commonly used chemicals in openly available consumer products. Hence, the debate around the dual-use consideration of novel innovations at universities does not cover these substances. Secondly, the moral obligations of scientists have already been discussed in a large variety of publications from multiple perspectives (Ehni, 2008; N. G. Evans, 2014; Kuhlau et al., 2008; Miller, 2018; Miller & Selgelid, 2007). By contrast, the roles and responsibilities of other stakeholders in the web of prevention, such as vendors, are absent from current debates. These, to this date rarely discussed, stakeholders shall be the focus of this study. Yet, the discussion concerning the moral obligations



of these stakeholder groups will use certain elements and concepts employed in the dual-use debate. Hence, I will discuss selective arguments of this academic debate at several points in this thesis in the context of arguing for the moral obligations of manufacturers, vendors, press representatives, internet users, and citizens in the web of prevention.

### Citizens

The largest group that ought to participate in the web of prevention is the public. As both targets and potential witnesses of terrorist activities, citizens of a society ought to contribute to the joint measures to counter these activities. However, the indiscriminate recruitment of citizens in order to participate in measures to prevent terrorist attacks using toxic and radiological weapons might not be an efficacious and ethically sustainable way to involve citizens in the web of prevention.

Instead, and based on existing research, it will be argued that the most appropriate and efficacious actions of citizens in the web of prevention are focused on awareness of and preparation for toxic and radiological attacks (Gouweloos et al., 2014; Pearce et al., 2013; Rogers et al., 2013; Spencer et al., 2012). As will be shown later on, these measures can both reduce the extent of the soft damage inflicted by these attacks and assist in the creation of the web of preparation to ensure resilience in the aftermath of an attack. For only if most people in society understand the mechanisms behind the soft damage caused by attacks using ricin, phosphine, and americium, can this damage can be reduced to a minimum and, thereby, render these attacks close to ineffective.

## **6. Moral obligations and counter-measures in the web of prevention**

### **1. Introduction**

In the last chapter, I identified the most important groups of stakeholders that ought to collaborate to prevent and prepare for attacks with ricin, phosphine, and americium. In this chapter, it will be shown that each of these groups possesses a specific moral obligation to be part of the web of prevention. On the basis of these obligations, each group of stakeholders is responsible for undertaking specific measures within this web.

However, it has to be noted that the moral obligations in question are different for different kinds of groups. Security institutions, such as the police, intelligence agencies and the military, possess a moral and institutional responsibility to combat terrorism in general and, therefore, prevent terrorist attacks using toxins. This moral responsibility of theirs is also their institutional responsibility and is grounded in their overarching institutional and moral purpose, namely, to provide security.

However, the moral obligations of other institutional actors, such as manufacturers of toxic substances or members of the press, are less clear-cut and not necessarily constitutive of these actors qua institutions. *Prima facie*, for example, it is not the institutional role of journalists to provide security. Accordingly, the moral responsibilities of these institutional actors in

relation to the prevention or mitigation of terrorist attacks using toxins may have to be justified by recourse to moral principles or moral purposes that might otherwise be somewhat tangential to these institutional actors or, perhaps, not specific to them, e.g., the moral principle to prevent harm if one can do so and at little cost to oneself.

In this chapter, the No Means To Harm (NMH) principle is introduced and this principle will be used to display how many groups of stakeholders are morally obliged to participate in the web of prevention and have specific morally required roles within the web. The reason that the members of these particular groups, in particular, are morally obligated to participate in the web is that the members of these groups provide terrorists with the means to conduct an attack using ricin, phosphine, and americium. In short, the moral principle, NMH, generates moral obligations on the part of the members of certain institutional actors to participate in the web of prevention, e.g., by taking measures to reduce the likelihood that toxins get into the hands of terrorists in the first place.

## 2. The NMH principle

The moral and institutional responsibility of governments and their security institutions to participate in the web of prevention against terrorist attacks is obvious since the physical security of the citizenry is a fundamental institutional role of governments and their security agencies. Yet, the moral responsibilities of other stakeholder groups in this web, such as vendors or internet users, are less obvious and stand in need of justification. In contrast

to the security agencies, it is not self-evident that stakeholders outside of a nation's security infrastructure are morally obligated to get involved in counter-terrorism measures. Hence, the role of each stakeholder group in the web of prevention has to be morally justified, and specific moral responsibilities and actions have to be derived from that role.

In order to do so, however, a moral framework is needed that is broad enough to apply to a wide variety of stakeholder groups and narrow enough to function as a basis to derive different roles and responsibilities for different groups within the web of prevention. Here, a moral framework that was introduced by Seumas Miller in connection to the dual-use debate is an excellent candidate to fulfill this task. In the discussion around dual-use research, Miller and others argue that researchers and research institutions possess a moral obligation to consider the possible harms that might arise from their research if used by others. This obligation is based on what Miller calls the No Means To Harm (NMH) principle (Miller, 2013, pp. 187–188, 2018, pp. 12–14).

According to this principle, one ought not to, foreseeably or avoidably, provide others, directly or indirectly, with means to do an extensive amount of serious harm. In connection with the dual-use issues in research, Miller formulates four criteria for the application of the NMH principle. First of all, the means in question can, in fact, be used for harmful purposes of some kind. Secondly, there has to be a danger that others are interested in using these means to create harm. Thirdly, the harm that might be inflicted through these means is of “great magnitude,” as Miller puts it. Finally, Miller stresses that the principle may apply to members of a group, and even

if the means in question is only indirectly provided by members of the group in question to those who do the harm (Miller, 2018, p. 13), e.g., a manufacturer might sell a toxin to a distributor whom the manufacturer knows has ties to a terrorist group.

In the service of constructing a web of prevention against the terrorist use of ricin, phosphine, and americium, we need to identify stakeholder groups to which the NMH principle relevantly applies. Specifically, to which groups are the criteria of the NMH principle applicable? As shown in chapter 3, all three substances have the potential to be used to do great harm. Furthermore, it was argued that Islamist and right-wing terrorist cells had displayed an interest in using these substances to do great harm to individuals and societies.

The discussion in chapters 2 and 3 concerning the grave risks of *soft damage* (such as anxiety, erosion of trust, etc.), in particular, posed by these substances should they get into the hands of terrorists demonstrates the grave risk they pose of a *high magnitude of harm*. So the harm in question might not be of physical nature but rather of a psychological and institutional nature. As such, the target of the attacks in question might be somewhat diffuse; the intended harm being the undermining of the citizens' confidence in the capacity of the government and its security agencies to protect them, generalized fear in the community, and the like. Finally, the ways of acquiring the three substances as well as the knowledge to use them (as discussed in chapter 3) show that multiple groups of actors (e.g., vendors or internet users) are (albeit indirectly and unintentionally) involved in providing potential terrorists with the means to inflict this great magnitude

of harm.

Hence, the NMH principle is not only applicable to dual-use research but also to the identification of moral responsibilities and the establishment of associated, indeed derived, institutional responsibilities within the web of prevention against terrorist attacks using ricin, phosphine, and americium. As will be shown in the following section, applying the NMH principle to a range of groups of actors within this web of prevention is central to justifying their obligation to participate in this web.

Additionally, the NMH principle enables us to formulate clear institutional responsibilities for each of the relevant institutions and do so in a manner so as to ensure that each institution – via the individual members of that institution – contribute to the common goal (collective end) that it is the purpose of the web of prevention to realize, i.e., the prevention and mitigation of the threat posed by terrorists using the toxins in question.

In short, the activity of the participants in the web of prevention can be understood in terms of a complex multi-layered structure of joint action in which different institutions perform different interlocking actions in the service of a collective end – and these interlocking actions themselves consist in joint actions performed by members of a given institution. (See discussion and diagrams in Chapter 4.)

Miller, however, stresses that the NMH principle, much like most moral frameworks, shall not be seen as an absolute principle (Miller, 2018, p. 14) but rather as one that exists in a qualified form. Specifically, Miller makes three qualifications to the basic NMH principle that are relevant here. First

of all, the principle of necessity must be accommodated. He notes with regard to the dual-use debate that the dual-use research in question might justifiably violate the unqualified NMH principle if the beneficial consequences of the research in question cannot be achieved by means of other research with less potential to be used for harmful purposes. Regarding our concerns here, this qualification means that, for example, it might be morally justifiable for vendors of phosphine-based products to sell these products under certain circumstances (and with certain restrictions<sup>66</sup>) if no less dangerous alternatives are available (Miller, 2018, p. 14).

This point is related to Miller's second qualification in the application of the NMH principle. For dual-use research, Miller notes that the principle of proportionality is a restricting factor in applying the NMH principle: refraining from providing others with the means to do harm in all instances and without considering the extent of the possible harm and benefits of the dual-use research in question could potentially violate the principle of proportionality. For in some cases, the potential harm in questions might be disproportionately low in comparison to the benefits of a particular action. In relation to responsibilities with regard to the three common-use toxins, this qualification to the basic NMH principle must also be made.

If an internet user irresponsibly publishes, for example, the toxic properties of powdered ricin on a social media platform, it seems disproportionate to ask of the owner of the platform to actively investigate that user with regard to possible ties to terrorism or extremist ideologies. For the potential harm that the stakeholder in question (i.e., the owner of the platform) provides to

---

<sup>66</sup> See below for detailed debate.

others (through the post of their user) is arguably too indirect and distant to justify such investigations. Here indirect and distant means that the causal chain that leads to potential harm is too long and complex to morally justify such an active role to prevent it on the part of the stakeholder in question, namely, the platform provider. On the other hand, the platform provider might reasonably be required to ensure such irresponsible publications do not take place or are speedily removed and to assist security agencies in their efforts to identify potential terrorists who might come to possess this information. This brings us to the last qualification to the basic NMH principle, according to Miller.

In dual-use research, there can be cases in which a wide variety of actors are involved in a highly complex and novel research program. As a consequence, there is a twofold indeterminacy with regard to potential harms that might result from the malicious use of the research outcomes of this program. First of all, there is uncertainty with respect to the nature and extent of the potential harm that might be caused. Secondly, there are multiple actors with different roles who are involved in conducting the research program, e.g., those acquiring materials for the research, the researchers, the publishers, and those using the products generated by said research. Hence, the causal chain from initially conducting the research in question to using its products for harmful purposes might be long, highly complex and diffuse. Therefore, attaching responsibility and different degrees of responsibility after the harmful outcome (should it take place) might be extremely difficult, if not impossible.

This two-fold indeterminacy is particularly germane to our concerns here.



First of all, the uncertainty in assessing the nature and extent of harm that is potentially caused by the terrorist use of the three substances has been discussed in detail in chapter 3 of the thesis. It was shown that the high degree of uncertainty raises the potential impact of attacks using the substances in question since the consequences of an attack are not predictable.

Secondly, the large variety of stakeholder groups identified in chapter 5 as potential participants in a web of prevention with respect to the terrorist use of these substances is based on their (unintentional) involvement in *enabling* an attack with ricin, phosphine, or americium. Each stakeholder group that was identified in chapter 5 (with the exception of security institutions) is, in some capacity, causally involved in the provision of the means to terrorists to do harm by using the three substances. Yet, each stakeholder group individually (and unintentionally) provides potential terrorists with one element only (e.g., material, knowledge, the capacity to do soft damage) to fulfill their plan to inflict large-scale harm by using the three substances.

Hence, each stakeholder group is, unintentionally, participating in creating the condition that might enable an attack with one or other of the three substances. This is not a joint action since the stakeholders obviously do not have as an end (collective end) that there be an attack or that they enable an attack. On the other hand, they do have a joint responsibility to cooperate so as to remove these enabling conditions. They have this responsibility (in the context of the applicability of the NMH principle) by virtue of their role in providing an element of the overall conditions that enable the terrorists to perpetrate their attack. For instance, vendors of toxic products are providing

terrorists with the materials, members of the press who publicize the attack and its aftermath facilitate its impact in terms of the soft damage it causes, and so on.<sup>67</sup> Applying the NMH principle to this scenario means to identify the way in which each stakeholder group contributes to providing terrorists with the means to perform an attack with ricin, phosphine, or americium. Subsequently, it is possible to formulate responsibilities and actions for these stakeholder groups that are aimed at discontinuing the provision of these means to the terrorists. This discontinuation is the key component of the web of prevention in the present thesis.

### 3. The responsibilities of the stakeholder groups in the web of prevention

#### 3.1. The manufacturers

Equipped with the NMH principle, I argue that manufacturers of the three substances provide the means for terrorist attacks in the following sense: By producing products that contain ricin, phosphine or americium, manufacturing companies provide potential terrorists with the materials which enable them to launch attacks using toxins. Yet, it has to be noted that the manufacturers only indirectly provide terrorists with these substances since although they produce them, they do not sell them directly to the terrorists. In this regard, the manufacturers might face an ethical dilemma analogous to the dual-use dilemma confronting researchers: simply

---

<sup>67</sup> See below for a detailed discussion of that argument.

discontinuing the manufacturing of products that contain these substances might not be an option since there are no viable alternatives available to fill the need filled by the product. Phosphine might be an example of this dilemma: currently, there are no less dangerous rodenticides available that function as efficacious as phosphine in specific applications. Hence, it is arguably necessary to produce phosphine-producing rodenticides, and, in light of the expected harm produced by the misuse of the substance, it would be disproportionate to discontinue the production of phosphine altogether. Yet, according to the unqualified basic NMH principle, the manufacturers of products containing phosphine are morally obligated to discontinue providing terrorists with the means to do massive harm, i.e., to conduct attacks using phosphine.

This dilemma can be removed or mitigated if the manufacturers participate in the web of prevention. First of all, the manufacturers can assess the danger that their products pose if used by terrorists to launch attacks on a community. Since the manufacturers have in-depth knowledge of the properties and the toxicological profile of their products, they are valuable partners for security agencies in relation to the latter's threat assessments; specifically, their assessments concerning the potential terrorist use of these substances. By cooperating with security agencies in this manner, the manufacturers are undertaking active measures to reduce, if not eliminate, their provision of the means to terrorists to do large-scale harm. They do this while continuing to manufacture these products and without themselves engaging in the investigation or apprehension of terrorists; both of these options being disproportionate responses. Moreover, in doing this, they dissolve the dilemma that they face; the dilemma consisting of choosing one

or other of the afore-mentioned unpalatable options.

A second way in which manufacturer of toxins can fulfill their responsibility to refrain from providing potential terrorists with the means to do large-scale harm (and thereby further participate in the web of prevention) is to invest in certain kinds of research. Specifically, manufacturers should cooperate with researchers and research institutions in order to design novel products that do not offer terrorists the potential to do large-scale harm. One example of this approach (the so-called “designing for security” approach to be discussed in chapters 7 and 9) is the invention of the optical smoke detector as a safe alternative to americium-based detectors.<sup>68</sup> By investing and collaborating with other stakeholders in order to find alternatives to the current products, manufacturers of toxic substances can ultimately discontinue violating the NMH principle and participate in the web of prevention.

### 3.2. The vendors

In addition to the manufacturers, the vendors of products that contain ricin, phosphine, or americium possess a moral responsibility to participate in the web of prevention based on the NMH principle. Companies that operate hardware and farmer’s supply stores that offer either castor beans, rodenticides or smoke detectors can potentially provide (albeit unintentionally) an enabling condition for the preparation of a terrorist attack using ricin, phosphine or americium in terms of selling products that contain these substances to potential terrorists. This potential of vendors to

---

<sup>68</sup> See chapters 8 and 11 for discussion.

provide an enabling condition for a terrorist attack might result in their violation of the NMH principle since the vendors in question might in fact provide terrorists with the materials to do great harm. Hence, the vendors of products that contain the three substances ought to be part of the web of prevention by doing what they reasonably can to ensure that they do not provide these means to terrorists. However, to what degree is it the obligation of the vendors to restrict access to these substances, given that most users do not, in fact, intend to use them to do great harm?

At first glance, this seems like a problem that might be easily solved by means of legislative measures. It seems that if policymakers were to restrict access to these substances to users with government-issued permits or other like documents, then the vendors could fulfill their responsibilities in a simple and sustainable manner; namely by checking the authenticity of the customer's permit with every purchase. The burden of determining who was a malevolent user and who was not would be, in effect, with the agency that grants the permits (i.e., a government institution). However, restricting access to the substances in this manner faces two main objections:

(1) Slippery slope argument (proportionality)

First of all, the principle of proportionality challenges this proposed approach. Most of the damage inflicted by all three substances is soft damage that can be contained through a multi-layered approach consisting of education and communication.<sup>69</sup> Yet, the hard damage inflicted by all three substances is limited and, arguably, does not justify the restrictions on

---

<sup>69</sup> See chapters 10 and the special focus chapter of this thesis for detailed discussion.

the sale of these substances described above. Introducing or tightening restrictions on the sale of, for example, castor beans would involve introducing restrictions on other products that contain naturally occurring toxins as well. This would create a slippery slope at the bottom of which legislators would be forced to restrict purchases of cherries or apricots since their pits contain a certain amount of amygdalin.<sup>70</sup>

## (2) Necessity argument

As already mentioned briefly with regard to proportionality, it seems not only disproportionate but also unnecessary to tighten or introduce restrictions on all of the three substances in question in order to effectively prevent their illegal use. As I will show in the following paragraphs, the responsibilities of the vendors that derive from the NMH principle can be discharged by means of various cooperative or joint actions performed as participants in the web of prevention. Accordingly, further restrictions are superfluous.

There are two steps that vendors should take in order to ensure that they do not provide enabling conditions for terrorist attacks using ricin, phosphine, or americium. First of all, vendors have to be aware of the fact that they are selling the means do great harm. Yet, it is likely beyond the capabilities of the vendors to perform terrorist threat assessments in relation to each and every one of their products. Hence, such threat assessments should be, as argued above, the joint responsibility of the manufacturers and security agencies. However, these threat assessments of the products in question

---

<sup>70</sup> Amygdalin is converted into cyanide in the human body and can be used as precursor for toxic compounds such as hydrogen cyanide via hydrolysis (Bolarinwa et al., 2014) .

should be made available to the vendors in order to inform them about the products which they sell. Moreover, the availability of these threat assessments and their access to vendors should be part of the web of prevention.

Secondly, once the vendors are aware of the potential dangers these products pose once in the hands of terrorists, the vendors ought to undertake measures to thwart terrorists' attempts to acquire the products. That, of course, is a difficult task since terrorists will do everything within their capabilities to disguise themselves as ordinary customers. Here, again, it seems too much to ask of the vendors that they perform assessments and conduct background checks of their customers in order to determine the intentions behind their purchases.<sup>71</sup>

Yet, in order to comply with the NMH principle, the vendors have to be able to identify purchases of certain products that were made with malicious intentions. I will argue in chapter 9 of this thesis that the tools in order to identify suspicious purchases of certain products have to be provided to the vendors by security professionals operating in the field of counter-terrorism. Hence, as part of the web of prevention, vendors can be trained in identifying specific aspects of purchases that are, according to a definition provided by security agencies, suspicious in nature. Equipped with these tools, the vendors are able to report individual purchases that might pose a security risk to the relevant government institutions. In doing so, the vendors would be able to comply with the NMH principle and not provide

---

<sup>71</sup> In fact, such a practice is not only beyond the responsibilities of the vendors, but can also lead to ethically troubling practices as chapter 7 examines in some detail.

terrorists with the means to do large-scale harm.

### 3.3. The press

While the manufacturers and vendors (unintentionally) provide terrorists with the materials to do harm, the press provides terrorists with the means to do large-scale soft damage to the terrorists' target society. As already discussed in chapters 1 and 2, terrorists need a high degree of publicity in order for their attacks to have significant impact. Terrorist attacks in which the potential extent of hard damage (i.e., deaths and physical destruction) is quite low but the potential extent of soft damage (i.e., widespread fear and panic, reduction of trust in government and security agencies, etc.) is very high (as is the case with attacks using ricin, phosphine and americium) require particularly high levels of publicity in order to be successful. Hence, widespread and ongoing press reporting of a terrorist attack in which ricin, phosphine, or americium were used assists the terrorist cause by ensuring that the extent of soft damage is maximized rather than minimized. In this regard, the press is violating the NMH principle in that it is (unintentionally) facilitating the terrorist goal of maximizing the extent of soft damage. Newspaper articles exaggerating the lethality of ricin taken in conjunction with published pictures of police officers in HAZMAT suits in the aftermath of the Cologne ricin plot exemplify this unintended assistance to terrorists, and there are many, many other examples.<sup>72</sup>

In order to comply with the unqualified NMH principle, media outlets ought to discontinue providing terrorists with the means to successfully spread

---

<sup>72</sup> See the special focus chapter of this thesis for a detailed discussion of that matter.



fear and panic in society, undermine trust in security agencies, and so on. However, to simply discontinue to report on terrorist incidents like the Cologne ricin plot altogether would be a disproportionate response and, more important, it would not be an ethically sustainable option for this group of stakeholders, given their role of providing the public with information that they are entitled to have and, for that matter, given members of the public need to take some steps themselves to reduce the terrorist threat. Again there is a dilemma in need of resolution. The discontinuation of reporting on these issues would potentially violate a democratic principle of utmost importance, namely the freedom of the press. On the other hand, unfettered reporting of terrorist attacks may well, as we have seen, violate the NMH principle. Yet, this is only *seemingly* a dilemma with regard to terrorist attacks using toxins.

It is possible for news outlets to find a compromise. Instead of a blanket ban on reporting terrorist attacks using common-use toxins, media outlets can minimize the soft impact of these attacks by reporting on these attacks in a circumscribed manner. Instead of reporting these terrorist attacks in a manner essentially driven by financial profits, e.g., by exaggerating and otherwise sensationalizing the attacks, media outlets could report them in a manner driven by the public good understood as a compromise between public security and the public's right to know certain facts. Note that public security and the public's right to know are not necessarily in conflict.

The press is, in some cases, presenting the facts in a way that is assisting the goals of the perpetrators of terrorist attacks. By presenting worst-case scenarios in their headlines (that are, sometimes, qualified in the actual

article), journalists are, in effect, assisting in the terrorists' enterprise of creating fear and panic in society. Yet, if journalists choose to report on the facts of these plots in a more objective and restrained manner motivated by public security and the public's right to know rather than financial profit, then they will reduce the oxygen that they provide to terrorists and, indeed, assist in combating terrorism, i.e., they might very considerably reduce the extent to which they provide terrorists with the means to harm society. In this scenario, the journalists would act in accordance with the qualified NMH principle.

However, it might be argued that there is a problem with this proposal to constrain journalists' reporting of terrorist attacks. Complying with the unqualified NMH principle might be thought to unduly restrict freedom of the press; for it would limit journalistic reporting to the facts (and, presumably, associated objective analysis and comment) only in cases of terrorist plots using toxins. The counter-argument to this is that such limited restrictions are justified by the security risk posed by terrorist attacks.

Moreover, rather than have these constraints imposed upon them by governments, journalists could choose to self-regulate. As part of the web of prevention and in conjunction with the other stakeholder groups, journalists and media outlets could develop an ethical codex for reporting on terrorist attacks using toxins and, thereby, independently choose not to report certain unnecessary sensational details or worst-case scenario with regard to these attacks. In Germany, similar codes of conduct and agreements for self-censorship in journalism are already in place with regard to reporting on suicides. Most of the German news media outlets agreed not to report

suicides and suicide attempts in detail unless these incidents have strong societal relevance (e.g., the suicide of a politician or person of interest) (See Deutscher Presserat, 1997). The reason behind this censorship is that exposure to reports of suicides can trigger suicidal behavior in mentally ill persons. Hence, German media outlets choose not to provide these persons with triggering reports that could cause harm to them.

#### 3.4. The users and owners of social media applications

Social media platforms allow internet users to share and distribute information and media files around the globe. However, malicious agents are able to use these platforms to harm society and persons. Crimes like cyber-bullying, the distribution of illegal images and video materials of various kinds, and online-radicalization efforts are only a few examples of the potential of social media to be used to inflict harm.

Regarding the present study, there are, at least, two ways in which these platforms can help potential perpetrators of terrorist attacks that utilize toxins. First of all, terrorists can use social media platforms and online messenger services to organize attacks and to search for and distribute manuals on how to assemble improvised weaponry. Here, online platforms such as Wikipedia, Twitter, Reddit or messengers like Whatsapp or Telegram (albeit unintentionally) provide potential terrorists with the information they need in order to harm society on a large scale. The owners of these platforms are violating the NMH principle by providing the infrastructure that enables terrorists and would-be terrorists to acquire and share the expertise that is needed to commit these attacks. However, not

only the owners but also the users of these platforms are, arguably, violating the NMH principle, at least to some degree. Social media platforms and other relevant online applications such as Wikipedia are structured in a decentralized way and exclusively offer content created by their users (Wikipedia, 2021). Hence, the users of these platforms are actively assisting the process of providing potential terrorists with the means to harm others. Users do this by, for example, sharing an instructional video on Twitter or by contributing to a Wikipedia entry on how to purify ricin from castor beans.<sup>73</sup>

The second way in which social media platforms and their users provide terrorists with the means to harm society is by amplification of the soft damage caused by an attack; this amplification is done through social media posts. (See discussion in Reed & Ingram, 2019, pp. 4–8). Similar to, yet much faster and with more global reach than media outlets, social media posts about terrorist attacks that utilize toxin weapons can contribute to a climate of fear and panic in the aftermath of an attack. For example, tweets spreading rumors as well as posts from misinformed users in the aftermath of an ineffective radiological attack can contribute to the portrayal of this attack as an almost apocalyptic nuclear incident with harmful radiation levels. Even if the attack only caused minimal physical harm, the soft damage could be enormous, thanks to social media users and, consequently, the owners of these platforms.

Clearly, the owners and users of social media platforms and online applications such as Wikipedia are violating the NMH principle by

---

<sup>73</sup> See chapter 8 for discussion.

providing terrorists with the means to harm society in, at least, two ways. In order to comply with the unqualified NMH principle, both groups of agents might have to cease to provide these means. Yet, this cessation would have to be a shared effort involving the platform owners cooperating with their users and the authorities. Efforts by the group of platform owners themselves to delete or report relevant posts might be problematic with regard to the principle of freedom of expression and might also require the platform owners to define what ought to be a relevant post for flagging or deletion; a complex ethical task for which they are ill-equipped and ought not to be responsible. On the other hand, the owners of social media platforms could cooperate with the security institutions and representatives of social media users as part of the web of prevention. In doing so, the particular responsibilities of the owners would have to be identified in accordance with the overall division of responsibilities in the web of prevention.

This cooperative arrangement between the three groups of stakeholders in the web of prevention could, for example, have the following form: members of security institutions (after appropriate input from government, civil society, etc.) provide a definition as to what kind of online contents ought to be flagged, deleted or reported and then communicate a transparent list of these contents to the owners of social media platforms. The platform owners, then, have to build a suitable means to review the content on their platform in order to report or delete those contents that are listed by the security agencies. However, the practice of flagging inappropriate content is not the individual responsibility of the platform owners but rather a shared responsibility of the owners and the users of social media platforms. Since

all of the content on social media platforms is produced by their users, these users share the responsibility of the owners to flag (albeit not to delete) content that enables terrorists to harm society. Hence, the owners of these platforms have to inform their users to stay vigilant and report content that the security agencies defined to be dangerous in this regard. Furthermore, the owners of social media platforms have to provide an accessible infrastructure to allow their users to flag content without any hurdles.

### 3.5. The researchers

Academic researchers ought to be part of the web of prevention since their work has the potential to provide terrorists with the means to harm others in two different ways: First of all, academic researchers and scientists have a responsibility that is formulated in the dual-use dilemma. Chemists and microbiologists might be engaging in the development and production of materials that might be used by malicious users to harm society. Yet, since this responsibility of scientists has already been discussed at length, it will not be a focus of the present study (Bezuidenhout & Rappert, 2012; Crowley, 2013; Ehni, 2008; N. Evans, 2013; Forge, 2010; Kant & Mourya, 2010; Marchant & Pope, 2009; Miller, 2018; Miller & Feltes, 2018; Miller & Selgelid, 2007).<sup>74</sup>

The second way in which academic researchers might (unintentionally) provide terrorists with the means to harm others is far less discussed but is a pressing issue for terrorism researchers in particular. Academics in the field of terrorism research that focus on the psychological or “soft” impact of

---

<sup>74</sup> However, the section on the responsibility of manufacturers covers, at least partially, aspects of the dual-use debate.

terrorist attacks might (unintentionally) provide terrorists with the means to harm society. The accurate description and analysis of the damage a terrorist attack with an ineffective weapon in terms of hard impact but, initially unknown to the terrorists, highly effective in terms of soft impact could attract the attention of terrorists and, subsequently, lead them to use these weapons. Hence, one could argue that studies like the present one may provide terrorists with the necessary knowledge to understand the mechanisms of soft impact weapons. In this way, these studies may well violate the NMH principle.

Yet, as I will show in detail at a later point in this thesis, researchers can accommodate this problem in multiple ways and, thereby, fulfill their responsibilities under the NMH principle. By using as an example my own analysis of the current availability of americium (which analysis I will provide in chapter 7), I will argue that raising awareness of the dangers posed by weapons that can cause a high degree of soft impact can, in fact, reduce that impact. For if not only terrorists but also the public are aware of the underlying mechanisms that facilitate the soft impact of, for example, an attack with an RDD, then this impact can be reduced dramatically.

Hence, in chapter 8, I will argue that researchers in terrorism studies have a moral obligation to analyze the mechanisms behind soft impact weapons and to make these findings accessible to the public. Furthermore, it will be argued that these researchers should actively engage in awareness campaigns with respect to terrorist attacks that utilize soft impact weapons.

### 3.6. The citizens

The most heterogeneous and most abundant group of stakeholders in the web of prevention are members of the public. In this section, the public is defined as citizens and residents of a country that are (potentially) directly or indirectly affected by a terrorist attack. Obviously, the web of prevention cannot involve every single citizen in a structured way, but it could include representatives of this group who could discuss citizens/residents' responsibilities in consultation with members of the other stakeholder groups. In the first place, citizens/residents have an obligation to protect one another as far as they can. In the second place, for citizens are also (unintentionally) to some extent providing terrorists with the means to harm society. As already shown in the previous chapters, the soft impact that is produced by an attack with a toxin is primarily a psychological impact that has economic and political implications. In the aftermath of such an attack, high levels of anxiety among members of the public lead to the abandonment of the attacked area (and public spaces in general) for a long time span and these levels of anxiety lead to erosion of trust in security institutions.

Yet, it has been argued that weapons such as an americium-based RDD would, most likely, have minimal physical impact and would not have the capabilities to harm anyone via exposure to radiation. Hence, the widespread anxiety in the aftermath of such an RDD attack would be based on false beliefs and misinformation about the harmful effects of radiation and contamination. By being unaware and uninformed about the real nature of the threat, the public enables the harm (soft damage) done by the



terrorists to be much greater than it otherwise would be. Citizens and residents, if well informed and rational, are in a position to nullify the soft damage that might be caused by terrorist attacks that utilize toxins.

However, there are ways in which the public is able to cease to provide terrorists with the means to do harm with soft impact weapons. First of all, citizens can minimize the soft impact of an attack with toxins by being aware of the actual, relatively low, physical threat that these substances pose and by being informed about the mechanisms that facilitate soft damage so that they do not respond in ways that amplify the impact of the attacks. Incidentally, only informed citizens manage to prevent the amplification of the threat of soft damage posed by chemical and radiological weapons and, thereby, reduce the psychological impact that attacks using these weapons might have. Furthermore, every citizen is individually responsible for following the advice given in the government's information material and, thereby, to reduce the risk of getting injured or killed in the immediate aftermath of an attack. On the collective level of a liberal democratic society, these individual responsibilities can each be seen as small contributions in the discharging of the joint responsibility of citizens to create societal resilience effectively.

While members of the public have these responsibilities to respond in a manner that mitigates the soft impact of terrorist attacks that utilize toxins – and thereby discharge their responsibilities within the web of prevention – they are themselves not responsible for assessing the dangers of common-use toxins, starting awareness campaigns, and making resilience plans. Instead, representatives of the public ought to be provided with these plans

and campaigns by governments on the basis of advice from security agencies, researchers and knowledgeable others.

#### 4. Conclusion

In this second part of my thesis, I have shown that each group of stakeholders has a role to play in the web of prevention, and this role is a moral and institutional responsibility (given the web of prevention is an institutional arrangement, even for citizens/residents), either in light of the moral duty to provide security or in the light of the NMH principle (or, in some cases, such as citizens and residents, in the light of both principles). These different obligations assign specific actions to each group of stakeholders. These actions can, in collaboration with other stakeholder groups within the web, help each group to fulfill their responsibilities according to the NMH principle (and, given the general moral obligation to protect others, if one can).

With all these different joint actions of members of each group, the web of prevention becomes a multi-layered cluster of counter-measures against terrorist attacks that utilize toxins. The moral and institutional responsibilities of members of all groups of stakeholders, as well as their respective actions under these responsibilities, can be summarized in the following table:

<u>Group of stakeholder</u>	<u>Source of responsibility</u>	<u>Required (joint) action</u>
Security institutions	Institutional and moral responsibility to protect individuals and society	Counter-terrorism measures in executive, legislative, and judiciary branch
Manufacturers	NMH principle; refrain from providing the materials	Threat assessment (in cooperation with security institutions) and designing for security
Vendors	NMH principle; refrain from providing the materials	Being aware of the threat, reporting suspicious purchases
Press	NMH principle; refrain from facilitating soft impact	Avoiding reporting that amplifies soft damage from terrorist attacks
Users and owners of social media	NMH principle; refrain from providing the knowledge and facilitating soft impact	Reporting terrorist-related content

Researchers	NMH principle; refrain from providing awareness of soft impact to terrorists and provide awareness of negligible hard impact from certain toxins	Making research accessible to the public and participate in awareness programs
Citizens	NMH principle; provide the soft impact and responsibility to protect one another	Be aware of the threat and respond in ways that mitigate its effects, be prepared to survive it

*Table 1: Obligations and actions of stakeholder groups in the web of prevention*

This chapter discussed the web of prevention against terrorist attacks that utilize ricin, phosphine, and americium and did so from a normative perspective. While there is some collaboration between the groups and some joint counter-measures visible in the current reality of CBRN counter-terrorism, most of the discussed groups of stakeholders are currently unaware of their obligations to participate in the web of prevention; indeed, this thesis is the first systematic attempt to elaborate the web of prevention for such attacks. Therefore, this thesis provides a description of cooperative measures that ought to be put in place rather than a description of a currently existing web of prevention.

Moreover, thus far, I have not elaborated on the proposed web of prevention in any detail. The next two chapters of this thesis will discuss the current cooperative measures against the terrorist use of ricin, phosphine, and americium. It will be shown that these measures suffer from problems that can be traced back to the unawareness of the various stakeholder groups with respect to their obligations, especially as these obligations derive from the NMH principle.



## **Part III:**

# **Current counter-measures**

## **7. Preventing the acquisition of common-use toxins for terrorist purposes**

### **1. Introduction**

As seen part of this thesis, the fight against terrorism involving toxic substances can be described as a joint action that involves multiple sets of moral agents who work together towards the common goal of protecting society from this brand of violent extremism. In doing so, different institutionalized groups of actors, such as security institutions, corporations, and research institutions, create partnerships that can, if efficiently organized, form a so-called web of prevention. This web might also include non-institutionally-based groups of moral agents, such as members of the citizenry, as well as organizations not directly involved in security or in security-relevant industries. A security-relevant industry would include the manufacturers of toxins that could be used to make bombs. A non-security relevant industry might be those in the hospitality industry who might, nevertheless, be on the look-out for suspicious activities, e.g., waiters who notice packages left in crowded restaurants.

The following chapter gives a short overview of the partnerships that are currently in place to prevent the acquisition of toxic or radiological materials by terrorists in selected European liberal democracies. In order to analyze the nature of these partnerships in detail, it is, first of all, necessary



to restrict the amount of the materials in question to the most relevant (i.e., dangerous) materials for our case. Based on the results of the threat analysis in chapter 3, these three substances will be ricin (for biological weapons), phosphine (for chemical weapons), and americium (for radiological weapons). Furthermore, obviously, the entire spectrum of partnerships between European security institutions and other stakeholders is far too broad to outline in this chapter. Hence, the present analysis will focus on the partnership between security institutions and corporations or NGOs and research institutes and the partnership between security institutions and (relevant groups of) citizens. Each of these types of partnerships will be analyzed by discussing one aspect of each type of partnership by recourse to an example. These examples include specific cases of foiled terrorist attacks but also specific partnership programs.

The first example provided in this chapter will be the partnership between security institutions and online vendors, as it was observable in the Cologne ricin plot in 2018. The second example of partnerships established to deny terrorists access to dangerous substances will be the current cooperative counter-terrorism measures with regard to phosphine in Germany. The third and last example provided in this chapter is the current European efforts to combat the safety and security threats posed by americium-based products. In this example, the manufacturers of these products and the European legal institutions will be the most relevant stakeholders.

Equipped with these three salient aspects of partnerships between security institutions and other stakeholders, this chapter aims to give a first overview of the web of preventing terrorist attacks using toxic substances in the

European Union. However, in accordance with the focus of this thesis, most examples provided in this chapter involve the German security architecture primarily. Specific legal restrictions concerning the availability of the three substances and specific aspects of cooperation between security institutions and vendors and manufacturers might differ in other European states. Yet the following overview is the first of its kind to use the concept of a web of prevention to map the cooperative measures that are currently in place to reduce the threat in European member states from improvised biological, chemical or radiological devices.

## 2. Online vendors and security agencies: Ricin

The described foiled terrorist plot that gained notoriety as the so-called Cologne Ricin plot<sup>75</sup> includes facts that are of the utmost importance for the present chapter: these facts explain how the German security agencies became aware of Sief H's plot and were able to interrupt and arrest the perpetrator before he could successfully assemble his device and mount his attack. According to journalistic sources, German intelligence agencies were informed about suspicious online activities of the suspect by a foreign intelligence service and, consequently, started to investigate H (Flade, 2018; Westdeutscher Rundfunk, 2018). Unfortunately, not much is publicly known about the nature of H's online activities or about the counter-terrorism measures that enabled the detection of said activities. Most journalistic outlets only state in very general terms that the purchase of

---

<sup>75</sup> For description see introduction of this thesis.

castor beans via an online vendor connected to the Amazon corporation led to the detection of H's plot. As already described in detail in chapter 3 of this dissertation, castor beans are the beans of the plant *Ricinus communis* and contain the powerful organic poison ricin (Dukic, 2017, p. 33).

Here it is crucial to note that when attempting to acquire already processed powdered ricin, strict regulations and restrictions apply in the European Union. Since ricin in its synthesized, powdered form is explicitly mentioned as a toxic chemical in Schedule 1 of the annexes of the *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction* (CWC) of the United Nations, it is treated as a chemical (and, for that matter, toxic) weapon agent in every country that has signed and ratified the CWC (Organisation for the Prohibition of Chemical Weapons, 1992).

Since all countries in the European Union have signed and ratified the CWC, the production, stockpiling, and use of ricin by both state and non-state actors is strictly forbidden. These restrictions also forbid the selling and the purchase of weaponized ricin in the European Union, albeit with exceptions for certain research institutions. Additionally, most European member states have national legislation that forbids the sale and possession of ricin. For example, in Germany, the distribution of processed ricin is strictly restricted and regulated by the *Gesetz über die Kontrolle von Kriegswaffen* (*KrWaffKontrG*), which only allows selected research institutions and Governmental contractors access to this agent.<sup>76</sup>

---

<sup>76</sup> *KfWaffKontrG*, Annex (§ 1 Abs. 1) II, 3.1., d).

Yet unprocessed beans of the castor plant are not restricted at all in the European Union. Neither the possession nor the purchase of these beans is regulated by any EU regulation or national legislation in Europe or North America ( Evans, 2014; Louis, 2018). Hence, citizens of the European Union can purchase castor beans without any restrictions. In connection with H's case and with regard to the discussion in this chapter, this detail is crucial. In practice, it means that H. had unregulated online and offline access to this product. According to most media outlets, H. chose the online vendor Amazon to purchase the raw materials for his biological device (Flade, 2018; Rheinische Post, 2019; Westdeutscher Rundfunk, 2018).

However, any search for the details concerning his purchases and, even more important, any attempt to analyze how and why his purchase of the completely unrestricted castor beans raised flags with European security agencies is likely to fail since journalists' accounts typically lack the required specific details. However, the account of the terrorism researcher and journalist Florian Flade, who researched and published the Cologne Ricin plot in the magazine CTC Sentinel, can be of help here (Flade, 2018). Flade gives a slightly more detailed account of H.'s purchases and supports this account by referring to conversations with anonymous members of British intelligence services. Flade writes that

(...) [a]t some point in the preceding weeks, a British intelligence agency had warned the Bundesnachrichtendienst (BND) about suspicious online shopping activities by a Tunisian living in Germany. The British had discovered the purchases through some form of electronic surveillance. Further

investigation established that this individual was Sief Allah H. In May 2018, he had bought at least 1,000 castor beans and an electronic coffee grinder via Amazon Marketplace (Flade, 2018, p. 2).

In contrast to most other journalistic sources, Flade provides crucial information for the Cologne case that helps to further characterize the way that H's acquisition of materials was detected and disrupted by intelligence agencies. First of all, Flade identifies the German intelligence agency that was the recipient of the warning from a foreign agency as the BND. Furthermore, according to Flade, the agency that detected H's suspicious purchases and, consequently, informed the BND was a British intelligence agency. Flade also specifies details about H's purchases and describes how he bought around 1,000 castor beans and a coffee grinder to process these beans via the Marketplace app of the online vendor Amazon. Lastly, Flade gives first insights into how the British intelligence agency detected this purchase on Amazon. He states that the agency became aware of H's activities via "some sort of electronic surveillance." Flade bases this claim on an interview with an anonymous source who he identifies as a German security official (Flade, 2018).

That last detail might be the most important point for the present chapter since it suggests that the unspecified British intelligence agency had electronic access to the customer activities on Amazon.com or was directly informed by the company about the purchase. Here both possibilities imply a partnership between the online company Amazon and the British intelligence agency in order to prevent the acquisition of ricin by terrorists

and other criminals.<sup>77</sup> However, Flade's description does not specify the nature of this partnership and what its activities are. Yet one can think of two possibilities regarding this partnership between Amazon and British intelligence services: Either A) Amazon allows British security institutions access to their databases upon request to enable the detection of suspicious purchases or B) Amazon is actively tracking suspicious purchases and reports these to British intelligence agencies.

A) The first possible partnership between British intelligence services and Amazon is of a passive nature and entails a minimum standard of cooperation with the government and its security agencies on the part of Amazon. Only if requested by security agencies does the company have to disclose the identity of purchasers of a certain product or the online activities of a certain individual. For Amazon, that would only entail having a database of customers and purchases and allowing security institutions very limited access to this database.

It is crucial to note that, if it is involved in a partnership of this nature, Amazon is cooperating with security institutions in an explicitly passive manner that is comparable to the partnerships between security agencies and internet service providers (ISP) in the European Union.<sup>78</sup> In most European

---

<sup>77</sup> Obviously, there is another possible scenario thinkable in which British security institutions monitored Amazon customer activities without any knowledge or consent on part of the Amazon company. However, this possibility will not be discussed in this chapter, since it does not involve any relevant partnerships between the company and security institutions. In that case Amazon would completely ignore its role and responsibilities within the web of prevention.

<sup>78</sup> This partnership has been regulated by the EU Directive 2002/58/EC since 2002. Yet every member state has to implement this directive in a way that is coherent with existing national legislation and the national constitution. For example, in Germany different

member states, ISPs have to keep records of the online identities of their customers by storing the IP addresses of their customers for a certain amount of time. That enables security agencies to inquire and request the names of specific customers by, for example, providing the ISP with an IP address that was detected by security agencies in connection with an online crime (Moser-Knierim, 2013). One indicator that Amazon might cooperate in this passive manner with security agencies can be found in the company's EU-specific privacy policy, where it is stated that "[w]e may be required to disclose personal information that we handle under the Privacy Shield in response to lawful requests by public authorities, including to meet national security or law enforcement requirements" (Amazon, 2019a). Here Amazon explicitly states that it only discloses certain customer information if requested to do so by security agencies.

However, while this practice of ISPs (regulated under EU Directives 2002/58/EC and 2006/24/EC but later nullified) has been a matter of controversy in the European Union (Ni Loideain, 2015), arguably companies like Amazon have a more stringent moral responsibility to cooperate with security agencies than do ISPs. Since Amazon provides a platform for private vendors and customers to exchange specific goods worldwide, the company is morally responsible to, at least, inform security agencies about illegal or highly suspicious activities on their servers. As already established in the previous chapter of this dissertation, companies like Amazon, which are offering goods and materials that can be used for

---

attempts to implement the directive were ruled unconstitutional and at the time of writing the German government has not yet managed to successfully implement EU Directive 2002/58/EC (See for discussion Moser-Knierim, 2013).

terrorist attacks, have a moral responsibility to, at least, closely cooperate with national security institutions by reporting suspicious activities. In doing so, they contribute to the overall effectiveness of the web of prevention and, thereby, discharge their (jointly held) part of the collective moral responsibility that underpins the web.

In the last chapter, the NMH principle was introduced to provide moral guidance to these companies. In line with this principle, the moral responsibilities of companies that sell or produce relevant materials (Bures, 2015; Hemphill, 2003; Petersen, 2008) to report suspicious activities might exceed their legal obligations and restrictions. I argue that Amazon and other online vendors clearly belong to this category of companies: As seen in events such as the Oslo bombings in 2011, criminals and terrorists, in particular, are using the internet to purchase materials for their activities. The perpetrator of the attacks on 22 July 2011 in Norway, Anders Behring Breivik, ordered several precursors and fuses for the ANALNM/ANALFO based IED via the internet (Hemmingby & Bjørgo, 2018; Kaati & Johansson, 2016).

Furthermore, an EU Committee staff working paper that accompanies the European Parliament and Council proposal for regulation of the marketing and use of explosives precursors states that “[e]xplosives precursors are reportedly more widely available on the internet than in physical markets” (European Commission, 2018, p. 19). This observation can also be extended to other dangerous substances, including ricin and its raw materials such as castor beans. Hence, it seems that online vendors like Amazon play a crucial role in the dissemination of these substances for illegal purposes.



Considering the terrible impact that these substances can have if they get into the hands of terrorists, one could argue that companies like Amazon have a moral responsibility that exceeds the legal responsibilities of ISPs and other online companies. Hence, Amazon ought to have a well-functioning reporting system in respect of suspicious purchases of castor beans or other ricin precursors. Thus Amazon ought to do more than just provide selective access to customer data when requested to do so by security agencies. However, this more active role gives rise to other ethical issues.

B) The second possible role that Amazon could play in the web of prevention with regard to ricin and castor beans is a more active role of *reporting* suspicious activities on their servers directly to security institutions rather than just enabling detection by providing security agencies access to their databases upon request. Since Amazon has the technical ability effectively to track and analyze purchases and customer behavior on their servers with the help of sophisticated algorithms, the company is also able to detect suspicious activities and purchases on their platform with little or no assistance from security agencies and, consequently, report these activities to the relevant security agencies. This activity of Amazon is also congruent with the company's conditions of use, according to which Amazon encourages its users to actively report any "[u]nknown, Suspicious, or Fraudulent Purchases, Orders, or Credit Card Transactions" (Amazon, 2019c). In addition to this call for user vigilance, Amazon also states in its privacy notice that

[w]e release account and other personal information when we believe release is appropriate to comply with the law; enforce or apply our Conditions of Use and other agreements; or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction (Amazon, 2019b).

This statement implies that Amazon directly detects and reports illegal, but also suspicious, behavior and purchases to the authorities rather than merely passively enabling the detection of these activities by the security agencies themselves. Another statement that supports the hypothesis that companies like Amazon ought to take a more active role in the detection of suspicious purchases comes from the above-mentioned working paper of the EU Committee staff. Here it is stated that

[s]ome Member States have recently started working with online retailers and marketplaces, including eBay and Amazon, to raise awareness, improve detection capabilities and enhance information exchange with competent authorities. The main challenges for operators are related to identifying products of concern, detecting non-compliant items, identifying meaningful suspicious activity indicators, and handling large and diverse amounts of data. There are however good practices in the processing of orders, automatic data capturing and application of algorithm to report suspicious transactions that could be helpful to some operators (European Commission, 2018, p. 19).

This quote clearly suggests that companies such as Amazon should cooperate closely with national security agencies of some member states of the European Union. Phrases like “improve detection capabilities” and “identifying products of concern, detecting non-compliant items, identifying meaningful suspicious activity indicators” further support the claim that companies like Amazon appear already to actively identify and report suspicious activities on their platforms.

However, even the working paper of the EU Commission staff fails to provide details of what this active counter-terrorism role of Amazon consists of. Furthermore, it is important to note that this working paper is mainly concerned with materials that can be used to assemble IEDs. Many of these materials are subject to EU regulations and restrictions. That gives Amazon clear legal guidelines on how to handle the purchase or selling of these products on their platforms. For example, a vendor who offers ammonium nitrate on an Amazon market place can easily be detected and reported to the authorities since ammonium nitrate is subject to a considerable number of restrictions in the member states of the European Union. Hence, every unregulated sale of ammonium nitrate on Amazon is not merely suspicious but also illegal and can be handled accordingly by the company.

However, products like castor beans provide a challenge to companies like Amazon if these companies decide to take an active role in identifying and reporting suspicious purchases on their platforms. Since the trade of castor beans is neither restricted nor regulated in the European Union, Amazon cannot simply consider each and every purchase of these beans as

suspicious (let alone illegal) or assume that behind every purchase is a terrorist or criminal intent. Hence, to efficiently report suspicious purchases, Amazon has to collect additional data about the purchaser in question and, for example, investigate what other products were purchased by this customer. In the case of H., the coffee grinder might have been one indicator of H's intention to grind the beans in order to produce ricin. However, these investigations into their customers raise ethical issues for Amazon:

It is important to note that the definition of what ought to be regarded as a suspicious purchase solely lies with Amazon in this case. It is only Amazon's employees and, specifically, its analysts who decide what is a suspicious activity that ought to be reported. This means that Amazon employees have taken up specific tasks of counter-terrorism analysts and, indeed, they are the sole source of what is to be regarded as a terrorism-related activity on the Amazon website. Keeping in mind that the purchase of castor beans is legal in the European Union and that other purchases (for example, the purchase of coffee grinders) are, of course, legal as well, it would be solely up to the Amazon employees to connect these two legal activities and to determine criminal (or terrorist) intent behind this combination of purchases.

In order to effectively take such an active role in the efforts to prevent terrorist weapon acquisition, Amazon employees would have to investigate the behavior and activities of particular customers in detail and, consequently, would have to make judgments about their likely intentions and ideological background. They might even need to investigate these persons' online activities beyond the Amazon platform.

However, by attempting to fulfill their moral responsibilities to report suspicious activities in such a proactive manner, Amazon employees are under pressure to perform the tasks of a counter-terrorism investigator of the kind employed by governmental security agencies. If they aim at fulfilling their moral duties in an efficacious manner, and without any assistance from governmental institutions, they would have to define and detect the suspicious (but legal) activities of individuals, they would have to investigate these individuals and their backgrounds, and, consequently, they would have to track the individuals and their suspicious activities and report these activities to law enforcement. It is obvious that, if it was contributing to the web of prevention to such an extent, Amazon would essentially be doing the work of government intelligence agencies and, thereby, be in a position to replace them to some extent.

However, as already shown in the previous chapter, national intelligence agencies and their employees have an institutional responsibility to prevent terrorism and are possessed of certain powers under national legislation. This enables and requires counter-terrorism analysts at times to make discretionary judgments that involve, for instance, weighing privacy against national security in particular situations but, nevertheless, they operate under legal restrictions. Moreover, the institutional design of intelligence agencies in a liberal democracy is such that they are subject to oversight by governmental committees to ensure the lawful and ethically sustainable use of their powers. It would be ethically problematic to leave this highly sensitive field of intelligence analysis solely to private businesses like Amazon that do not answer directly to governments and are not subject to government oversight and, more generally, to mechanisms of democratic

accountability. An active role in *investigating* the suspicious (yet prima facie legal) behavior of individuals would clearly exceed the jointly held moral responsibility that Amazon has in the context of the web of preventing biological, chemical, or radiological attacks and, simultaneously, would potentially undermine or otherwise compromise the work of governmental agencies which were designed to conduct these investigations in a manner that conforms with liberal democratic values.

Adding to these ethical issues, it is important to note that private businesses like Amazon are subject to strict privacy laws in the European Union that are designed to prevent them from detailed and intrusive monitoring of individual customers or individual customer behavior. Hence, it seems not only ethically troubling but could also be illegal for Amazon to play an active role in determining and investigating suspicious behaviors of individual customers. These privacy rights might be overruled in the case of an immediate, massive terror threat, yet the assessment of such a threat and the decision to overrule privacy rights are tasks that only ought to be performed by national security institutions. In fact, as shown in the previous chapter, such assessments and decisions are exclusively part of the institutional responsibilities of security agencies within the above-introduced web of prevention and ought not to be performed by other stakeholders.

As illustrated by this short case study, there seems to be a partnership between Amazon and European security institutions that attempts to provide for the role Amazon and other corporations play in the web of prevention. It has been shown that a passive role of “enabling detection” (option A) might

not be sufficient to fulfill Amazon's moral responsibility under the NMH principle. However, more active participation in the web of prevention consisting of investigating and reporting suspicious activities (option B) exceeds Amazon's moral responsibilities and creates serious ethical problems. There is, therefore, a need to rethink options A and B. This will be done in chapter 9 of this dissertation.

### 3. Hardware stores and reporting suspicious purchases: Phosphine

While the case study of the Cologne ricin plot is primarily concerned with responsibilities in detecting suspicious combinations of purchases, the case of phosphine requires a focus on purchases of suspicious *amounts* of the substance. As already described in chapter 3 of this dissertation, the purchase of small packages of calcium phosphide is allowed without any restrictions in some EU member states, including Germany. Hence, it is necessary to further analyze what kind of cooperative measures are in place to regulate the sale of these packages in Germany and whether these measures are sufficient to contribute to the counter-terrorism agenda.

Due to its high toxicity, phosphine is regulated on the German market through different laws. There are specific regulations concerning the storage and handling of the companies selling phosphine and phosphine-producing substances. In addition, the German law concerning the prohibition of certain chemicals (*ChemVerbotsV*) and the legislation concerning dangerous goods (*GefStoffV*) include regulations on the purchase of these products by private consumers. The laws only permit the purchase of phosphine-

producing substances (like aluminum or calcium phosphide) if the purchaser has a permit, which is granted after having specific government-licensed training in the handling of toxic gases for pest control (*Begasungsschein*).<sup>79</sup> This regulation seems to be a suitable measure for restricting phosphine users only to those specifically trained and documented persons who can provide legitimate reasons for the use of this gas (such as, for example, being an employee of a pest control company).

It is reasonable to believe that, to some degree, potential terrorists will be deterred from acquiring phosphine-producing products simply because the process of the training and the documentation of the license poses a great risk of exposure and, ultimately, arrest. The case of the *Begasungsschein* is a good example of cooperation between government institutions and the industry that produces and sells phosphine-producing products. The government introduced the necessary legislation in order to limit the use of phosphine to those who have legitimate purposes while also providing manufacturers and vendors with the necessary tools to verify that their customers have legitimate uses for their products. The government-issued permit allows the companies to fulfill their moral obligation in terms of the NMH principle in a suitable way and without spending an excessive amount of resources on this security measure.

However, while this cooperative system of counter-measures assigns an appropriate role for each of the stakeholders, there is a loophole in the legislation that could be used by malicious actors. Hence additional or heightened institutional responsibilities need to be assigned to both

---

<sup>79</sup> See chapter 3 for discussion.



companies and government agencies if they are to fulfill their respective moral obligations. This loophole is the exemption in the *ChemVerbotsV* and the *GefStoffV* that permits small amounts of phosphine-producing products to be sold to private customers who do not have a license. As already briefly mentioned in chapter 3 of this dissertation, private customers are allowed to purchase small packages of calcium phosphide tablets without the *Begasungsschein*, if they are at least 18 years of age and if the vendor does not suspect any illegal use of the substance by the customer<sup>80</sup>. However, the vendor is required to inform the customer about the dangers and possible health hazards connected to the product.

Furthermore, and most important for this chapter, the vendor is required by the *ChemVerbotsV* to document every purchase of phosphine-producing products. Specifically, the identity and address of the customer, as well as the exact amount of purchased products and the intended use of the product by the customer, have to be documented together with the date of the purchase. The records of the purchase have to be archived for at least five years by the vendor. In the German industry and local administration, this documentation is commonly referred to as *Giftbuch* (book of toxins).

Analysis of the legislative hurdles to purchasing small amounts of phosphine-producing chemicals in Germany reveals that the government (in cooperation with the security agencies) has shifted the entire responsibility to combat the illegal use of the product to the companies selling said products. First of all, there is the matter of the documenting of every

---

<sup>80</sup> In the German original “(...) wenn, (...) keine Anhaltspunkte für eine unerlaubte Verwendung oder Weiterveräußerung vorliegen“ *ChemVerbotsV*, art. 8, 3, (1).

purchase. The relevant legislation (in this case, the *ChemVerbotsV* and the *GefStoffV*) leaves it open to the vendors who sell calcium phosphide as to the precise manner in which to document the purchases of the substance. Specifically, this means that it is up to the vendors whether to document the purchases in a physical notebook or in a digital database. However, the law specifies that the documentation of these purchases is also allowed in digital form. This documentation serves two goals: Firstly, all purchases of calcium phosphide by customers without a license are documented with the full name and details of the customer so that security agencies can, if necessary, review this documentation and identify suspects, individuals of interests or suspicious purchases in general. Secondly, the documentation of these purchases allows the vendors to limit the number of purchased products to what are called “common amounts for non-professional users” (*haushaltsübliche Mengen*)<sup>81</sup>.

As seen in chapter 3 of this dissertation, phosphine-producing products do not have to be processed or mixed with other products (except H<sub>2</sub>O) in order to be used as a weapon. However, phosphine is only likely to have serious health effects on exposed individuals if deployed in substantial amounts. Hence, other than in the case of ricin and the Cologne ricin plot, security issues with the purchase of phosphine are based on the purchased amounts rather than on their combination with other purchases (such as coffee grinders). Due to this focus on the size of the purchase, the *Giftbuch*, which

---

<sup>81</sup> Based on an unstructured interview between the author and a representative of one of the most relevant vendors of calcium phosphide in Germany. The interview partner preferred to remain unnamed.

documents the number of purchased products, seems an adequate solution to track suspicious purchases of calcium phosphide.

However, this focus and the current measures in place to prevent excessive purchases of calcium phosphide in Germany pose two problems; one theoretical, the other applied. The theoretical problem arises from the general notion of non-professional users in legislation. Non-professional users are allowed to purchase products that emit no more than 15 grams of phosphide for occasional household use. However, it is not specified what “occasional use” means in this context. Hence, the government leaves it to the vendors to decide what the definition of “occasional use” is and, therefore, what specific amounts of the product can be sold. The vendor has to decide in each and every case if the purchase of, for example, five packages of calcium phosphide is a legitimate amount for “occasional use” or a suspicious purchase request that the vendor should not, according to the *ChemVerbotsV*, fulfill.

Secondly, in relation to the application of the legislation, it might be impossible to stop the purchase of excessive, and hence highly suspicious, amounts of calcium phosphide for vendors of hardware and farmer’s supply stores in Germany if the customer in question buys only a few packages per store but in multiple different stores. As confirmed by a representative of a relevant German company, the *Giftbuch* is present only as a physical notebook in each store that sells calcium phosphide. This book is an entirely decentralized tool to document calcium phosphide purchases and, therefore, is not able to detect a purchase of suspicious amounts of this product that is spread across several different stores. Hence, potential terrorists might be

able to purchase large amounts of this product without this being detected and without disguising their identity when making these purchases. Due to the decentralized toxin books in each and every store, the vendors would not be able to detect this highly suspicious purchase and, hence, would not be able to fulfill their moral obligation to report it to the security institutions. Consequently, the industry-wide centralization of the *Giftbuch* might be one of the most important steps for relevant companies in order to contribute efficiently to the web of prevention. Chapter 9 of this dissertation will discuss this detail in depth.

However, in order to undertake the necessary steps to ensure that the distribution of calcium phosphide tablets in Germany has adequate security, the relevant stakeholders have to be, first of all, aware of the threat that phosphine poses with regard to terrorism. This required awareness is not comparable to the security awareness required of manufacturers and security in relation to, for example, ammonium nitrate. Since phosphine has not been used by terrorist organizations or lone operators in attacks against Western democracies yet and is not considered a chemical warfare agent, most of the relevant stakeholders participating in the web of prevention do not identify this substance as relevant with regard to counter-terrorism.

For example, one of the leading companies that produce calcium phosphide tablets in Germany, the company Wuelfel, does not believe that malicious actors might have a use for its products. Specifically, a representative of Wuelfel states that “[i]n our opinion the mentioned products [i.e., amongst

others calcium phosphide] cannot be used for illegal purposes.”<sup>82</sup> This statement shows clearly that the management of Wuelfel is not aware of the security threat phosphine poses in relation to terrorism.

Yet it remains open whether these companies have a moral responsibility to be aware of all possible safety and security threats that their products can pose. Obviously, within the above-constructed web of prevention, the relevant government institutions have a strong moral obligation to identify security threats arising from consumer products. Furthermore, these institutions are obligated to inform the relevant companies about the threat as well as to undertake necessary steps in order to mitigate or remove these threats. Raising awareness of the potential terrorist use of phosphine would, hence, be part of this responsibility of security institutions.

However, arguably also companies that *manufacture* phosphine-producing chemicals (such as calcium phosphide) have a moral responsibility to be aware of possible security issues arising from their products. In order to comply with the NMH principle, Wuelfel and other relevant corporations ought to inform themselves of, and undertake threat assessments in relation to, potential malicious uses of their products. Since those companies are obviously the most knowledgeable stakeholders in the web of prevention with regard to the properties and potential uses of their products, all corporations that are manufacturing phosphine-producing products are, jointly with government institutions, morally responsible for being informed about potential illegal use of their products. For only with this threat

---

<sup>82</sup> In the German original: ““Die genannten Produkte eignen sich nach unserer Auffassung nicht für illegale Zwecke”. Quote based on an e-mail conversation between the author and a representative of Wuelfel GmbH.

awareness, can they cooperate with government institutions in order to effectively mitigate or remove the threat and, thereby, make sure that their products are not misused as a means to harm society. Ways to organize this threat awareness communication between security institutions and companies effectively and in an ethically sustainable manner will be discussed in chapter 9.

However, what of companies who do not produce, but merely sell products such as calcium phosphide? As already seen in the Amazon case above, it might be very difficult for some vendors to be aware of every possible security threat arising from their products. Threat assessments concerning every new product that a store introduces are not the moral responsibility of these companies; or, at least, the NMH principle does not require this of these companies. Since vendors like Amazon or farm supply stores do not have in-depth knowledge of these products and do not manufacture them, it is sufficient that they are aware of general risks evolving out of these products (such as toxicity, explosive properties, etc.) in order to fulfill their responsibilities by the lights of the NMH principle. Threat assessments and awareness campaigns are beyond their responsibilities here.

Hence, it is the responsibility of the other stakeholders in the web of prevention (i.e., government institutions, e.g. security agencies, and manufacturers) to inform the vendors about the security risks evolving out of the sale of phosphine-producing products. This responsibility is partly covered in Germany by the *GefStoffV*. Here it is stated that every vendor that offers phosphine-producing products (and other dangerous goods) has to acquire a government-issued certificate and a training program that

informs, amongst other things, about security-related issues of these products on a general level.

Lastly, it has to be noted that there is good reason to believe that, in the special case of phosphine, even the government agencies in the European Union do not live up to their moral and institutional responsibility to be informed and aware of the potential terrorist use of phosphine. While in the United States, phosphine is considered a TIC with a moderate danger of terrorist use by the Department of Homeland Security (DHS), the European security institutions have not published any assessment of this specific chemical in relation to terrorism. Furthermore, academic research in the field of phosphine and terrorism is scarce as well. The author could only identify few articles that even mention the connection or use of phosphine by terrorists (G. Ackerman & Jacome, 2018; Binder et al., 2018; Bogle et al., 2006; Gurjar et al., 2011; Mika & Fiserova, 2011; Quillen, 2016). This is partly due to the fact that it was only recently that phosphine was discovered as a potential weapon and tested by terrorist organizations like ISIL. Unlike, for example, chlorine, phosphine is not widely considered a chemical weapon agent.

To sum up, it has been shown that the counter-measures against the terrorist use of phosphine involve cooperation between government institutions, manufacturers and vendors of phosphine-producing products. The purchase of large amounts of these products ought to be a particular focus for these cooperative counter-measures. Furthermore, it was shown that awareness of the threat is essential to an effective web of prevention for phosphine-based terrorism.

#### 4. Re-designing for security: Americium

Unlike the cases of ricin and phosphine, the cooperative measures of security institutions and companies to prevent the misuse of americium in smoke detectors are focused on the technology itself rather than its distribution. As already discussed in some detail in chapter 3 of this dissertation, ionizing smoke detectors with  $^{241}\text{Am}$  are strictly regulated in all of the mentioned liberal democratic states, with the exception of the United Kingdom and the United States of America. However, rather than discussing the absence of regulations concerning ionizing sources in these two countries, this chapter will show that in the European Union (except the UK), the security threats posed by  $^{241}\text{Am}$  based smoke detectors could be successfully removed or mitigated by favoring and introducing a competitive, less dangerous product: the optical smoke detector.

In Chapter 3 of this thesis, it was shown that both the European Union and the IAEA call upon their member states to perform rigorous risk assessments regarding the sale and use of ionizing smoke detectors. Reliable smoke detecting technologies with optical LEDs as sensors play an important role in the risk assessment of many European countries. For example, the IAEA published the French risk assessment concerning the use and distribution of  $^{241}\text{Am}$  based smoke detectors in 2016. Here, the justification to use ionizing smoke detectors until the time of the re-assessment was explained by the fact that

[a]t the time when these detectors were being installed on a large scale, they were able to offer a better response time than the available non-ionization technologies. The use of radiation



was thus fully justified in order to comply with the fire related standards in force and to protect people against the risk of fire (IAEA, 2016, Annex III).

However, the authors of the threat assessment also state that this status has changed over the last decades in France and the European Union. They argue further that

[s]ince the large scale installation of detectors of this type, their efficiency in comparison with that of other non-ionizing technologies has been progressively reassessed. This has followed the successive technological developments of non-ionizing detectors (particularly optical detectors and thermal detectors) that enable the detection of smoke as early as do ionization chamber smoke detectors (IAEA, 2016, Annex III).

In this risk assessment, it is clearly visible that for the French government, further developments in optical smoke detection technologies enabled a re-assessment of the necessity to use ionizing smoke detectors. Next to potential radiation risks connected to the disposal of ionizing smoke detectors that are mentioned in the French assessment, the developments in optical sensor technology also, at least implicitly, helped to efficiently deter the illegal (and potential terrorist) use of  $^{241}\text{Am}$  in countries like France. The use of ionizing smoke detectors in private households could be easily banned since optical smoke detectors offered comparable reliability without the radiation-related risks. This reliability of optical sensing technologies for smoke detection was confirmed by international standards such as the

Construction Products Regulation 305/2011 in the European Union, which was crucial for the French risk assessment (IAEA, 2016, Annex III).

One core element in the French web of prevention against terrorist attacks with americium-based RDDs is the restriction of access to americium by way of legislation banning ionizing smoke detectors. Hence, one could interpret this counter-measure as realized solely by government institutions without any assistance from companies or other stakeholders.

However, a closer look at the above-quoted risk assessment in France reveals that the necessary prerequisite to being able to ban the americium-based smoke detector was the free market-based innovation and marketing of qualitatively equivalent optical smoke detectors in the European Union. Hence, by offering an affordable alternative to ionizing smoke detectors of equal quality, companies and market-sponsored research institutions contributed a key element to the struggle to deny terrorists access to  $^{241}\text{Am}$ . After the innovation of the first optical smoke detector by Donald F. Steele and Robert B. Enemark for the US-based company Electro Signal Lab in 1975, this technology continued to be developed and became more reliable, cost-efficient and available across the globe (Steele & Enemark, 1975). Thus, in the case of americium, an alternative technology and its acceptance in the market prevented the misuse of this substance by making products with americium superfluous for private customers.

Accordingly, the cooperative measures to prevent the acquisition of  $^{241}\text{Am}$  arose from an interactive process comprising increasingly strict international and national regulations on the processing, use, and disposal of radioactive

materials on the one hand, and development of innovative products that do not include radioactive substances on the other hand. The market-driven development of these products enabled the industry to circumvent the more and more strict (and, hence, expensive) regulations, but also made it possible for international and national regulatory bodies to tighten the regulations on radioactive products.

Finally, governments such as the French government had the opportunity to prohibit the sale of certain radioactive products (specifically, ionizing smoke detectors) since appropriate alternative technologies had successfully entered the market. In the case of the shift in the market from ionizing to optical smoke detectors, one can further assume that in the EU the end-consumers influenced this shift as well. Due to the phenomenon of “radiophobia” in many Western societies<sup>83</sup>, it is reasonable to assume that many customers preferred optical smoke detectors over ionizing ones as soon as these products reached the same level of reliability and were sold for affordable prices.

At first glance, this mechanism and, in particular, the design changes in smoke detector technology strongly resemble a concept that is called “value-sensitive design” or “design for values” in the ethics of technology.<sup>84</sup> According to Jeroen van den Hoven, Ibo van de Poel, and others, Design for Values is the practice of incorporating moral and societal values directly into the design process of novel technologies in order to ensure that these technologies are developed in a morally and socially responsible way (For a

---

<sup>83</sup> See chapter 3 for discussion.

<sup>84</sup> The concept of Design for Values will be further explored in chapter 9 of this thesis.

detailed discussion see Van den Hoven et al., 2015). The above-described security-related effects that resulted from developments in optical smoke detector technology could be seen as a process of designing the value of security into this particular technology. By providing a technological alternative to the ionizing smoke detectors that posed a security risk, Steele, Enemark, and other developers of optical smoke detection technologies incorporated the value of security into the design process of these novel smoke detection technologies. Simply by designing these products without any hazardous radiological substance, these developers contributed to counter-measures against radiological terrorism and did so in close (even if implicit) cooperation with legislators and other government agencies. These latter actors were able to steer the development of new technologies in particular directions by using regulations and stricter rules concerning radiological materials.

Hence, one could argue that the cooperative process of technology developers, companies, and legislators and other government institutions to change existing technologies by re-designing them or by designing new, alternative technologies for the value of security is a suitable measure to fulfill the moral responsibility of all relevant stakeholders with regard to the NMH principle and as part of the web of preventing radiological terrorism. A detailed discussion of how the concept of Design for Values can contribute to the web of prevention with regard to radiological terrorism can be found in chapter 9 of this dissertation.

However, while designing novel technologies and alternative technological solutions for the value of security might be a suitable way for companies

and developers to fulfill their responsibilities to contribute in the web of preventing radiological threats, arguably this very measure was not applied in case of the development of optical smoke detection technologies. Although it seems that the value of security was one of the core motivations for both designers and legislators to design (or to promote the development of) the optical smoke detector, there is no written statement or study about the intentions behind the development of this novel technology available. Hence, one can only assume that Steele, Enemark, and others were partly motivated by security concerns in inventing the optical smoke detector.

Yet, the legislative documents that promoted the development and marketing of optical smoke detectors and that encouraged the introduction of stricter rules on the manufacturing and sale of ionizing products, justified this promotion, marketing and encouragement in terms of safety and security concerns. For example, the above-mentioned re-evaluation concerning the sale of ionizing smoke detectors by the French government proposed to prohibit the sale of these products and justified this proposal in terms of safety concerns with regard to the disposal of ionizing sources. The same goes for other international legislative measures like, for example, the European Council Directive 2013/59/Euratom. In this directive, the motivation to call upon national risk assessments concerning consumer products with ionizing sources is formulated in very broad terms.

Yet, the directive clearly refers to the risks associated with occupational, medical, and public exposure to radiation. Hence, in this directive, general safety, security, and health-related concerns led to the recommendation to re-evaluate the sale of ionizing smoke detectors. While the national and

transnational legislators and institutions apparently considered the value of security in their directives and encouragements, it would be highly speculative to assume that the innovators of optical smoke detectors considered this exact value in the design process as well. However, chapter 9 of this dissertation will show that designing the value of security into novel technologies is an excellent way for companies and research facilities to live up to their specific moral responsibilities within the web of prevention and in accordance with the NMH principle.

The design and development of optical smoke sensing technologies contributed to effective and ethically sustainable counter-measures against the acquisition of americium for illegal purposes and did so whether this was explicitly intended or not. However, it is important to note that this replacement of ionizing smoke detectors for private customers with optical detectors can only be observed in some countries of the European Union. In other Western countries such as the USA, ionizing smoke detectors are still being sold without any restrictions and are considered the gold standard in smoke detection technologies. Optical smoke detectors are available on the US market as well, but the United States Fire Administration (USFA) recommends installing both ionizing and optical smoke detectors in private homes. The reason for this recommendation lies in the USFA risk assessment of smoke detecting technologies that states that

Ionization smoke alarms tend to respond faster to the smoke produced by flaming fires than photoelectric smoke alarms [while] [p]hotoelectric smoke alarms tend to respond faster to

the smoke produced by smoldering fires than ionization smoke alarms (U.S. Fire Administration, 2020).

This example shows that national and international risk assessments concerning ionizing smoke detectors, such as those of the IAEA and the European Union, might come to very different conclusions. Here, a harmonization of assessments on an international level, as called for by the IAEA, would help to close security gaps in the web of prevention against americium-based RDDs. Chapter 9 will discuss this point in some detail.

## **8. Denying terrorists access to the knowledge to use common-use toxins as weapons**

### **1. Introduction**

Denying terrorists the opportunity to acquire the expertise to prepare attacks using common-use toxins is a particular challenge for the stakeholders in the web of prevention. Among the different groups of stakeholders, security agencies and internet companies, in particular, are involved in combating the distribution of knowledge on how to assemble toxic weapons. However, the users of websites and social media platforms are also morally responsible and, at least in some cases, involved in preventing terrorists from getting their hands on the information they need in order to prepare attacks.

In this chapter, selected cooperation between different groups of stakeholders will be described and, subsequently, evaluated based on the respective responsibilities of the stakeholders involved. Specifically, I will describe existing cooperation between security agencies and internet companies, as well as with internet users, in order to combat the distribution of knowledge of how to assemble toxin-based weaponry. Yet, as seen in this chapter, many of the existing measures can hardly be described as cooperation but are rather the efforts of one stakeholder group only (e.g., security agencies, researchers, or internet users) and lack the participation or support of the other stakeholder groups. The inability of the stakeholder



groups to recognize their moral responsibilities with regard to these counter-measures will be the main point of the evaluation undertaken in this chapter.

A detailed description of all facets of global counter-measures against the distribution of terrorist expertise would clearly be beyond the scope of this chapter. Rather, three counter-measures of different stakeholder groups were selected and will be discussed as illustrative of a systemic problem in current cooperative measures to deny terrorists access to expertise. However, all three measures will be discussed only with regard to one of the three substances that are the focus of this thesis. Hence, the first section of this chapter will concern the efforts of internet users to deny terrorists access to knowledge concerning ricin manufacturing. The second section discusses the role of security agencies and corporations in combatting the distribution of phosphine manuals. The last section of this chapter will discuss the role and responsibilities of researchers in combatting the attempts of terrorists to get insights into RDD manufacturing and, in doing so, will consider the content of this thesis as potentially illustrative of this issue.

## 2. The case of ricin and Wikipedia

Since its launch in the year 2001, the online encyclopedia “Wikipedia” has been compiling a vast amount of knowledge in over 51 million articles in 309 languages (Wikipedia, 2019b). In contrast to traditional encyclopedias, Wikipedia is not an edited lexicon authored by a limited team of experts but relies solely on the input of its more than 315,000 users. Hence, every single Wikipedia entry is written and edited by multiple users and can, potentially,

be changed and adjusted by any user of the website. According to some experts and proponents of the website, this unique approach enables Wikipedia to tap into a so-called “collective intelligence” of all its users (Lévy & Bononno, 1997; Malone et al., 2009). Rather than relying on the expertise of a limited amount of expert authors, Wikipedia articles can be improved by anyone who is knowledgeable to some degree in respect of the particular topic of the article.

In addition to general criticism of the efficacy of this collective intelligence approach, the openness of Wikipedia poses certain security risks with regard to terrorism. Specifically, and for the present study most relevantly, Wikipedia offers a platform for potential terrorists to acquire the expertise that is necessary in order to prepare attacks using common-use toxins. Hence, the administrators and users of Wikipedia (unintentionally) provide terrorists with, at least, some means to harm society. This section describes the current approach of Wikipedia and its users to discharge their moral responsibilities under the NMH principle. In doing so, this section will use the Wikipedia article for ricin as an example (Wikipedia, 2020a).

First of all, it is important to note that the current version of the Wikipedia entry about ricin does not include any information about the extraction process of ricin from castor beans. Yet, an earlier version of the same article from 2006 included two chapters called “Toxicity and manufacture” and “Ricin extraction process” that contained instructions on how to extract and purify ricin from castor beans. In this regard, especially the chapter “Ricin extraction process” is somewhat detailed and might, in fact, provide malicious individuals with some insights into the manufacturing process of

ricin from castor beans.<sup>85</sup> However, on 5 January 2007, the Wikipedia user with the pseudonym “Beetstra” edited this chapter and removed all relevant details from the part about the extraction process. In the place of these details, the user added the following paragraph:

### **Patent**

The process for creating ricin is well-known, in part because a patent was granted for it in 1952. The inventors named in U.S. Patent 3,060,165 (granted October 23, 1962) "Preparation of Toxic Ricin", assigned to the U.S. Secretary of the Army, are Harry L. Craig, O.H. Alderks, Alsoph H. Corwin, Sally H. Dieke, and Charlotte Karel. The patent was removed from the United States Patent and Trademark Office (USPTO) database sometime in 2004, but is still available online through international patent databases. Modern theories of protein chemistry cast doubt on the effectiveness of the methods disclosed in the patent.

### **Extraction process**

The extraction method described in the patent[citation needed] is very similar to the preparation of soy protein isolates. Modern extraction plants might use membrane filtration to make highly purified ricin isolates (Wikipedia, 2007).

In this passage, it is clear that the user “Beetstra” chose to refer to published sources (such as the patent of ricin extraction) instead of giving his or her

---

<sup>85</sup> The author refrains from quoting this specific passage in this version of the Wikipedia article in order not to provide a detailed account of ricin manufacturing.

own account of this process in the article. In this way, the user balanced their commitment to giving as much information as possible against their concern that a too detailed account could provide others with the means to do great harm. In later versions of this article, the above-quoted phrase was edited again and, subsequently, removed altogether. It is essential to note that, in 2007, the user edited the Wikipedia article only after a vivid discussion with other users in the “Talk” section of the article. Every Wikipedia article includes a tab that is dedicated to propose changes or discuss edits with other Wikipedia users before conducting them. For the present study, the discussion that preceded the changes conducted by “Beetstra” is of relevance.

Yet, before analyzing this discussion of the Wikipedia users in detail, the role of Wikipedia as an institution has to be mentioned. It is essential to note that the Wikimedia Foundation (the institution behind Wikipedia) strongly opposes any legal and moral responsibility for any possible use of the content on the website. Specifically, the owners of Wikipedia state that “Wikipedia is generally not censored by the editors (...) [.] The editors of Wikipedia decide by community consensus as to what content is added” (Wikipedia, 2020c). Further, Wikipedia includes a disclaimer that specifically states

None of the authors, contributors, administrators, vandals, or anyone else connected with Wikipedia, in any way whatsoever, can be responsible for your use of the information contained in or linked from these web pages (Wikipedia, 2020b).

On a more general level, Wikipedia expresses its openness with regard to content by excluding its content from all standards of secrecy imposed by organizations and countries. In a statement called “What Wikipedia is not” the team of the website writes

Some organizations' rules or traditions call for secrecy with regard to certain information about them. Such restrictions do not apply to Wikipedia, because Wikipedia is not a member of those organizations; thus Wikipedia will not remove such information from articles if it is otherwise encyclopedic (Wikipedia, 2021).

All these quoted passages show in a clear manner that Wikipedia, as an institution, is not accepting any legal or moral responsibility for its content. Rather, the founders of the platform stress that, in their opinion, neither Wikipedia as a platform nor its authors possess any responsibility concerning the use of the information that Wikipedia provides. Hence, according to the information given on the Wikipedia website, neither the platform nor its authors can be made responsible for the malicious use of any information on Wikipedia.

In the last quote, the initiators of Wikipedia go even further and stress that Wikipedia does not feel obligated to remove information that might be considered classified or sensitive to “[s]ome organization’s rules.” Here, one could understand this remark to include information that might be regarded as sensitive with regard to national security by law enforcement and intelligence organizations. Hence, when it comes to providing malicious agents with the knowledge to do large-scale harm, Wikipedia (as an

organization) is not aware (or does not accept) its responsibility according to the NMH principle. Rather, the initiators of the platform argue for the freedom of all knowledge regardless of its possible, malicious consequences.

However, while security concerns might not be a reason for Wikipedia (as an organization) to change or delete an article, the rules of the encyclopedia rule out weapon manufacturing manuals for other reasons. In the article “What Wikipedia is not,” the initiators of the platform state that

(...) Wikipedia is an encyclopedic reference, not an instruction manual, guidebook, or textbook (...). While Wikipedia has descriptions of people, places and things, an article should not read like a "how-to" style owner's manual, cookbook, advice column (legal, medical or otherwise) or suggestion box. This includes tutorials, instruction manuals, game guides, and recipes. Describing to the reader how people or things use or do something is encyclopedic; instructing the reader in the imperative mood about how to use or do something is not. Such guides may be welcome at Wikibooks instead (Wikipedia, 2021).

This quote illustrates that the guidelines of Wikipedia might, in fact, prohibit weapon manufacturing manuals on the website. Yet, the deletion of such manuals would only happen on the grounds of the website’s policy of excluding manuals, guides, and recipes. Security concerns do not play any role in this process.

Contrary to Wikipedia, as an organization, some users of the websites recognize their moral responsibility with regard to weapon manufacturing manuals to some degree. This awareness shows in the discussion board of the “Ricin” article on Wikipedia. In 2006, the user Hqduong opened a thread with the title “Isn’t this dangerous” and raised the following point: “Should we be giving instructions online on how to extract Ricin? I don’t [know] the policies on Wikipedia is on this... But The instructions [sic] here a little too detailed in my opinion.” (Wikipedia, 2007, 2019a). Note that by the time of publishing this comment, a detailed chapter about the extraction process of ricin was part of the Wikipedia article. Other users shared Hqduong’s concern. For example, a user with the pseudonym BluePlatypus referred to the Wikipedia policies in this connection:

Regardless of terrorist concerns, the exact details of how to produce it is irrelevant to an encyclopedic article. It's non-notable and/or outside the scope of relevancy. By comparison, if I look up Chocolate brownie or Plum pudding or some other food dish, it doesn't give a recipe for it, does it? (Wikipedia, 2007, 2019a).

Later on in the discussion, BluePlatypus specified this argument and stated, “It’s unencyclopedic. Whether it’s public information or not is irrelevant” (Wikipedia, 2007, 2019a). Other users agree with this point. For example, a user with the pseudonym ClockworkSoul writes, “It does seem odd, though, that we won’t keep a recipe for biscuits, but we’ll keep one for ricin” (Wikipedia, 2007, 2019a).

Furthermore, users, such as ClockworkSoul, raised specific security concerns and verbalized, at least implicitly, the moral responsibility of Wikipedia and its users with regard to providing terrorists with the knowledge to do great harm. Specifically, the user writes:

[W]e must consider the ramifications in terms of publicity should some nut actually create the stuff (it wouldn't be the first time), and investigators discovered that the source of the recipe [sic] was Wikipedia. Considering that our listings find such a high priority on Google would make this article very tempting in that regard (Wikipedia, 2007, 2019a).

While ClockworkSoul stresses the dangers to Wikipedia's public image, other users refer to matters of moral responsibility even more explicitly. For example, the user Kmaguir raised the point: "If extracting it is, in and of itself, a crime, Wikipedia shouldn't link people to an image that shows them how to extract it. It's not something to "play" with--it's a dangerous substance." (Wikipedia, 2007, 2019a). Note that the user uses the name "Wikipedia" not as an organization but as a conglomerate of its users. Hence, ClockworkSoul suggests the self-censorship of the article's authors with regard to the ricin extraction process.

Yet, it has to be noted that some participants in this discussion board formulated arguments in favor of keeping the chapter on ricin manufacturing. Most of these arguments were based on the belief that this information is public knowledge and available on other websites as well. An anonymous user, for example, stated: "It is readily available on the internet



and in books” (Wikipedia, 2007, 2019a). A user with the pseudonym Fangz gives a more detailed argument and writes:

[K]nowing about the extraction process is very relevant and useful, if you want to learn about Ricin itself. Case in point - when we hear about ricin plots being foiled, it would be useful to learn of what materials or evidence may be present. If we don't include this information for ricin, we might as well pare down the nuclear bomb article to 'it makes big booms'. It's public information. Being scared about negative publicity from a hypothetical event is silly (Wikipedia, 2007, 2019a).

Clearly, Fangz defends the principle of freedom of information in this argument. However, as seen above, other users identified the boundaries of this principle by raising awareness of the moral obligations of Wikipedia authors with regard to security. Although not explicitly mentioned, especially users like Kmaguir, at least implicitly, refer to the NMH principle by stressing that Wikipedia authors shouldn't provide people with manuals on how to manufacture such dangerous substances. Apparently, arguments like this one prevailed in the present discussion and, ultimately, led the user Beetstra to delete the chapter on ricin extraction in 2006.

For our present analysis of collective responsibilities in the fight against terrorist attacks using ricin, there are some essential points to make based on this discussion of Wikipedia users. First of all, it is clear that in this discussion, some Wikipedia users (and, for that matter, authors) are aware of their responsibilities concerning knowledge with security implications. Although not explicitly formulating these responsibilities in the form of the

NMH principle, the Wikipedia community decided in case of the ricin article in favor of a kind of self-censorship in order to avoid providing malicious agents with the knowledge to do harm.

Secondly, the quoted passages from this discussion showed that the Wikipedia users unsuccessfully sought to justify their decision in favor of self-censorship by referring to the content-related rules of the Wikipedia foundation or by referring to restrictions or recommendations from security institutions. For example, the user Hqduong expressed at the beginning of the discussion: “I don’t [know] the policies on Wikipedia is [sic] on this.” Furthermore, it remains unclear to the participants of the discussion whether manufacturing ricin is, in fact, a crime according to some national legislation. The user Kmaguir raised this insecurity by starting his remark with the phrase, “If extracting it is [sic], in and of itself, a crime.”

Hence, while the internet users acknowledge their moral responsibilities in this case, they have not been provided with guidelines identifying their responsibilities and arguments in favor of these guidelines from the owners of the website and from the security institutions. As seen above, Wikipedia, as an organization, does not acknowledge its responsibilities in this regard. Rather, it shifts all responsibilities onto its users. Furthermore, the users in the discussion could not find any guidelines from national security institutions on how to behave with regard to publishing or sharing these kinds of manuals. Hence, these institutions currently lack the ability to raise awareness and formulate clear rules for internet users in this regard. While one party in this web of responsibilities, namely the users, have many members who identify their moral responsibilities and act accordingly, the

other parties (i.e., the owners of Wikipedia and the security agencies) fail to communicate and cooperate in a way that enables all stakeholders to live up to these responsibilities.

### 3. The case of phosphine and the Europol Internet Referral Unit (IRU)

Because of the important role of manuals and online instructions in sharing technical knowledge among terrorist groups, law enforcement and intelligence agencies are concentrating some of their counter-terrorism efforts on denying potential terrorists access to these manuals. For example, the European police agency Europol set up an Internet Referral Unit (IRU) as part of its European Counter Terrorism Centre (ECTC) in 2015 (Europol, 2015). This unit is one of those responsible for monitoring and removing terrorist propaganda content as well as weapon manufacturing manuals from the internet. According to its first-year report, the IRU flagged and asked for the deletion of 8949 pieces of web content by European internet service providers in its first operational year alone (Europol, 2016). The national law enforcement agencies of several (former) European member states, including Germany and the United Kingdom, have similar units for the monitoring and deletion of relevant terrorist content on the internet, including weapon manufacturing manuals. One example of these units is the German Joint Internet Centre (GIZ) which functions as a hub of German law enforcement and intelligence agencies (Bundesamt für Verfassungsschutz, 2017b). According to journalistic sources, the GIZ reported 5,500 pieces of

relevant content to internet service providers and asked for their removal in 2016 (Haensgen, 2017).

Although there are no specific numbers of chemical or radiological weapon manufacturing manuals flagged for deletion by the IRU or GIZ, it can be concluded that the European Union and its member states actively attempt to prevent terrorists from gaining relevant expertise concerning these weapons by removing online manuals and other relevant web content. However, the absence of specific statistics concerning the deleted materials, as well as too little available information on the criteria these agencies recommend in relation to the deletion of online manuals and other materials, makes it nearly impossible to fully judge the efficacy of these counter-terrorism measures.

Yet, the deletion of potentially dangerous content on the internet cannot be conducted by security agencies alone. Since this content is posted and uploaded onto the servers of social media companies and other internet-based businesses, agencies like Europol have to contact said companies and ask them to delete specific pieces of content (such as weapon manuals) from their servers (Europol, 2015, 2016). This need for cooperation in denying terrorists access to dangerous knowledge is a good example of an existing web of prevention against terrorist attacks using common-use toxins. The two relevant stakeholder groups in this web are security agencies as well as social media and internet-based companies. According to the official outline of the IRU, this team of analysts at Europol search the most relevant websites (such as Facebook, Twitter, etc.) for extremist content and terrorism-related posts. Once such a post is found and judged to be of

terrorism-related nature, the IRU contacts the owner of the website to request the deletion of said content (Europol, 2015, 2016). Since the content is stored on the servers of a private company, the analysts at IRU do not delete this content themselves but have to ask for the cooperation of the respective company in order to remove this piece of content. According to the IRU, almost all requests for deletion that have been forwarded to social media companies were accepted by these companies so far (Europol, 2016).

Although it seems that the work of the IRU (and, for that matter, the related work of the GIZ in Germany) is well-coordinated and cooperation with internet companies is efficacious, there are, at least, two issues with the current web of prevention that was described in the paragraph above. The first issue is related to the content that the IRU may or may not request to be deleted, while the second issue concerns the role of the internet companies in the web of prevention.

Issue I: Solely based on their own information material, it is unclear what kind of content relevant to weapon manufacturing IRU's analysts request to be deleted. There are at least two criteria that the IRU might use in determining what content should be deleted:

A. The deletion of weapon manufacturing manuals that are either published by or obviously connected to terrorist groups or terrorist ideologies. These manuals show the clear intention of instructing persons to commit attacks. Examples of such content would be instructions in the terrorism-related magazines *Inspire* (al Qaeda) or *Rumiyah* (so-called Islamic State) (See Conway et al., 2017).

B. The deletion of all web content that gives instructions how to manufacture toxic weapons, irrespective of the intention behind the publication of this content. Examples of such content would include hobby manuals, entries in forums of weapon enthusiasts or so-called citizen scientists, etc.

Criterion A is almost certainly used by agencies such as Europol and GIZ in the determination of materials that should be deleted. Next to the fact that these kinds of manuals are usually embedded in illegal propaganda materials, the instruction to building chemical weapons (such as phosphine devices) with the obvious intention to commit violent crimes or acts of terrorism is a criminal offense in many liberal democracies. For example, in Germany, the criminal code explicitly prohibits “instructions to commit a serious, subversive crime.”<sup>86</sup> Arguably, however, materials that meet criterion B may also be among those filed for deletion by security agencies. In fact, in some liberal democracies, weapon manufacturing manuals are illegal regardless of their intentions. An example would be the German Weapon legislation that forbids the publication of instructions to assemble explosives or other lethal weapons.<sup>87</sup>

The deletion of both online materials using the above-mentioned criteria A and B poses problems of efficacy and ethics. While the deletion of materials that fall under criterion A is backed by the law (as seen above) and seems to pose only minor ethical concerns, practice of deleting content using only criterion A might not be efficacious enough to combat terrorists’ acquisition

---

<sup>86</sup> See *StGB* §91.

<sup>87</sup> See *WaffG* §40 Abs. 1.

of expertise to assemble phosphine-based weapons. First of all, the mere practice of deleting online content could be seen as useless since, as researchers have argued, a high volume of terrorist content is being distributed on the internet with a tremendous amount of speed so that it is close to impossible to deal with the problem simply by recourse to (tactical) content removal (Fisher, 2015). Rather, some authors argue, security agencies should focus on the bearers of weapon expertise in terrorist organizations such as weapon manufacturers and veterans of the Syrian civil war as well as their operational spaces, such as training camps (See e.g. J. J. F. Forest, 2008). For only if the explicit (theoretical) knowledge of manuals is combined with the tacit (experienced based) knowledge of these individuals, can terrorists acquire expertise in weapon manufacturing (Kenney, 2010; Mueller & Stewart, 2015, pp. 180–181).

Yet this general critique can be countered by three arguments. First of all, one should note that online weapon manufacturing manuals represent only a fraction of the relevant online content that is being filed for deletion by security agencies. Arguably, the quantum of specific weapon manufacturing manuals could, in contrast to, e.g., general Jihadi propaganda materials, be dealt with by constantly removing (albeit not definitively deleting) these pieces of content. As a complementary measure to actions targeted at bearers of tacit knowledge, this may help to make it harder (albeit not impossible) for terrorist groups to gain expertise at lower (ethical) costs than, for example, the destruction of training facilities or the arrest of suspected bomb manufacturers. Furthermore, there are instances in which lone wolf terrorists acquired the technical expertise to build weapons, such as IEDs, exclusively via the internet without having access to tacit

knowledge. Anders Breivik would be such an example (See diary part of Breivik, 2011). Finally, ethicists like Raphael Cohen-Almagor have argued that the policing of the world wide web, as well as the preservation of moral values on the internet, should be seen as a collective moral responsibility of governments, industries, and users in general (Cohen-Almagor, 2015).

A second, specific problem with the efficacy of the deletion practices by using only criterion A is more telling: As shown in this thesis, terrorists have not only been using manuals of terrorist groups to get insights into weapon technologies. The terrorist Ayman Al-Zawahiri retrieved valuable information from biomedical journals and the right-wing terrorist, Anders Breivik, appears only to have used legal online sources to acquire basic knowledge on how to assemble chemical and radiological devices. The latter example is well documented in Breivik's manifesto *2083 – A European Declaration of Independence*. In a detailed section on the possibilities of acquiring and assembling RDDs, Breivik mentions several sources that he apparently used to acquire the expertise expressed in this section. These sources include the U.S. Department of Energy, a "government security overview," (Breivik, 2011, p. not specified) the U.S. Nuclear Regulatory Commission, press coverage of the Goiania incident in Brazil<sup>88</sup>, and the IAEA (Breivik, 2011). Clearly, all of these mentioned sources do not belong to material that security agencies would delete in accordance with criterion A.

---

<sup>88</sup> During this incidents, villagers in Brazil were exposed to Caesium-137 that originated from abandoned medical facilities close to the village of Goiania (See International Atomic Energy Agency, 1998).



Because of these obvious drawbacks with only using criterion A, security agencies may consider opening up their deletion criteria to also include some or even all those sources that fall under criterion B, i.e., all online sources that give insights into how to manufacture chemical weapons regardless of the intentions behind these sources. Using this approach would have the advantage that terrorists like Anders Behring Breivik would be more effectively prevented from retrieving the information they need to build chemical or radiological devices.

However, this approach would run into problems as well, albeit different ones. First of all, the use of criterion B generates a theoretical problem since this criterion applies to documents that are too heterogeneous to be lumped together. This criterion would, at the one extreme, entail documents with ambiguous but suspected terrorist intentions such as *Assorted Nasties*, which never mentions any ideological or violent propaganda (and hence is openly available on Amazon in some countries) but was repeatedly associated with white supremacist groups. As seen above, these manuals would be illegal in some countries regardless of a connection to terrorism. Thus far, the deletion of this kind of content does not seem to be a problematic issue.

At the other extreme, however, criterion B would also include sources such as Wikipedia articles and governmental websites that do not present full manuals but inform about (the dangers of) chemical weapons in a detailed manner and, thereby, help terrorists to gain substantial expertise as the example of Anders Breivik showed. These sources do not have any affiliation with terrorism, and some of them, in fact, try to counter these

crimes by informing the public about the dangers of chemical terrorism. Thus, for security agencies, it would be a difficult task to agree upon a way to define criterion B – narrowly so as only to include books like *Assorted Nasties* or broadly so as to include the (legal) sources that terrorists like Breivik, in fact, used.

However, this problem of focus is not the only issue that security agencies would face with criterion B. Using this criterion in their online content flagging practices would certainly be more efficacious than relying only on criterion A. However, the deletion of information covered under the broad definition of criterion B would come at a high cost. First of all, it would take significant amounts of financial and personal resources to search for and flag content in line with this broad definition since potentially every website could contain bits and pieces of information that would help terrorists to gain expertise in the field of chemical and phosphine-based weapons. Even with large amounts of resources, this approach seems to be an impossible endeavor.

Additionally, such a practice would be ethically troubling. As web activists and researchers alike have pointed out, the deletion of web content without clear terrorist intentions could be seen as troubling in liberal democracies since it could lead to web censorship as practiced in authoritarian regimes (Mihr, 2017, p. 48; Ryan, 2007). For example, descriptions on educational websites or hobby forums regarding chemical weapon precursors could be – and are – seen as protected by the value of freedom of information that is a human right under international law (See for general discussion Mendel, 2003). However, if so, the value of freedom of information conflicts with

matters of national security and, more generally, with the ethical principle of NMH.<sup>89</sup>

Issue II: The second issue that has to be discussed with regard to the work of the IRU in the web of prevention is the relationship of the unit to corporations such as influential social media companies. As already shown in some detail in the second part of this thesis, security agencies and social media companies share a moral responsibility to combat the distribution of terrorism-related content on the internet. Yet, the work of the IRU does not address the moral obligations of these companies. The analysts in this unit search websites, such as Twitter and Facebook, for extremist content and other content that is relevant with regard to counter-terrorism. Once they find such content, they contact the respective company in order to request the deletion of this content from the servers of this company.

It is clear that, based on the NMH principle, companies like Twitter and Facebook possess a moral obligation to fulfill this request and, in fact, delete this content. However, I argue that, as part of the web of prevention, these companies should participate to a greater extent in measures to deny terrorists access to knowledge to manufacture weapons with toxins.

The example of phosphine will illustrate this claim. As shown in part I of this thesis, the self-proclaimed Islamic State experimented with and tested the use of phosphine as a weapon in Syria and Iraq in 2018 and 2019. Hence, this chemical, and the manuals on how to weaponize it, are of great relevance to counter-terrorism measures. However, obviously, social media

---

<sup>89</sup> This issue was discussed in the previous section of this chapter.

companies, such as Twitter and Facebook, cannot be expected to know about the security-related relevance of phosphine. It is not a moral obligation of these companies to identify trends and novel threats with regard to terrorism. This task is one of the responsibilities that security agencies, such as Europol, have in the overall context of the web of prevention. Yet, once a new threat or trend is identified and analyzed by a security institution, social media companies should actively participate in identifying and removing online content on their servers that is implicated in this threat.

For example, if Europol analysts identify phosphine as a possible security threat, Facebook and Twitter are obligated to work together with analysts at Europol in order to remove or mitigate that threat.<sup>90</sup> Since employees of these companies have great abilities to efficiently search for and delete specific content on the servers of these companies, this part of this specific counter-terrorism measure should be, at least partially, the task of these employees. In comparison, the current situation in which Europol analysts are searching the openly available parts of these social media websites for relevant content and, subsequently, requesting the deletion of said content is much less efficacious. Furthermore, the current way the IRU is working does not include the owners of social media sites to the extent that is sufficient for them to fulfill their responsibilities in accordance with the NMH principle.

In summary, it has been shown that the current arrangement in which Europol's IRU searches for terrorism-related content on the internet and

---

<sup>90</sup> See chapter 10 of this thesis for discussion.

requests the deletion of this content does not accommodate the moral obligations of the owners of the websites on which this content is to be found. The owners of social media websites do not actively cooperate with security agencies to combat the worldwide distribution among terrorists of ‘dangerous’ knowledge.<sup>91</sup> These companies do not fulfill their obligations in the web of prevention despite the fact that they have the best capabilities to search for and delete specific content if provided with clear instructions on what to search for by security agencies such as Europol.

#### 4. The case of americium and this dissertation

Another fragment of the web of collective responsibility that pertains to publishing dangerous knowledge that might assist terrorists concerns the role of the researcher. Yet, this chapter shall not discuss the role of scientists that are involved in the manufacturing or research and development of toxic and radiological products. Rather, the role of researchers in the field of terrorism studies and the present Ph.D. thesis, in particular, will be the focus of attention in this section.

As already discussed in some detail in the present thesis, substances like americium do not offer terrorists the opportunity to physically harm a very large number of individuals, i.e., they are not literally weapons of mass destruction as, for instance, nuclear weapons are. However, using radioactive substances such as americium in an improvised weapon would

---

<sup>91</sup> See chapter 10 for a definition of “dangerous knowledge.

inflict wide-spread fear and confusion in the target population. This and other aspects of what I call “soft damage” might be even more useful to the perpetrators than a large number of deaths or physical injuries. Such weapons and their capacity to do soft damage make them potentially very useful to terrorists. Indeed this claim is one of the most important points that I make in this thesis. Knowledge of the destructive power of soft damage enables security analysts and researchers to adjust their threat assessments in a manner that includes substances that were ruled out in prior assessments because of their low physical impact. Americium is a case in point here.

However, the advantage that this thesis might hold for counter-terrorism analysts has a downside. One could argue that the detailed description of the relevance of americium for the terrorist agenda could provide terrorists with the knowledge that they need in order to do large-scale soft damage. Let us suppose that a terrorist cell is not aware of the advantages that soft damage holds for their endeavor. Reading this Ph.D. thesis might provide them with the necessary understanding of the importance of soft damage as well as with a readily available weapon (an americium-based RDD) in order to inflict such damage. In this case, the present study and its author would have certainly provided malicious agents with the means to do large-scale harm to society. Hence, as a stakeholder in the above-formulated web of prevention, it seems like the author would have violated the NMH and failed to live up to his responsibilities.

One obvious way to meet the moral responsibility imposed by the NMH principle would be self-censorship. In order to comply with the moral principle in question, one could exclude any discussion of the dangers of

soft damage from the present Ph.D. thesis, or one could choose to restrict access to certain parts of this thesis to counter-terrorism professionals only. While the first option is arguably disproportionate considering the possible dangers evolving out of these text passages, the second option seems to be a suitable solution to comply with the NMH principle. By making this analysis available to researchers and professionals in the field of counter-terrorism only, the probability that potential terrorists could access and use the relevant content of this thesis in order to acquire the expertise to do harm would be significantly lowered. Hence, restricting access to this thesis and other comparable pieces of research would count as meeting the responsibility of due care on the part of the authors. Yet, there are, at least, two arguments why restricting access to all studies discussing soft damage of improvised weapons might not be necessary by the lights of the NMH principle. In fact, restricting access to these studies might, in fact, hurt counter-terrorism efforts, as the following passage outlines.

First of all, it is clear from the communication between and the manifests of terrorists that the potentially massive effects of soft damage are already known to them. For example, the terrorist Anders Behring Breivik notes the power of soft damage specifically with regard to radiological terrorism in his manifesto “2083”. In this quote, which was already discussed in chapter 3 in some detail, Breivik stresses the psychological and economic impact of RDDs while acknowledging that their physical impact is very limited. A similar awareness of the devastating soft impact of RDD attacks is visible in the document “Nuclear Pollution” of al Qaeda affiliates. Here, the authors stress that “(...) the government will close that area and everything around” (Ranstorp & Normark, 2009, p. 57) ground zero of an RDD attack.

Furthermore, they claim that “(b)y this, you cause a large economic crisis to this country.” (Ranstorp & Normark, 2009, p. 57). All of these quotes in documents of terrorists show that terrorists are well aware of the soft damage that an RDD is capable of inflicting. Hence, self-censorship with regard to discussing the effects of soft damage in studies like the present one is not necessary since the terrorist community already seems aware of the potential utility to them of soft damage.

Yet, one could argue that the discussion of specific means to inflict this damage with ricin, phosphine, and americium, as discussed in this thesis, might give a terrorist novel and innovative ways to inflict soft damage. However, a close look at historical incidents and publications of security analysts shows that all three substances have already been used or, at least, considered as weapons by terrorist groups in the past and seem to be well-known substances in the terrorist community.<sup>92</sup> Hence, the only piece of novel information that potential terrorists could gain from this Ph.D. thesis would be the destructiveness of possible weaponization of these substances in terms of soft damage. Hence, to a terrorist, the novel or innovative aspect of this thesis would clearly lie in the research and counter-terrorism community’s underestimate of the effect of soft damage.

Moreover, self-censorship with regard to this effect of soft damage would be not only unnecessary but also potentially harmful. For the academic discussion of the mechanisms of soft damage such as widespread fear helps

---

<sup>92</sup> See chapter 3 of this thesis. Obviously, this openness with regard to the terrorist use of these substances ought to have limits. Hence, I refrained from giving details into the manufacturing process of ricin and I decided to leave out any description of the extraction of americium from ionizing smoke detectors. Finally, I left out specific manufacturing steps of phosphine-based weaponry as described in terrorist manuals.



to defuse this damage to some degree. Studies like the present one raise awareness concerning the dangers of attacks that inflict soft damage and provide researchers, counter-terrorism specialists, and citizens with essential knowledge of this concept. Thereby, academic discussions of soft damage such as psychological or economic damage can help to reduce that damage in the aftermath of an attack. For only if citizens are aware of the mechanisms behind the irrational element of fear in an RDD attack, widespread panic can be prevented in the aftermath of such an attack.

In the same line of reasoning, discussions like this Ph.D. thesis can, at least potentially, prevent economic damage after an attack with an RDD. Raising awareness of phenomena like radiophobia and the limited physical impact of RDDs is a means to reduce the economic impact of these attacks as well. Finally, the effect that the present thesis could have in terms of diminishing the soft damage inflicted by CBRN attacks, in general, would obviously also include the soft damage inflicted by attacks using ricin, phosphine, and americium. Furthermore, this thesis has shown at lengths that the impact of attacks using these substances consists almost exclusively of soft damage. Hence, raising awareness of soft damage and its effect on the public is also a means to substantially reduce the attractiveness of ricin, phosphine, and americium to terrorists.

To sum up, it has been shown that researchers who discuss the dangers of RDD attacks currently do not self-censor these discussions in order not to provide terrorists with the means to harm others via soft damage caused by weaponized phosphine, ricin, or americium. Yet, it was also argued that such self-censorship on behalf of the researchers is not necessary.

Furthermore, it was shown that academic discussions of the nature of soft damage are, in fact, able to help to minimize that damage in the aftermath of an attack. Hence, researchers who dedicate their work to this topic fulfill their moral responsibilities in accordance with the NMH principle. However, in a second step, these researchers ought to publish this work and make serious attempts to make it available to the other groups of stakeholders in the web of prevention.

# **Part IV:**

## **The web of prevention**

## **9. A web to prevent the acquisition of dangerous substances**

### **1. Introduction**

The last chapter provided an overview of selected, cooperative measures to prevent the acquisition of ricin, phosphine, and americium for illegal or terrorist purposes. In this overview, issues of efficacy and ethical sustainability concerning these existing measures were discussed. As shown in some detail, these issues can weaken the web of prevention against the illegal use of these substances. In particular, these issues prevent effective cooperation between the different stakeholders participating in this web. Therefore, stakeholders such as companies are not able to fulfill their jointly held moral responsibilities to contribute to the prevention of illegal use of these products. Based on the discussion of these specific issues in the existing web of prevention, one can specify four points of improvement for this web. These points would not only contribute to a more efficacious counter-terrorism strategy but would also enable all stakeholders to live up to their respective joint responsibilities within the web.

Before discussing these four points of improvement in detail, it is crucial to note two prerequisites. First of all, just as in the discussion of the existing counter-measures, these points of improvement are focused on counter-measures against the acquisition of ricin, phosphine, and americium in selected countries. However, these four points of improvement do offer a

stepping stone to identify some more general, structural problems in the counter-terrorism architecture. It goes without saying that they do not provide a silver bullet for counter-terrorism in liberal democracies; rather, the aim is to provide some of the key elements in the overall CT strategy.

Secondly, all four of these points of improvement require a certain level of institutionally structured cooperation of those stakeholders who are, or should be, participating in the web of prevention. Hence, the foundation of a more efficacious and ethically justifiable collaboration in the web of prevention is the formation of a coordination center in which all relevant stakeholders can meet and communicate directly with each other. The GTAZ committee in Germany is an example of how such a coordination center could be organized. In this center, 42 Government institutions communicate and cooperate in ten working groups in order to coordinate their counter-terrorism measures.<sup>93</sup> Other countries, such as the Netherlands or the USA, have similar approaches with the National Counterterrorism Center (NCTC) or the Fusion Centers of the DHS (Van Der Veer et al., 2019).

However, most of these cooperative centers only include one of the groups of stakeholders that are necessary to form an efficacious web of prevention against the toxins in question. While different governmental institutions can communicate and cooperate closely in these centers, relevant local businesses and selected groups of citizens are excluded from participating. However, as shown in this dissertation, what is required is the participation

---

<sup>93</sup> A detailed description of the structure of the GTAZ can be found in chapter 5 of this dissertation.

and close cooperation of all of these groups of stakeholders in an efficacious and ethically sustainable web of prevention. Hence, centers that include representatives of all these stakeholder groups are needed in order to prevent the illegal use of ricin, phosphine, and americium. Only such a center would enable the stakeholders to make the necessary four improvements to the existing counter-measures. Here already existing approaches to connect a variety of stakeholders with each other to improve security strategies can provide some direction.

For example, in Germany, the German Federal Office for Civil Protection and Disaster Assistance (BBK) and the German Federal Office for Information Security (BSI) formed an initiative named Action Plan Critical Infrastructures (UP KRITIS) that helps to connect businesses with security institutions in order to improve the protection of critical infrastructure in Germany (BBK, 2019). Within this working group, the BBK, the BSI and other federal and state-level security institutions are communicating with each other, but also with relevant businesses that either operate critical infrastructure or are in different ways pertinent to the protections of these infrastructures. Amongst others, the UP KRITIS is responsible for promoting seamless communication between all stakeholders during an incident, for organizing joint exercises as well as for working on joint threat assessments (BBK, 2019).

As will be shown in this chapter, the idea of the UP KRITIS and similar approaches in other countries can be applied to the web of prevention against the illegal use of the three discussed common-use toxins. Hence, the

establishment of an institution<sup>94</sup> is necessary to strengthen the web of prevention and to improve the existing cooperative measures. The following four points of improvement require four separate branches or working groups in this institution. Therefore, addressing these four points of improvement involves establishing an institution in the form of a joint center (e.g., the Joint Center Against the Terrorist Use of Common-Use Substances). A summarizing visualization of the center with examples of joint and individual actions in the center in a German national context will be provided at the end of the thesis.

## 2. What substances are dangerous

The first point of improvement that can be extracted from the critical discussion of the current counter-measures against the acquisition of the three substances is awareness. The groups of stakeholders in the web of prevention are responsible for identifying substances of concern with regard to terrorism or have to be, at least, aware of the relevance of these substances to counter-terrorism efforts. Here the identification of the danger posed by certain substances shall be the responsibility of the security agencies as well as those corporations and companies that produce the substances in question. While security agencies possess in-depth knowledge about current trends in terrorism and weapon choices of terrorist groups,

---

<sup>94</sup> The selection which substances shall be in- or excluded from being discussed in this center can be determined by using the Terrorist Weapon Rating Scale. In accordance with the assessment performed in this dissertation, ricin, phosphine, and americium shall be discussed in particular by the members of this center.

companies that produce toxic or otherwise dangerous products are aware of the properties, the health effects, and the ease of use of these products. Only if both the threat awareness of the security agencies and the technical knowledge of the companies in question are shared and conjoined, is a realistic and efficacious threat assessment for common-use toxins possible.

In order to assess the threat posed by a certain toxic substance, direct communication between security agencies and those companies that produce said substance in accordance with established protocols is crucial. Here the joint center can help to provide a platform where these two groups of stakeholders can meet and share their respective knowledge, establish protocols and provide updates as required. However, as seen in the last chapter, especially phosphine and americium do not appear to be a priority of most national security agencies and, therefore, companies that produce products with these substances lack awareness of the possible misuse of these substances. The reason for this lack of awareness in security agencies is the fact that neither of these substances is expected to cause large amounts of hard (i.e., physical) damage. However, as chapter 3 of this dissertation showed in some detail, the impact produced by an attack with these substances is more complex than merely the kinetic or health effects. Hence, in order to assess the complexity of the threat posed by these substances, the responsible groups of stakeholders should consider using a matrix of threat analysis such as the terrorist weapon rating system presented in this thesis. This way, both security agencies and the businesses involved in the production of these substances could manage to gain deep insights into the dangers posed by certain products. While security agencies would be, for example, able to share insights into the soft impact, the tactical advantages,



and the likelihood of attacks using these products, businesses could contribute details about the hard impact, the availability, and the required expertise to make use of the products.

While security institutions and manufacturers are responsible for jointly assessing the dangers of certain products, those businesses that sell said products cannot be expected to assess the possible threats posed by every single product they sell. However, as seen in the last chapter, those companies are responsible for ensuring that they do know about the danger of the substances they sell being acquired by terrorists to conduct terrorist attacks so that they can inform security agencies about suspicious purchases (see next section). Moreover, it is the joint responsibility of the security agencies and the manufacturers of these products to share their terrorist threat assessments of the products with the vendors of the products.

However, as seen in the critical discussion in chapter 8, currently, many vendors that sell, for example, phosphine-producing products, are completely unaware of any security-related issues with these products. Again, the joint center could be of great assistance in ensuring awareness in this regard. The center would be a simple yet efficacious mechanism to share the threat assessment of certain substances with representatives of the vendors that sell products that contain these substances. As participants in the joint center, the vendors can gain valuable insights into the security-related issues of their products by means of direct communication with the authors of the threat assessment (i.e., security agencies and manufacturers). That would enable this group of stakeholders to be aware of the risks posed

by the products they sell and, thereby, to fulfill their moral responsibilities according to the NMH principle and as part of the web of prevention.

The final group of stakeholders discussed in the last chapter that ought to be participants in the joint center are the representatives of civil society, i.e., selected citizens. Arguably, it seems unreasonable to ask every citizen to have an in-depth awareness of all terrorism-related threats. Hence, and as researchers have shown, broad and unspecific calls for general vigilance concerning terrorism and suspicious behavior are neither efficacious nor ethically sustainable.<sup>95</sup>

Furthermore, it also seems unreasonable to ask every citizen in a society to have an in-depth awareness of the threats that certain substances such as phosphine pose. Rather it shall be the responsibility of the other groups of stakeholders in the joint center to identify specific groups of citizens in a society that possess societal roles that are of strategic advantage to counter-terrorism efforts. To some extent, this has already been done in some best practice examples of vigilance in the USA (with the bomb-making materials awareness (BMAP) program (Department of Homeland Security, 2018a)) and in the Netherlands (with an awareness campaign concerning chemicals with relevance to terrorism (Nationaal Coördinator Terrorismedbestrijding en Veiligheid, 2018)). Within the joint center, representatives of security agencies, manufacturers, and vendors are able to jointly identify relevant groups of citizens, such as frequent customers or employees of hardware or

---

<sup>95</sup> Journalists and researchers have repeatedly questioned the efficacy of vigilance campaign such as the “See something, say something” campaign in the USA (Department of Homeland Security, 2018b). Next to arguments that these campaigns do not help counter-terrorism efforts, some researchers also identified ethical issues with these campaigns (Gunn, 2016; Larsson, 2017; Molotch, 2014; O’Haver, 2016; Reeves, 2012).

gardening stores that are able to help efforts to detect suspicious purchases.

<sup>96</sup> The threat awareness of these groups of citizens is crucial if vendors are to fulfill vendors' moral responsibility according to the NMH principle.

However, it has to be stressed that these citizens, like customers of gardening stores, do not share the vendors' responsibility to report suspicious purchases. Hence, raising the citizen's awareness of the threat should be seen as an endeavor to optimize efforts to fulfill the vendor's moral obligation. The customers (i.e., relevant citizens) themselves are, in this case, free of any moral obligation. A hardware store customer's awareness concerning, for example, the terrorism-related threat posed by ionizing smoke detectors would be, therefore, solely the joint moral responsibility of the other groups of stakeholders (vendors, security institutions). Hence, the presence of relevant groups of citizens in the joint center's working group on suspicious purchases would only be a voluntary role without any moral obligation.

### 3. What purchase is suspicious?

Once the relevant stakeholder groups in the joint center have identified substances that are dangerous if they get into the hands of terrorists, the participants in the center shall discuss ways to deny terrorists access to these

---

<sup>96</sup> Please note that individuals that are employed by a vendor to sell the vendor's products share the collective moral responsibility to be aware of the threat according to the NMH principle. However, it is the vendor's responsibility to inform new employees about their responsibilities in this regard and to enable their awareness with trainings and flyers such as the BMAP flyer in the USA.

substances. As already discussed in the previous chapters, especially the vendors who sell these substances possess a crucial set of responsibilities here. Specifically, the vendors are morally responsible for reporting suspicious purchases of these vulnerable products to security agencies in order to avoid providing others with the means to harm society (NMH principle).

However, to successfully fulfill this moral obligation, the vendors need the other groups of stakeholders as partners in determining what kind of purchases they ought to report to security institutions. The vendors, the manufacturers, as well as the security agencies have to cooperate in defining for each relevant substance what one ought to count as a suspicious purchase of said substance. Since both the manufacturers and the relevant employees of the security institutions share in-depth knowledge concerning the possible misuses of these substances, they are both capable and responsible for determining what kind of purchases of these substances might be linked to terrorist endeavors.<sup>97</sup> However, this determination has to

---

<sup>97</sup> One current example of such a determination is the National Code of Practice for Chemicals of Security Concern of the Australian government (Australian Government, 2016). Here, security agencies both identify toxins of concern and give clear instructions to vendors what kind of behaviour is suspicious and, hence, ought to be reported. However, this Code of Practice does not include direct cooperation and ongoing communication with vendors and manufacturers within a center or other forum. Furthermore, it only functions as an encouragement for good practice rather than being a cooperative counter-terrorism measure built on a collective responsibility of the involved stakeholders. The Australian government writes specifically: “The code is based on good business practices that prevent the loss and theft of chemicals. It encourages organisations to consider and examine their own risks from a national security perspective and to take steps to reduce risks to ensure that chemicals are not stolen or diverted for terrorist purposes.” (Australian Government, 2016). Clearly, the Government only informs the vendors in this Code and does not aim to cooperate with them in a joint action against chemical terrorism. Another example of such an approach are the Chemical Sector-Specific Agency Voluntary Security Programs of the DHS in cooperation with the Chemical Sector-Specific Agency (SSA) in the USA

be undertaken in close cooperation with the vendors who sell these products in order to enable them to fulfill their responsibility and, thereby, to be a functional part of the web of prevention. The joint center, which functions as the organizational hub of this web of prevention, provides the three stakeholder groups with a forum in which they can exchange knowledge and ideas and, as a result, define what ought to count as a suspicious purchase for each relevant substance.

As already discussed in chapter 7 of this thesis, the notion of a suspicious purchase depends on the nature and uses of the substance in question and, hence, can differ from one substance to another. For example, in the case of ricin, the purchase of castor beans in combination with other products such as coffee grinders or other grinding utensils might be a reason for suspicion. Since the process of extracting ricin from castor beans entails the grinding of parts of these beans, this combination of purchases gives reason to believe that the customer intends to produce powdered ricin from the castor beans. However, since the vendors do not have (and are not expected to have) the detailed knowledge about ricin production that the security agencies possess, it seems unreasonable to expect the employees of a

---

(Department of Homeland Security, 2017). The DHS and the SSA offer digital programs to educate about the security threats in the chemical industry that were designed in cooperation with private businesses. Furthermore, they offer the Chemical Sector Security Awareness Guide in which they provide examples of suspicious behaviour with connection to the chemical industry. However, just as the Australian approach these programs are both voluntary and do not include a close and ongoing communication and cooperation between security agencies, manufacturers, and vendors. In the USA, the DHS oversees the Chemical Security Analysis Center (CSAC) that produces threat assessments with regard to toxic chemicals and the chemical industry in the United States. Yet this center does not explicitly include stakeholders other than the DHS and the scientific community with selected business partners (Department of Homeland Security, 2020) Additionally, it is important to note that neither the US Government nor the Australian government consider phosphine or americium high-risk substances in their assessments.

company that sells castor beans to identify the security-related relevance of such a combined purchase. More specifically, it is not the vendor's moral responsibility within the web of prevention to independently research the ricin manufacturing process in order to detect suspicious combinations of castor bean purchases in their stores. Rather, the other groups of stakeholders and, in this case, especially the relevant employees of the security agencies, are morally obligated to inform the vendors about the security-related relevance of the combined purchase of castor beans and grinding material.

Yet, it is not to be expected of the security agencies that they disclose to the vendor in detail what would make this purchase suspicious with regard to terrorism. Here it would be a reasonable approach for the representatives of security agencies in the joint center to discuss this matter with the vendors without disclosing too many details about the process of ricin manufacturing. Rather, a list with possible combinations of purchases that ought to be reported seems more than sufficient for the vendors in order to fulfill their responsibilities within the web of prevention. Ignorance towards the details of why this purchase ought to be regarded as suspicious would not hinder the vendors from fulfilling their part in the web.

Obviously, the combined purchase of castor beans and coffee grinders is only one of many examples of suspicious purchases related to the three substances. For example, the combined purchase of either castor beans or calcium phosphide, together with materials like acetone and hydrogen peroxide, ought to be reported as well. The combined purchases of the two substances acetone and hydrogen peroxide could be linked to the intention

to manufacture a peroxide-based explosive like triacetone triperoxide (TATP) (Cardash & Johnston, 2014; Conway et al., 2017). While this purchase itself gives reason for suspicion, the combination of these two substances with an additional toxic substance, such as calcium phosphide, would be even more alarming since it might be part of a plan to manufacture an IED-based chemical device. Since the combined use of calcium phosphide, acetone, and hydrogen peroxide for legitimate reasons is highly unlikely, it seems justified for the vendor to, at least, inform the security institutions about that purchase so that employees of the relevant institutions are able to investigate. Obviously, not every combined purchase mentioned in this section will be part of a terrorist plot. It is within the realm of possibility that a customer without malicious intentions happens to purchase a combination of products defined as suspicious by the members of the joint center.

In order to keep these false positives to a reasonably low level, all members of the joint center are expected to carefully consider the possibilities of these false-positive. Next to the value of security that is strengthened by reporting the combined purchases, the stakeholder groups ought to consider other societal values that might be harmed by reports that turn out to be false positives. For example, the value of privacy is negatively affected by reporting a certain combination of purchases to the security institutions without having any circumstantial evidence about the intentions of the customer. Here, especially the representatives of the general public in the joint center can be valuable partners in weighing the value of security against other societal values in cooperation with security agencies and security institutions. This direct communication of these stakeholder groups

in the center enables the design of a list of suspicious purchases that is sensitive towards a variety of societal values.

Obviously, not only the combined purchase of certain products but also the amount of a substance that is purchased by a customer could be considered suspicious. As seen with the example of phosphine purchases in chapter 7, certain common-use toxins, including phosphine, are only impactful terrorist weapons if deployed in large amounts.<sup>98</sup> Hence, a purchase might be considered suspicious without other combined purchases but only judged by the amount of phosphine-producing products that were purchased. In contrast to suspicious combinations of purchases, the definition of what ought to be considered a suspicious (or dangerous) amount of a certain substance is often already provided through legislation. For example, in Germany, private consumers are only allowed to purchase products that produce not more than 15 grams of phosphine without a license. Yet as seen in chapter 8, the current system to enforce this legal restriction is not working properly. Hence, the stakeholders at the joint center have to cooperate in order to find effective detection mechanisms for purchases of suspicious and illegal amounts of dangerous goods.

#### 4. How can we optimize detection mechanisms?

In order to report suspicious purchases, the vendors of dangerous goods have to possess effective mechanisms to detect these purchases. In the case

---

<sup>98</sup> See also chapter 3 for discussion.



of online vendors like Amazon, it seems fairly simple to install these mechanisms once the stakeholders agree upon what combinations and amounts of products ought to be suspicious. Since Amazon and other online vendors already document all purchases on their platform in centralized databases, these companies have the capabilities to directly search for suspicious purchases and to report them. There is, in fact, a good reason to believe that at least Amazon is already doing so in some capacity, as the case of the Cologne ricin plot has shown.

However, this system of reporting becomes somewhat more difficult with vendors that are not selling their products on the Internet. For example, it is illegal to sell substances such as calcium phosphide openly via the Internet in Germany and many other European countries.<sup>99</sup> Hence, this product is only available in selected hardware stores and farmer's supply stores. In order to be able to provide German security institutions with information about the purchases of certain dangerous goods, the relevant vendors are legally obligated to document these purchases in the so-called *Giftbuch* in Germany. Yet as already discussed in some detail in chapter 7, in many stores, this *Giftbuch* is a physical notebook that can be reviewed by local law enforcement or other security institutions if requested. This system of documenting is not sufficient to fulfill the vendor's moral responsibility to actively report suspicious purchases in accordance with the NMH principle. Furthermore, it does not prevent the purchase of an illegal amount of calcium phosphide.<sup>100</sup>

---

<sup>99</sup> See chapters 3 and 7 of this dissertation.

<sup>100</sup> See chapter 7 of this thesis for a discussion of both of these points.

In order to enable the vendors to live up to their moral responsibilities in the web of prevention and to enforce the existing legislation concerning calcium phosphide purchases, security institutions have to work closely together with vendors in the joint center. Only close cooperation of both stakeholder groups can make sure that the employees of the vendors are able to detect and, consequently, report excessive purchases of calcium phosphide.

One possible solution to the current inadequate measures would be the centralization of the *Giftbuch* in the form of a digital database. By using a cloud-based, digital documentation system, every relevant hardware store employee can check all purchases of calcium phosphide and other dangerous goods that a certain customer made in all connected stores. Equipped with this centralized documentation system, the vendors can easily deny customers excessive amounts of dangerous goods or, if necessary, directly report the customer to the German authorities. German legislators seem sympathetic to this approach since in the respective legislation, it is explicitly mentioned that the *Giftbuch* can also be present in digital form, as briefly mentioned in chapter 7 of this thesis.

Yet, it would not solve the issues with the current situation in Germany if every relevant vendor would create their own database. In order to fulfill their moral responsibilities, all relevant vendors have to agree upon an industry-wide documentation system that includes clear rules of access and use by all companies. For example, it might be important to install rules that prohibit the use of the database for business intelligence-related activities by any party involved. Furthermore, it is crucial that the database fulfills all relevant privacy and data protection standards of German and European

authorities. Lastly, it has to be determined (perhaps after consultation and discussion) whether the servers for the database should be possessed and maintained jointly by the relevant vendors or whether it should be owned by a Government institution. The joint center offers the necessary forum for the vendors to discuss these specific issues with each other and with the relevant security institutions.

The example of the centralization of the *Giftbuch* is admittedly a fairly specific case and focused on specific substances (calcium phosphide) under specific national legislation (Germany). However, it can be used as a case study to illustrate the potential of an institutionalized web of prevention involving a joint center. Only close cooperation enables the relevant groups of stakeholders to identify and close loopholes in the current measures to deny terrorists access to dangerous substances. Note that in this example, the loophole in question would not be closed by legislative measures alone but via the joint efforts of all groups of stakeholders that are morally responsible for closing it. This and other joint efforts illustrate the power of the web of prevention.

## 5. How can we replace dangerous substances and technologies?

Another focus that the stakeholder groups in the web of prevention ought to consider is the design of technologies that might enhance the web of prevention and, thereby, contribute to security. By connecting not only the members of security institutions with vendors but also with manufacturers,

citizens, and especially relevant researchers<sup>101</sup>, the joint center provides a great opportunity for discussions not only of practical institutional measures but also of the weighing of values, such as privacy and security, and indeed of potential product innovations; products that might increase the effectiveness of the web in a manner consistent with relevant societal values. This approach was already briefly discussed in chapter 8 with the example of ionizing smoke detectors. However, in this example, it was evident that, while the value of security was, indeed, positively affected by the invention of the optical smoke detector, there is no evidence that the designers of this technology were actively taking this value into account in the design process. However, the concept of design for values makes these value considerations in designing new technologies explicit.<sup>102</sup>

Yet to actively design certain products for the value of security (in a manner consistent with other values, including privacy and free and fair markets), manufacturers have to, first of all, identify potential products and product domains (e.g., pesticides) in which innovation for security might be fruitful or even necessary. Here, again the joint center can be of help as a forum. Following the NMH principle, it is the joint responsibility of security institutions and manufacturers and designers of products to discuss the security-related relevance of new and existing products in the joint center with a focus on counter-terrorism. Specifically, the relevant stakeholders ought to identify cooperatively which domains of products (e.g., pesticides)

---

<sup>101</sup> For the moral responsibilities of researchers in the web of prevention, see chapters 5, 6, and 8.

<sup>102</sup> Please note that the research on design for values and value sensitive design is too extensive to be summarized in this section. Rather, this chapter will be deploy an applied, general notion of design for security in order to add to the possible measures that ought to be discussed within the web of prevention.

have relevance to counter-terrorism efforts. Subsequently, all members of the joint center ought to discuss the value of security in combination with other societal values that might be (negatively) affected by designing certain products for security.<sup>103</sup> Examples of such value conflicts would be the conflict between security and privacy (e.g., in reporting suspicious purchases) or the conflict between security and safety (e.g., in prohibiting efficient ionizing smoke detectors without having a comparably efficient alternative technology).

However, it cannot be expected that security agencies and manufacturers can usefully discuss these complex ethical issues without assistance from relevant experts. The joint center itself ought to be designed and organized in a value-sensitive way to account for the complexity of value debates between security and other societal values (For a general discussion, see Miller, 2015). In addition to members of security institutions, manufacturers, vendors, and representatives of citizens, researchers in the fields of applied ethics and social sciences ought to, at least, participate in the Centre in an advisory capacity. As seen above, societal values such as privacy, autonomy, safety, and security play pivotal roles in the debates of the groups in the joint center. Hence, competence in applied ethics is needed to steer and moderate these debates.

Equipped with the expertise of all these groups, the stakeholder groups in the joint center can, subsequently, decide in which way an existing technology or substance ought to be changed or even replaced by a novel

---

<sup>103</sup> For general discussions on value conflicts, see debates in the ethics of technology (Grunwald, 2015; Miller, 2015; van den Hoven et al., 2015).

innovation in order to account for the value of security. An interesting example of how such a process might look like in practice is the case of ammonium nitrate.

In addition to restricting the access to ammonium nitrate fertilizers by means of regulations, European legislators also make efforts, in cooperation with manufacturers, to bring about changes in the composition of these substances in order to make them unattractive for terrorists.

For example, the regulation 80/876 EEC<sup>104</sup> from 1980 determined that the oil retention of AN prills should not exceed 4%. Furthermore, it prescribed that the maximum amount of combustible material in AN fertilizers should not exceed 0.2%. Here, it is clear that legislators and manufacturers embedded the values of safety and security into a process of further innovation of AN fertilizers. By increasing the density of AN prills, the substance does not soak up oils and, thereby, cannot be used to manufacture the explosive ANFO. Furthermore, non-combustible additives to the fertilizer are supposed to make the substance more stable and less prone to detonating. All these innovations were clearly inspired and driven by the societal values of safety and security.

This ongoing innovation process of AN fertilizers can be interpreted as a form of design for values and, thereby, can function as an example for many design for value approaches. For example, it fulfills three major characteristics that are part of most design for values understandings (as defined in van den Hoven et al., 2015, p. 4):

---

<sup>104</sup> Council Directive 80/876/EEC on the approximation of the laws of the Member States relating to straight ammonium nitrate fertilizers of high nitrogen content.

- (1) The designers, working cooperatively with legislators, were able to embed the values of security and safety into the design process by rendering AN fertilizers inert.
- (2) Thinking about the embedding of these values has a moral relevance in our society since it adds to the struggle to create a safe and secure society in which terrorists are not able to inflict large-scale harm.
- (3) It was possible to embed these values into the design process since security and safety risks were already known. Large-scale accidents in transporting AN fertilizers and terrorist attacks, such as the Sterling Hall Bombing (1960) (Bates, 1992) or the Oslo Bombing (2011) (Appleton, 2014), caused manufacturers to innovate the product further for the values of safety and security.<sup>105</sup>

Yet, it has to be noted that the process of rendering AN-based fertilizers inert is ongoing and by no means complete. Terrorists and other malicious actors keep finding ways to circumvent the process or to innovate in ways that enable them to use AN fertilizers as explosives. The attack of Anders Behring Breivik in this regard is the latest (and shocking) example of such efforts.<sup>106</sup> Lastly, it should be mentioned that, at least in the case of radiological threats, there are comparable proposals to design for security. For example, a recent report of the World Institute for Nuclear Security (WINS) suggests innovating in order to replace current, high-activity

---

<sup>105</sup> Note that these values did not seem to play a major role in the initial innovation of AN based fertilizers. It seems reasonable to assume that the scale of the security related dangers were not visible at the time of the invention of first AN based fertilizers. This lack of knowledge and uncertainty is known as the Collingridge dilemma in the field of Design for Values (van den Hoven et al., 2015, pp. 2–3).

<sup>106</sup> For a detailed discussion on the ways in which Breivik circumvented the AN security innovations, see the unpublished master thesis of the author (Feltès, 2015).

radioactive sources such as Cobalt in industrial and medical applications. This report, with the title “Considerations for the Adoption of Alternative Technologies to Replace High Activity Radioactive Sources” might function as a blueprint for similar efforts in the joint center (World Institute For Nuclear Security, 2017).





## **10. A web to deny terrorists access to dangerous expertise**

### **1. Introduction**

As shown in part III of this thesis, the current measures to prevent the misuse of ricin, phosphine, and americium face serious issues. The majority of these issues stem from an insufficient degree of cooperation between the stakeholders who have a moral responsibility to participate in these measures.

In addition to those measures directed at combating the acquisition of dangerous materials, measures to restrict the circulation of knowledge and expertise among terrorists are a focus of this thesis. The discussion of the current measures in this domain concluded that four issues are particularly important in current efforts to combat the distribution of knowledge of toxin weapon manufacturing: first of all, one has to discuss what kind of knowledge should be treated as dual-use knowledge in this regard. Secondly, the issue of whether it should be morally permitted to publish such knowledge has to be addressed. Thirdly, all relevant stakeholder groups have to find suitable ways to ensure that internet users are able to report ‘dangerous’ knowledge available on the internet; knowledge that enables terrorists to perpetrate terrorist attacks and which would otherwise not be available to them. Finally, it has to be discussed among the stakeholder groups what should happen to ‘dangerous knowledge available

on the internet once its existence has been reported to social media providers and/or the authorities. Should it, for instance, be removed? This raises the issue of censorship.

This chapter will address all four of these questions separately and will show that an appropriately designed ‘fit for purpose’ web of prevention is needed to address these problems. Yet, such a web of prevention needs to be institutionalized. The centerpiece of this process of institutionalization is the joint center described above. Other elements of this institutional infrastructure include laws and regulations and associated enforcement mechanisms, as well as awareness-raising programs tailored to stakeholder groups with specific roles to play in the web of prevention. The four issues that arise regarding the response to ‘dangerous’ knowledge are a matter for discussion and decision by legislators and counter-terrorism security agencies in an overall context of cooperation with social media service providers, internet users, and scholars in the field of terrorism research and ethics. The following four sections provide an overview of potential responses to ‘dangerous’ knowledge on the part of stakeholders participating in the proposed joint center; responses that are both efficacious and ethically justifiable.

## 2. What kind of knowledge is dangerous knowledge or dual-use knowledge?

The first issue the stakeholder groups have to address in the joint center is the definition of dangerous (or harmful) knowledge in connection to

terrorism with toxins. As seen in chapter 8 of this thesis, it might be extremely difficult to assess whether a social media post, a Wikipedia entry, or even a specific manual should be regarded as vulnerable to exploitation by terrorists. While weapon manuals with visible ties to extremist ideologies should obviously be regarded as dangerous knowledge, hobbyist videos on Youtube or Wikipedia entries such as the one on ricin might have been written without any intention to harm others. Yet, these videos and entries can be used by third parties (i.e., terrorists) to create weapons that produce large-scale harm. Hence, the knowledge in question can be regarded as dual-use knowledge (For general debates of the term dual-use knowledge, see Atlas, 2009; Kuhlau et al., 2013; Marchant & Pope, 2009; Marris et al., 2014; Nixdorff, 2013; Rychnovská, 2016).

Stakeholders in the joint center can quickly identify and deal with dangerous knowledge i.e., weapon manuals with clear ties to Islamist or right-wing extremism. Security institutions, such as Europol and the IRU, are already browsing the internet for these manuals and request the deletion of such content as it is illegal in most jurisdictions, including in Germany.<sup>107</sup> Other groups of stakeholders are legally obligated to comply with the requests of the authorities in this regard. However, it is unclear to what degree stakeholders such as social media providers or internet users have to participate in the counter-terrorism work of the IRU and other institutions. Sections 4 and 5 of this chapter will discuss this question.

---

<sup>107</sup> For the respective German legislation, see the German Criminal Code (*Strafgesetzbuch*), article 91.

A more pressing issue to discuss for the stakeholders in the joint center is the question of how to deal with dual-use knowledge. In contrast to the above-mentioned, dangerous documents, sources of dual-use knowledge were not produced with the intention to harm others. Rather, they were produced by authors with the intention to provide benefits to society but, potentially, could be used by terrorists and other malicious agents in order to harm society.

As already argued in earlier chapters of this thesis, it is the joint responsibility of different groups of stakeholders participating in the web of prevention to discuss what kind of knowledge ought to be considered dual-use-knowledge with regard to terrorist attacks which use ricin, phosphine, and americium. This discussion has to be led by representatives of security institutions but should also involve social media service providers as well as researchers and internet users. Especially this last group of stakeholders is a key component in the discussion concerning dual-use-content on the internet since a considerable amount of online data is produced by internet users rather than companies or academic researchers. Wikipedia is a case in point.

Internet content producers have to cooperate closely with service providers and security agencies in order to determine whether certain information qualifies as dual-use knowledge or not. As the example with the Wikipedia article on ricin showed, some internet users have already identified their obligations and have attempted to start a conversation about this issue. However, it requires the involvement of the other two groups of stakeholders if online dual-use information is to be identified efficiently and effectively.

First of all, the security agencies are a key partner in determining whether certain information is dual-use knowledge since employees of police and intelligence institutions are experts in matters of national security. With their expertise in the fields of terrorism, weapon technologies, and criminology in general, analysts of security agencies are able to identify what information could be useful to potential terrorists. However, they need the input of internet users, service providers/publishers, and researchers in the field of ethics in order to discuss the difficulties and dilemmas evolving out of the publishing (or censoring) of dual-use knowledge.

This discussion is a vital part of an ethically justifiable and efficacious counter-terrorism strategy that involves multiple groups of stakeholders. The suggested joint center would provide an institutional setting in which the required discussion could take place. However, as a starting point for a discussion concerning dual-use knowledge involving all these stakeholders, the next section of this thesis offers an argument against censorship of certain kinds of dual-use knowledge. While this argument reflects the perspective of one group of stakeholders (i.e., publishing researchers), it explicitly invites criticism and comments from the other groups in order to set a foundation for an institutionalized debate on this important matter.<sup>108</sup>

---

<sup>108</sup> Note that there already exists a vital academic debate concerning dual-use knowledge in science (Atlas, 2009; Kuhlau, Höglund, Eriksson, & Evers, 2013; Marchant & Pope, 2009; Marris, Jefferson, & Lentzos, 2014; Nixdorff, 2013; Rychnovská, 2016).

### 3. Should we publish dual-use knowledge?

The question of whether or not to publish work that contains dual-use information has been discussed in academia at great length (Kuhlau et al., 2013; Marchant & Pope, 2009; Marris et al., 2014; Miller, 2018; Rychnovská, 2016). The vast majority of academic discussions concerning dual-use knowledge aims at scientists and researchers in biotechnology, chemistry, and engineering sciences. However, as chapter 8 of this thesis showed in detail, terrorism researchers are also involved in dual-use issues. Indeed, some of the content in this thesis itself might be thought to involve dual-use issues.

As outlined in Chapter 8, one way to reflect the moral responsibility of terrorism researchers might be by way of self-censorship. In order to comply with the NMH principle, one could exclude any discussion in the present thesis of the dangers of soft damage, or one could choose to restrict access to certain parts of this thesis to counter-terrorism professionals only. While the first option is arguably disproportionate in the light of the possible dangers posed by the information in this thesis, the second option might seem at first glance to be a suitable way to comply with the NMH principle. By making this analysis available to researchers and professionals in the field of counter-terrorism only, the probability that potential terrorists could access and use these elements of this thesis in order to acquire the expertise to do harm would be significantly lowered. Hence, restricting access to this thesis and other comparable pieces of research would count as compliance with the due care responsibilities of the authors.

Yet, in chapter 8 of this thesis, I showed with the help of two arguments why restricting access to all studies discussing soft damage of improvised weapons might not be necessarily required by the NMH principle. Indeed, I concluded that restricting access to these studies might, in fact, hurt counter-terrorism efforts as public access to studies investigating the mechanisms of soft damage has the potential to diminish the effect of soft damage in the aftermath of a terrorist attack.

However, this argument entails that researchers in the field of terrorism researchers ought to undertake active steps to make their work available to a broad public audience. Next to the general moral obligation of researchers and scientists to publish their work and inform the public about their findings, terrorism researchers discussing soft damage share a moral obligation derived from the NMH principle to be proactively involved in raising public awareness of soft damage by means of cooperating with the other stakeholder groups in the web of prevention. In the joint center as a communication hub, researchers can work together with security institutions and representatives of the public in order to design information materials and workshops to educate the public about the effects and danger of soft damage in terrorist attacks. Hence, not censorship but proactive public communication of their research helps researchers to fulfill their moral responsibilities. The suggested joint center can function as a think tank for this communication process.



#### 4. Who should report dangerous knowledge?

While the publication and treatment of dual-use knowledge can be debated, the status of *dangerous knowledge* (as outlined above) on the internet does not leave much room for debate. As shown in this thesis, the vast majority of the content that is classified as dangerous knowledge shows direct or indirect connections to terrorist propaganda or includes calls to commit crimes against the public.<sup>109</sup> Hence, in most Western countries, these documents, videos, and illustrated manuals are illegal and ought to be deleted from the servers that they were published on. As shown in a detailed analysis in chapter 8 of this thesis, currently, governmental agencies or police institutions such as Europol are the leading (and arguably the only) stakeholder that is seriously concerned with the systematic detection and deletion of dangerous knowledge.

However, as already mentioned, institutions like Europol do not delete content from the internet themselves but call upon the service provider on whose server the dangerous content is stored to delete it. This procedure is not only legally unproblematic but also more feasible from a technical perspective. Yet, the current approach to prevent the distribution of dangerous knowledge shows that security institutions are currently the only stakeholders that perceive themselves morally responsible for actively searching for and requesting the deletion of dangerous knowledge. This

---

<sup>109</sup> Note that in the following I exclusively refer to terrorist propaganda in *combination with* technical instructions on how to prepare weapons for an attack. Clearly, this combination qualifies as dangerous knowledge and ought to be removed. The discussion whether or not terrorist propaganda in general (and without any instructive materials) qualifies as dangerous knowledge and ought to be subject of deletion is an ongoing debate in academia and shall not be discussed any further in this thesis.

perception stems from the institutional responsibility of these agencies to protect society from harm. However, as argued in chapter 6 of this thesis, security institutions share the responsibility to detect, report, and delete dangerous knowledge with online service providers and, to some degree, with internet users. Hence, I argued that not only groups like Europol's IRU but also these other stakeholders ought to be involved in measures to prevent the publication and sharing of weapon manuals and other dangerous knowledge.

Of course, service providers shall not bear the same degree of responsibility as police and intelligence agencies. Yet, as the content in question might be published on their servers and shared via their online infrastructure, they ought to have a more active role in the web of prevention than they currently have. It is only by actively cooperating with other stakeholder groups that the service providers are able to fulfill their responsibilities imposed on them by the NMH principle. By parity of reasoning, it cannot be expected of the internet users that they undertake the same measures as security agencies in the prevention of the distribution of dangerous knowledge. Furthermore, they do not have the moral responsibility of service providers since they do not control the circulation of dangerous content by virtue of owning servers and online platforms. However, by using these platforms and by sharing millions and millions of pieces of content each day, internet users constitute a vital part of the infrastructure that allows content to spread across the globe in milliseconds. This content might include weapon manufacturing manuals or other dangerous knowledge that could be used to harm society on a massive scale.

The joint center is the ideal hub in order to define and communicate the respective measures and actions that each of these stakeholder groups ought to undertake: As the owner of the infrastructure on which dangerous content is stored and shared, online service providers ought to actively search for and, consequently, delete such content. Furthermore, they ought to report to national security institutions the details about the individuals who published and shared this content. This would, depending on the platform, include meta-data like user names, e-mail addresses, cell phone numbers, and IP addresses. While being responsible for detecting and deleting the content, service providers are not responsible for identifying the individuals behind the user names that published dangerous content. Moreover, the service providers ought not to investigate whether these individuals have ties to terrorist groups or exhibit any signs of radicalization. These investigations clearly belong to the responsibilities of security agencies that possess the means and legal authority to identify and prosecute these individuals.

Yet, this measure is not the only responsibility that security agencies have in respect of dangerous knowledge and as participants in the joint center. For while it can be expected of service providers that they detect dangerous content that is stored on their servers, it cannot be expected of them to know (or even worse, define) what ought to classify as dangerous knowledge. Here, representatives of security agencies should cooperate closely with these service providers in order to create a list of criteria that help the employees of the service providers to identify dangerous content. Yet, the authority to determine what ought to count as dangerous knowledge ought not to lay exclusively with the service providers but shall be divided between the legal authorities, security agencies, and representatives of the

public. Hence, while the service providers are responsible for searching for and reporting dangerous documents on their servers, they are not responsible for identifying the nature of dangerous knowledge or for investigating the users that published said content.

The users of social media platforms or other internet services are the third group of relevant stakeholders in the web of prevention in so far as it pertains to the distribution of dangerous knowledge. As seen above, every person that uses a social media or other online platform shares a responsibility to help to prevent the spreading of dangerous content; ultimately, this responsibility is derived from the NMH principle.

However, it would seem excessive to ask all users of these platforms to actively search for and report dangerous content. Since this content is not stored on the computers of these users and (usually) not distributed and shared by them, their moral responsibility in accordance with the NMH principle only stems from the fact that every single user of a social media platform provides (in conjunction with all other users) the infrastructure to share content worldwide. As a member of an important element of this infrastructure, i.e., as a user of social media platforms, every user has the moral obligation to stay vigilant in respect of dangerous content that exists in the network or platform that he or she uses.

Hence, all users of social media platforms or other online services have a moral responsibility to report dangerous content that they come across to the owners of these platforms and services. However, due to their (in comparison to the service providers) diminished moral responsibility, users

are not obligated to actively search for such content. Furthermore, the owners of online platforms have to provide an accessible and simple infrastructure to enable their users to report pieces of content without any hurdles and without raising concerns regarding privacy on the part of the users. Here the current mechanism to report inappropriate or illegal content on the video platform Youtube can serve as a bad example (Youtube, 2021). In order to report a video on Youtube, users have to either sign in to an existing account or have to register and sign up for a new personal account. Only after logging in to an account, the reporting of a video on Youtube is possible. This procedure has, at least, two disadvantages:

- (1) The requirement to either log into or create an account in order to report dangerous content adds a hurdle for users. That might prevent those users from reporting content who are only willing to report content if the procedure can be concluded with one mouse click on a symbol.
- (2) The requirement to log in to an account might raise privacy concerns that could prevent users from reporting an illegal video. Since the user obviously watched the video before reporting it, some users might be concerned that Youtube could forward their account information to the authorities if they report the video.

The example of Youtube's current reporting system shows that users and platform providers have to communicate and cooperate in order to enable internet users to fulfill their responsibilities. For only a functional reporting system that does not actively dissuade users will assist platform providers to detect dangerous content on the internet. The institutionalization of the web

of prevention and, in particular, the joint center will facilitate this cooperation and communication. Moreover, the joint center also ensures that the vigilance of the internet users is directed at the specific content defined as being dangerous rather than any content a user feels is unacceptable. Representatives of all three stakeholder groups ought to create awareness-raising programs, including information material, reporting guidelines, and so on; this material will include descriptions of dangerous knowledge as defined by the security agencies. Equipped with these awareness campaigns, internet users are provided with a broad understanding of what kind of content they should report if they happen to come across it on the internet.

To sum up, it has been argued that two groups of stakeholders ought to be involved in the reporting of dangerous knowledge: the internet users and the service providers. Furthermore, service providers ought to actively search for dangerous content and provide security agencies with particular specified information about the users who published or shared such content. Finally, the security agencies are responsible for investigating these users and for providing the two other stakeholder groups with a workable definition of dangerous knowledge.

## 5. Who should be responsible for deleting dangerous knowledge?

In the last section, the somewhat abstract responsibilities of three stakeholder groups with regard to dangerous knowledge were transformed into concrete measures in the context of the establishment of a joint center

comprised of members of these stakeholder groups (among others). Yet, so far, the majority of these suggested measures are aimed at identifying and reporting dangerous knowledge in online content. A necessary, second step in this cooperation of the stakeholder groups is the deletion of such content in order to prevent the distribution of dangerous knowledge such as weapon manufacturing manuals and related documents. However, the question arises as to which group of stakeholders is morally responsible, and ought to be held institutionally responsible for removing content from the internet and, in particular, dangerous knowledge?

I argue that two of the three stakeholder groups have a moral obligation in this regard. This obligation is based on a simple factor: the technical and legal capability to delete the content in question.

Most of the content on the internet is stored locally on computers (servers) from which a certain website or platform is hosted. Hence, only those persons that have access to these servers are capable of deleting content from the respective online platform. Obviously, the first group that fulfills this technical requirement is the group of online platform service providers. Since these providers host their online platforms on their own servers or, at least, servers that they have unrestricted access to, these providers are capable to add, change or delete any content on these servers at any time. Hence, online service providers are, from a technical perspective, able to delete content, including dangerous knowledge, from their servers in a matter of seconds.

Furthermore, in most cases, these service providers legally own the servers and the content that is created and stored on these servers by internet users. While some content is protected from the provider's interference by national or European privacy laws and/or the provider's data protection guidelines, those pieces of content that violate the provider's terms of services are usually not protected. As already shown above, content that consists at least in part of dangerous knowledge usually violates the terms of service agreements and, further, the law in most Western countries. Hence, the access and the deletion of such content from their own servers is not only a legal right but, in some jurisdictions, a legal obligation of online service providers.

The second group of stakeholders that is, at least potentially, capable of deleting content from servers consists of government security agencies. Due to their in-depth knowledge of the online environment and information technology in general, employees of intelligence agencies and federal or state police offices possess the skills and tools that enable them to access servers remotely and to delete specific content or even all content from these servers (Baer, 2011). In addition to this technical capability, employees of police agencies are also equipped with the legal authority to delete illegal content that is stored on servers and accessible via the internet. For example, if the owner of the server is either not identifiable or not willing to cooperate, police agencies in many European countries, including Germany, have the authority to access servers and confiscate content from these servers.<sup>110</sup> However, this capability ought not to be used by police agencies

---

<sup>110</sup> For the respective German legislation, see the German Code for Criminal Procedure (*Strafprozessordnung*), article 100b.



to access and delete any server content at will, but restricted to illegal content, notably content prohibited under counter-terrorism legislation (For a general discussion concerning Germany, see Baer, 2011).

As seen above, both service providers and government security agencies ought to be responsible for the deletion from the internet of documents and media content consisting at least in part of dangerous knowledge. However, I have argued that there should be a division of labor and two distinct sets of interdependent institutional responsibilities should be defined; one set for each group of stakeholders. Moreover, these institutional responsibilities reflect prior moral responsibilities and, in accordance with the division of labor, they should be applied in a serial or diachronic manner, i.e., content must first be defined and identified before being deleted (This is referred to by Miller as a chain of institutional responsibility (Miller, 2014)).

I argue that, in most cases, the moral obligation to delete the dangerous content is possessed by the service providers alone and ought to be fulfilled by appropriate actions. Hence, if the owner of a server is known to a government institution and this owner is subject to the legal authority of this institution, then this owner of the server possesses the moral (and, in most cases, legal) obligation to delete dangerous content. However, if the owner of the server is not identifiable or the server is physically outside of the reach of the security agency in question, then this agency ought to delete content from this server *if* the content in question could be used to harm society on a massive scale. One example of such a situation would be the publishing of manuals to commit attacks using phosphine in Germany from IS servers that are physically located in Syria. In this scenario, the owner of

the server is not willing to delete the content, and the server is located outside of the reach of German authorities. However, the content on this server is clearly dedicated to instructing terrorists to bring great harm to German society. In cases like these, I argue, security agencies are not only morally allowed, but also possess the moral obligation to access the servers and delete this content.<sup>111</sup>

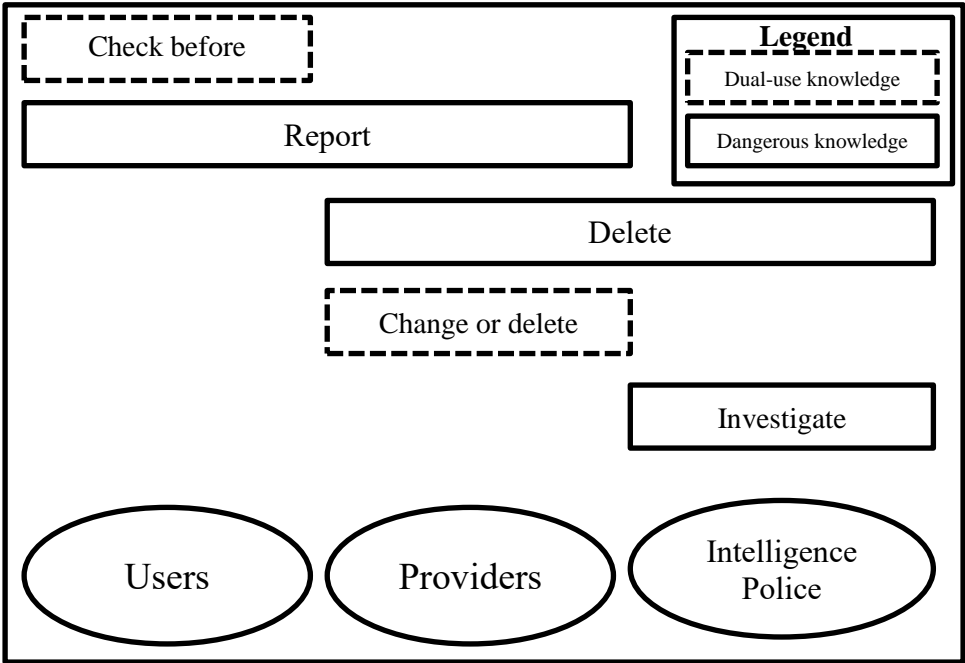
While the legislation to allow or prohibit the accessing of foreign servers by national security agencies is inadequate, I argue that such a measure is ethically justifiable according to the institutional responsibility to protect the public that is the core of the institutional outline of police and intelligence agencies. However, this institutional and moral obligation only applies to cases in which the server in question is used to distribute content that poses an imminent and massive threat to a nation's CBRN security.

To sum up, it has been shown that both service providers and security agencies possess a moral responsibility to delete dangerous content from the internet. However, depending on the location of this content, one or another group of stakeholders ought to act and delete it. The joint center that was proposed in this thesis can help to coordinate these responsibilities and actions of the stakeholder groups appropriately. All responsibilities and proposed actions of all stakeholder groups participating in the web of prevention for the purpose of preventing the circulation of knowledge and acquisition of expertise in relation to perpetrating deadly toxin attacks can

---

<sup>111</sup> It is controversially debated whether or not such a law enforcement operation would be legal in any way. Legal scholars like Wolfgang Baer call for an international (or at least European) legislation that governs transnational cyber-operations of national law enforcement agencies (Baer, 2011). Other current debates can be found in Cajani (2018)

be summarized in the following diagram. Please note that (1) the institutionalization of the web of prevention with the proposed joint center as the hub is a necessary prerequisite for all of the cooperative measures that were proposed in this thesis. (2) Furthermore, the web of prevention and its constitutive measures suggested in this thesis should not be seen as an exhaustive set of counter-measures for preventing terrorist attacks using ricin, phosphine, and americium. Rather, the discussion of the suggested cooperative actions in the joint center shall be seen as a stepping stone and example to create a strong and impermeable web of prevention against terrorist attacks in Germany and other Western countries.



*Fig. 6: Moral responsibilities of relevant stakeholder groups*



# **Special focus and general conclusion**

# The aftermath of an attack, the press, and the public

## 1. Introduction

So far, this thesis has almost exclusively discussed measures to *prevent* terrorist attacks that use ricin, phosphine, and americium. Yet, an essential part of an efficacious counter-terrorism strategy is a set of measures directed at the immediate aftermath of an attack. In situations in which all measures to prevent an attack fail, security agencies have to have plans in hand on how to react to and contain the situation and how to ensure resilience<sup>112</sup> and recovery after a terrorist attack.

Attacks using toxic substances as weapons are particularly relevant in this regard since specialized personnel and specific measures and equipment are needed in order to respond appropriately to these attacks. These measures and the issues that arise in the aftermath of a terrorist attack using toxins have been addressed by a large variety of academic studies (Capone, 2018; Eyison et al., 2020; National Research et al., 2014; Rebera & Rafalowski, 2014; Valkanova et al., 2019). However, these studies have tended to focus on the role of security institutions, first responders, and medical professionals. Yet other stakeholders play (or ought to play) a role in

---

<sup>112</sup> The term resilience refers to a complex concept, but will be defined in a narrow sense in this thesis as “ability to return to a stable equilibrium (...) [i.e.,] state or condition prior to the disruption [or terrorist attack]” (Doorn et al., 2019, p. 114). For further discussion on resilience, see Doorn (2017) and Copeland et al. (2020).

ensuring recovery and resilience in the aftermath of such an attack and, more specifically, in the aftermath of an attack that uses common-use toxins. This chapter will discuss two of these stakeholders who have responsibilities to contribute to the process of recovery from an attack with ricin, phosphine, and americium: the media and the public at large, i.e., ordinary citizens. As already examined in detail, all of these three substances have the potential to inflict a massive degree of psychological and political damage (soft damage) in a target society if they are used in a terrorist attack. The two above-mentioned groups of stakeholders are both catalysts and recipients of this soft damage. Hence, both the press and the public are capable of either amplifying or diminishing the soft damage inflicted by a terrorist attack.

The present chapter focuses on this two-sided role of the media and the public in the aftermath of a terrorist attack with common-use toxins as weapons. Firstly, it will be shown that currently neither the news media nor the public cooperate with the security institutions to the degree that is sufficient to fulfill their responsibilities according to the NMH principle. Secondly, a set of cooperative measures will be suggested that, if implemented, would enable both the public and the news media not to provide terrorists with the means to cause psychological and political harm to society or, at least, not to do so to anything like the extent to which they have been doing so thus far. The joint center proposed in this thesis is essential to coordinate these cooperative measures by means of facilitating dialogue between the stakeholder groups.

## 2. The role and responsibilities of the news media

### 2.1. The current situation

As already discussed in this thesis, publicity and media reports are essential prerequisites for a successful terrorist attack (Eid, 2014; Mythen & Walklate, 2006; Williamson et al., 2019). Without the attention of the media, terrorists would not be able to communicate their ideological agenda by means of their attacks. The impact of a terrorist attack in the form of casualties and physical destruction is generated by the terrorist in order to attract the attention of the public and, more specifically, the news media and, thereby, cause soft damage. Terrorists can only perform successful attacks if they manage to create sufficient publicity to create a large and appropriate audience for their ideological message.<sup>113</sup> By reporting about terrorist attacks at length, the press is, therefore, playing a part in the terrorists' strategy, albeit perhaps unwillingly (Ayish, 2014; and other discussions in Eid, 2014). According to the NMH principle, the simple act of reporting on a terrorist attack does not seem to be troublesome, even if it might be advantageous to the agenda of the terrorists. However, as I will argue in the following section, journalists violate the NMH, at least in some capacity, if they report *in a certain manner and to a certain extent* on terrorist attacks that use common-use toxins as weapons.

As already briefly mentioned in chapter 6 of this thesis, extensive journalistic reporting on terrorist attacks transports the psychological and political impact of an attack to a wide audience even if this attack did not

---

<sup>113</sup> See chapter 1 of this thesis.



manage to inflict a large amount of physical damage. Hence, journalists that, for example, report on a <sup>241</sup>AM based RDD attack without any casualties by portraying it as a “dirty bomb” or radiological terrorism provide the perpetrators of the attack with the means to harm a massive amount of persons psychologically and the government of the target country politically. These journalists would clearly violate the NMH principle with their style of reporting on the attack. Such a sensationalistic style of reporting on a terrorist incident involving a common-use toxin is not a mere thought experiment but has actually occurred in the past. One example of a case in which sensationalistic journalist reporting transported increased the soft damage of a terrorist incident is the already mentioned article on the Cologne Ricin Plot in the German daily newspaper “Rheinische Post”.<sup>114</sup>

After the arrest of Sief Allah H., the Rheinische Post published an article about the details of H’s plot. In the title of this article, the author claimed that the amount of ricin that H. produced had the potential to kill up to 13,500 persons (Rheinische Post, 2019). Although German counter-terrorism forces managed to arrest H. before he could commit the attack, the journalist reporting on the incident and the hypothetical scenarios that were formulated in the headline of the article, arguably, evoked a substantial amount of anxiety among the German public. Furthermore, one could argue that this style of reporting contributed to an erosion of public trust in the German security apparatus. The mere prospect of an attack with up to 13,500 fatalities was more than enough to spread fear and distrust in German society. In effect, news outlets such as the Rheinische Post provided

---

<sup>114</sup> See chapter 6 of this thesis.

H. with the means to increase the harm his terrorist act, or attempted terrorist act, could cause.

In summation, currently, at least some media outlets do not seem to be aware of their responsibilities in the aftermath of terrorist attacks using common-use toxins as weapons. The journalists behind the discussed article (but presumably many other journalists as well) do not perceive themselves as part of a web of prevention and do not cooperate with other groups of stakeholders to the degree that is sufficient to fulfill their responsibilities as part of this web.

## 2.2. The media in the web of prevention

Journalists have to discontinue to provide terrorists with the means to greatly increase the soft damage terrorists' attacks cause. They have to do this in order to fulfill their moral responsibilities as part of the web of prevention and to comply with the NMH principle. Yet, this is only achievable if journalists cooperate with other stakeholder groups in the web of prevention. The example of the above described German newspaper article can be used to illustrate what such cooperation might look like.

In the text of the article in Rheinische Post, the author explains that the estimate of 13,500 potential fatalities on the basis of the ricin in Sief H.'s apartment was given by a German security official. However, the author admits in a short sentence that the same official also stated that the number of 13,500 was a mathematical calculation on the basis of the LD<sup>50</sup> value of ricin (Rheinische Post, 2019). Yet, the LD<sup>50</sup> value exclusively displays the lethality of a perfectly purified substance under ideal laboratory conditions.

Later on in the article, the author, in effect, admits that this was an exaggeration when he stated that the interviewed security official estimated the lethality of H.'s actual ricin device to be in the low hundreds. While this death toll would still be horrific, it would not be the almost apocalyptic number of 13,500 fatalities after a single attack, as was propagated in the title of the article.

The security official that was interviewed for the article gave a differentiated estimate of the possible consequences of an actual attack with H.'s device. Yet, apparently, this estimate was not as sensationalistic as the author of the article needed it to be in order to attract the attention of the reader. Hence, he chose to use the estimate that was based on the LD<sup>50</sup> value of ricin as the headline of the article. However, the author of the article clearly violated the NMH principle with this choice and style of reporting: with this headline, the article provided H. with the means to greatly increase fear among the German public.

Yet, this does not mean that journalists have to discontinue reporting on these attacks and plots altogether. Rather, journalists ought to change the style of their reporting in relation to events such as the Cologne Ricin Plot. In the aftermath of exceptional plots and attacks, journalists are able to comply with the NMH principle if they report on the respective plot or attack in a strictly neutral fact-based manner. This neutral fact-based style of reporting intends to avoid emphasizing those aspects of the attack or plot that are hypothetical and do not reflect the situational facts (For general discussion, see Rubin et al., 2012). The emphasis on the LD<sup>50</sup> value of ricin in the headline of the article in *Rheinische Post* is an excellent example of

this misleading exaggeration of an aspect of a terrorist plot in a manner that does not reflect the facts of the situation. At first glance, this argument for restricting journalistic reporting to a neutral and fact-based style in cases of terrorism using toxic substances as weapons might be viewed as an argument for restricting the freedom of the press. However, misleading exaggeration is not an exercise of freedom of the press; it is a manifestation of morally irresponsible journalism.

This call for restricting the style of reporting in these exceptional cases is solely based on the moral obligations of journalists. Moreover, while failure to discharge these obligations might be morally wrong, it is not necessarily something that ought to be legally sanctioned. Rather, this moral obligation shall be understood as something to be written into an ethical code among journalists concerning the style of reporting on exceptional incidents. Similar ethical codes are already in place among journalists. For example, most German media outlets agreed upon not reporting in a detailed or sensationalistic manner on suicides unless it concerns a person of public interest since research demonstrates that such reporting on suicides and attempted suicides might increase suicide rates.<sup>115</sup>

By reporting on terrorist attacks and plots in a strictly neutral manner and without sensationalistic elements, journalists do not provide terrorists with an essential element of the means to harm their target society psychologically and politically or may reduce that element. In the immediate aftermath of an attack or plot, journalists are often confronted

---

<sup>115</sup> This agreement is part of the ethical code of journalists that was published by the German Council of the press (Presserat) (Deutscher Presserat, 1997).

with contradictory information from security agencies. Driven by sensationalistic motives, some journalists choose to report only those elements of this information that contain worst-case scenarios. Moreover, while some journalists have published exaggerated or otherwise misleading material, other journalists might rely on this material and, in effect, republish it in the aftermath of an attack or plot yet do so without any sensationalistic intentions. Further, if security agencies provide contradictory information, then even journalists without any intention to sensationalize might publish exaggerated or otherwise misleading reports. Therefore, not only journalists but also members of the security institutions possess a moral responsibility with regard to their communications to journalists and, therefore, with respect to journalist reporting on attacks using common-use toxins such as ricin as a weapon.

In order to enable journalists to report on the facts of an attack in an above-favored manner, security agencies ought to communicate these facts in a clear and structured way to the media, including the key elements of what has happened, and, therefore, what to report on. This communication strategy should not leave any room for misunderstanding, as happened in the case of the Cologne Ricin Plot. Naturally, security agencies cannot control what journalists report to the extent of preventing irresponsible journalists from willful misinterpretation, sensationalistic exaggeration, or even ‘fake news’ (For a definition, see Quandt et al., 2019).

Nevertheless, representatives of the security agencies can mitigate the problem by providing media representatives with a clear and simple set of facts that enable well-intentioned journalists to report without inaccuracies,

misinterpretations, or misunderstandings of a kind that leads to unwarranted sensational or otherwise damaging reporting (See literature review in Rubin et al., 2012). Furthermore, representatives of counter-terrorism institutions ought to work closely together with journalists and raise awareness of the essential role that media reporting plays in the aftermath of an attack.

In addition to cooperation and communication between journalists and security institutions, there is a need for representatives of the public to be involved in this dialogue. Their feedback on how the public perceives the reporting after a terrorist attack can help journalists to understand their moral responsibilities and, thereby, adjust their reporting to comply with public needs. It is particularly important to educate journalists and media representatives on the psychological damage of terrorist attacks; damage that can be increased through irresponsible media coverage. In order to communicate and cooperate efficiently and directly, journalists, security agencies, and representatives of the public ought to make use of the suggested institutionalized web of prevention against the terrorist use of common-use toxins.

### 3. The role of the public in the aftermath of a terrorist attack with common-use toxins as weapons

#### 3.1. The current situation

Once a terrorist group has acquired the knowledge and technology to assemble a biological, chemical, or radiological weapon, security agencies

have to assume that an attack with such a weapon might, in fact, take place. Hence, governmental security agencies are cooperating with national and international crisis management institutions to create scenario-based simulations on how to respond to terrorist attacks using toxic substances as weapons (See for general discussion Lakoff, 2007). Tasks like decontamination, the restoration of public order, and the neutralization of the threat are only few components of these post-attack recovery measures (See for decontamination Rebera & Rafalowski, 2014; TRADOC, 2007, p. 27).

Since terrorist attacks have, just like natural disasters, local impacts in most cases (e.g., a music festival in a small town in Germany (Niebergall, 2016)), a national response strategy with the required resources might not be in place soon enough to respond to a biological, chemical or radiological attack effectively (Veil, 2008, p. 388). Thus, local fire departments, regional crisis managers, and the local police forces are crucial components in responding to these attacks.

In addition to these groups of actors, many governments of liberal democratic societies encourage their citizens to inform themselves about the threat of terrorist attacks and to undertake certain measures to prepare for these attacks. In practice, these measures usually include information materials like leaflets, videos, or presentations that provide some basic facts about the nature of the threat and possible strategies to stay safe during and immediately after an attack. By educating the public about the threat, security agencies hope to reduce the psychological impact of an attack, and by suggesting ways to respond to attacks, counter-terrorism agencies aim at

reducing the physical impact (i.e., the number of casualties) during an attack (For RDDs see Rogers, Amlôt, & Rubin, 2013). In sum, the aim is to increase societal resilience against a terrorist attack with chemical, biological or radiological weapons.

Examples of this resilience strategy can be found in nearly every liberal democracy, including the United States of America and Germany. The US DHS, for instance, published on its website a detailed description of the nature and prospective impact of a radiological attack. In this factsheet, the DHS also gives instructions on how to react to an attack with an RDD (Department of Homeland Security, 2017).

Another example of this resilience measure is on the website of the German Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). The agency has an online leaflet about so-called exceptional situations of danger, including terrorist attacks using CBRN agents (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2017c). Specifically, the leaflet and the website of the BBK describe the nature of different dangerous chemical, radiological and other agents and give recommendations such as removing contaminated clothing and following radio announcements closely. Furthermore, the BBK published a factsheet that is focused on chemical warfare agents in particular. Just like the more general leaflets, this factsheet also includes recommendations on how to respond to a chemical attack (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2017a).

In addition to the leaflets and factsheets that are focused on attacks using chemical and radiological weapons, both the US and German governments



have been publishing numerous information materials to prepare their citizens for disaster situations in general – including terrorist attacks. For example, the website [ready.gov](http://ready.gov) informs US citizens about strategies to respond to disaster situations and encourages everyone to prepare for these situations by means of storing drinking water, food, and other essential supplies at home (Ready.gov, 2017). A similar approach has been followed by the German government. German citizens can find a detailed leaflet on the website of the BBK that encourages every German citizen to lay in a stock of essential goods in order to prepare for disasters such as floods and storms, but also for attacks on critical infrastructure or high profile terrorist attacks (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2017b). This leaflet was advertised on German national television as described below.

The first and most prominent problem with the approach to increase societal resilience through leaflets and information materials can be identified by taking a closer look at the distribution mechanisms of these and similar disaster information materials. Here it becomes apparent that all of the above-introduced examples (i.e., the materials published by the DHS and the BBK) follow a strict top-down approach (General discussion in Veil, 2008, p. 388). The discussed governmental agencies attempt to communicate directly with their citizens by providing centralized information materials on a nation-wide level. This approach, however, does not seem to be efficacious enough to, in fact, increase societal resilience among a large percentage of their citizens.

As regional disaster managers in the USA reported in interviews for a study with regard to similar information materials and leaflets focused on natural disasters, only a fraction of their clients (i.e., citizens in their working area) is taking the advice given in these materials seriously (op. cit. Veil, 2008, p. 389). Rather, a large percentage of citizens do not know about these materials or seem to be of the opinion that these preparatory measures are not necessary. This attitude (that was described as complacency by some disaster managers in the study (op. cit. Veil, 2008, pp. 388–389)) is likely to be present towards those leaflets focused on CBRN terrorism as well since these materials have been distributed through the same top-down strategy.

Moreover, there are other shortcomings in relation to societal resilience measures. Consider the focus of many counter-terrorism and disaster management agencies in the USA and other countries. It seems that most of these agencies almost exclusively focus on preventive measures or, at least, communicate their efforts in a way that suggests an exclusive focus on prevention (Veil, 2008, pp. 388–389). One of the interviewed regional disaster managers criticized that “[s]o much time is spent talking about prevention that people forget things can still happen” (op. cit. Veil, 2008, p. 388).

In addition to this problem of efficacy, the distribution of information materials and preparedness advice to increase societal resilience also entail some ethically relevant problems that have to be dealt with. The most pressing issue in this regard is the fact that governments (unintentionally) influence public opinion about how serious the threat of terrorism with chemical or radiological weapons is.

One recent example that may summarize this issue best is the publication of the “Ratgeber für Notfallvorsorge und richtiges Handeln in Notsituationen” (Guide for emergency preparedness and correct disaster response) as part of the publication “Konzept Zivile Verteidigung” (Concept civil defense) by the German BBK in 2016 (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2017b). The BBK and the German government explained the need for this publication and their encouragement of disaster preparedness in terms of new, hybrid threats such as terrorism, cyber warfare, and attacks against critical infrastructure.

However, while both the Ministry for Interior Affairs and the BBK never mentioned concrete threats or an upcoming attack, the publicly announced and broadly discussed guide caused a fear in German society that a large-scale (terrorist) attack might be expected in the near future (Eubel, 2016). This fear led to a harsh critique by the opposition party SPD, whose members stated that too little communication, or even miscommunication, on the part of the government, as well as the bad timing of the publication (in the aftermath of several terrorist attacks on German soil in July 2016), caused panic in the German public (Eubel, 2016).

A similar effect might be observable in case of the publication of information materials that are directly focused on attacks using chemical and radiological weapons, such as the factsheets and leaflets on the websites of the DHS and the BBK. Bald public announcements that encourage citizens to study and adhere to the advice given in these publications could easily be misinterpreted as an implicit warning that a chemical or radiological attack is to be expected. This misinterpretation could certainly

increase public fear of such attacks, thereby, increasing the psychological impact of, in particular, attacks that use common-use toxins as weapons. Further, this increased psychological impact of potential attacks using these improvised weapons could make substances such as ricin, phosphine, and americium even more attractive to terrorists. Public announcements and dissemination of these information materials, however, seem to be a good (and, at first glance, the only) way to motivate citizens to inform themselves and to prepare for attacks. This dilemma is acute and deserves more attention.

### 3.2. The public in the web of prevention

As already seen in the section above, there is a dilemma. On the one hand, citizens do not seem to pay attention to information campaigns consisting of public announcements and widely disseminated information material that seeks to increase social resilience to terrorist attacks. On the other hand, aggressive campaigns that emphasize threats and urging compliance with specific measures may cause panic and, thereby, actually assist the terrorists' cause. As with the problems addressed in this thesis, this dilemma can be dealt with by applying the concept of collective moral responsibility. First of all, notions of collective moral responsibility can be used to support the claim of disaster managers and researchers that societal resilience is more than just a top-down recommendation or imposition by the government, but, in fact, a collective civic responsibility in a liberal democracy, i.e., a responsibility that every citizen shares (See Veil, 2008). Chapter 6 of this thesis showed this in some detail.

Furthermore, not only citizens but also the other stakeholder groups are involved in this task of ensuring resilience. Citizens of a liberal democracy can only be held responsible for the above-described measures if they are given the means to comply with them. Thus, governmental agencies, businesses, and the press share the responsibility to optimize the way information materials and other measures for societal resilience are designed, distributed, and communicated in a liberal democracy.

For example, one possible application of this joint responsibility may be to actively include members of as many societal groups, as well as national, regional, and local agencies, as possible in the process of creating and – even more important – distributing information materials concerning the dangers of attacks using weaponized common-use toxins. This approach enables circumvention of the harmful top-down approach that, as seen above, can easily result in either lack of attention by citizens or miscommunication and panic. An interesting example of such an approach involving several societal groups and with regional emphasis may be the McReady campaign created in cooperation with US citizens; it distributed disaster preparedness factsheets through McDonalds restaurants (Veil, 2008, p. 389).

The suggested joint center would provide an excellent opportunity for representatives of the public to meet and discuss with the other stakeholder groups the ways to raise awareness concerning the above described civic responsibilities. For only if security institutions, the press, and businesses (such as seen in the example of the McReady campaign) jointly provide citizens with the information that they need in order to react without panic

and excessive anxiety in the aftermath of an attack, then every individual citizen is capable of fulfilling their moral responsibility with regard to the NMH principle. In practice, a good option to achieve this goal would be to jointly create information materials that, firstly, describe and motivate civic responsibilities (raising awareness), secondly, outline the facts about the psychological and political damage caused by terrorist attacks, as well as facts about the (limited) physical destructiveness of terrorism using toxic substances (also raising awareness), and, thirdly, the diminishing soft damage that results if certain measures are taken in compliance with civic responsibilities (resolving the dilemma). Equipped with information materials of this sort, every single citizen in society could potentially become a strong thread in the web of combatting terrorists that use weaponized common-use toxins.



## General conclusion

The essential role of the public in the web of prevention shows, maybe more illustrative than all other examples in this thesis, how small individual actions of each and every one of us can help to combat and, eventually, eradicate the horrors of this special branch of terrorism. In summary, the findings of this thesis and the analyzed and suggested counter-measures against the terrorist use of ricin, phosphine, and americium can be displayed in a set of tables. These tables summarize the three groups of counter-measures with the respective (1) stakeholder groups, (2) moral obligations of each stakeholder group, (3) suggested actions of each stakeholder group, (4) and most important partnerships for the stakeholders to fulfill their respective responsibilities.

<b>Stakeholder group</b>	<b>Responsibilities</b>	<b>Measures</b>	<b>Main partners</b>
Security institutions	Prevent acquisition of materials	Raise awareness of dangerous goods and suspicious purchases, investigate purchases	Vendors and manufacturers



Vendors	Do not provide substances to terrorists	Document purchases and report suspicious purchases	Security institutions
Manufacturers	Do not provide substances to terrorists	Inform about dangers of novel substances, change design for security	Security institutions

*Table 2: Web of prevention – materials*

<b>Stakeholder group</b>	<b>Responsibilities</b>	<b>Measures</b>	<b>Main partners</b>
Security institutions	Prevent acquisition of expertise	Raise awareness of dangerous knowledge, investigate internet users, delete content	Social media providers, Internet users
Social media providers	Do not enable terrorists to acquire expertise	Search for, report and delete illegal content	Security institutions, Internet users

Internet users	Do not be complicit in the distribution of ‘dangerous’ knowledge to terrorists	Report illegal content if found	Social media providers
----------------	--	---------------------------------	------------------------

*Table 3: Web of prevention – expertise (only dangerous knowledge)*

<b>Stakeholder group</b>	<b>Responsibilities</b>	<b>Measures</b>	<b>Main partners</b>
Security institutions	Ensure resilience	Raise awareness and coordinate response	The press, the public
Media outlets	Do not enable terrorists to cause soft damage	Change style of reporting	Security institutions, the public
The public	Do not provide terrorists with the means to cause soft damage	Be aware of the threat and prepare in order to survive it	Security institutions

*Table 4: web of prevention – resilience*

Note that the table on the preventative measures against the acquisition of weapon-related expertise by terrorists addresses only one kind of expertise; the expertise that was defined as dangerous knowledge in chapter 10 of this thesis.<sup>116</sup> The respective table to summarize the stakeholders, responsibilities, actions and partnerships in dealing with dual-use knowledge has a slightly different focus. Hence, it will be displayed separately from the other tables.

<b>Stakeholder group</b>	<b>Responsibilities</b>	<b>Actions</b>	<b>Main partners</b>
Security institutions	Prevent acquisition of expertise	Start a discussion about what ought not to be published and raise awareness	Researchers, content creators
Researchers	Do not provide expertise to terrorists	“Think before publish” <sup>117</sup> , be aware of the nature of dual-use	Security institutions

---

<sup>116</sup> I define dangerous knowledge as weapon manufacturing manuals and other instructive materials that have a clear connection to terrorism (e.g. IED manuals in al Qaeda publications).

<sup>117</sup> I.e., consider the potential negative consequences of the information you intend to publish. See chapter 10 for discussion.

Content creators	Do not provide expertise to terrorists	“Think before publish”, be aware of the nature of dual-use	Security institutions
------------------	--	--	-----------------------

*Table 5: Web of prevention – expertise (dual-use knowledge)*

This overview of stakeholders, responsibilities, actions, and partnerships that are or ought to be in place to fight terrorist attacks using improvised biological, chemical, and radiological weapons shall be, in a last step of visualization, used in order to web an institutionalized web of prevention. This web shall be thought of in the form of a joint center that allows for all stakeholder groups to communicate and coordinate cooperative actions against the terrorist use of common-use toxins. In this center, the security institutions ought to be in the command position, which coordinates cooperation between all those stakeholders who are part of the center in the form of spokes or chairs. The outline of the center can be depicted in the following structure:

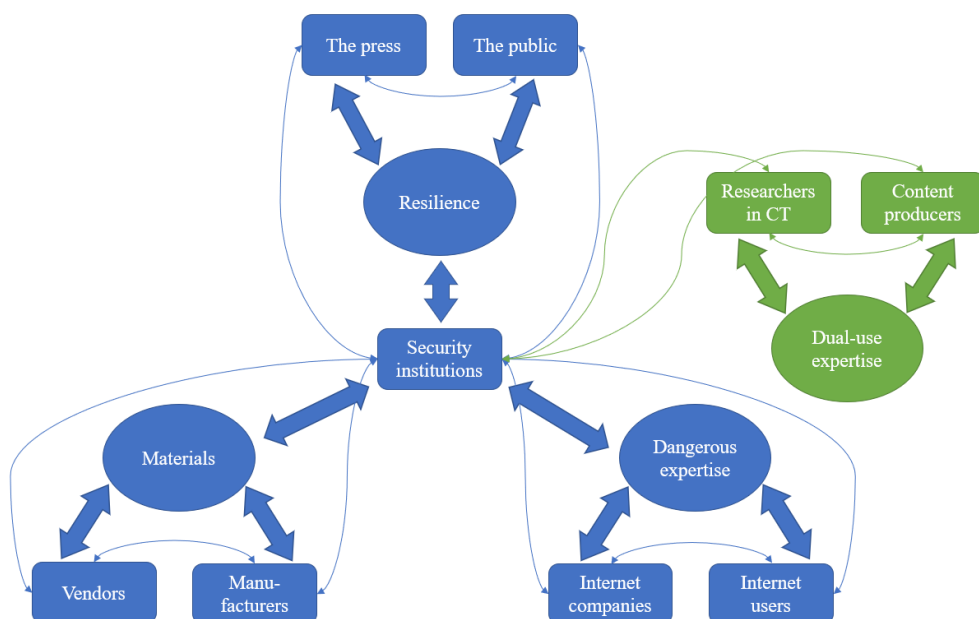


Fig. 7: Web of prevention

Yet, the institutionalized web of prevention, as suggested in this thesis, is not limited to the fight against terrorist attacks using ricin, phosphine, and americium. *Thinking about the specific roles and moral responsibilities of multiple groups of stakeholders in the fight against terrorism and understanding the mechanisms behind terrorism as a collective phenomenon that can be either fueled or diminished by businesses, the press, and the public can teach us to fight a variety of threats to our liberal democracy more efficaciously and ethically sustainable.* In connection with this more general point, this thesis has shown that:

- (1) Every member of our society takes, albeit unwillingly, part in providing terrorists with the means to harm us.
- (2) Hence, all of us are jointly and individually responsible for discontinuing this support and for defending our society.
- (3) Awareness of these joint and individual responsibilities in defending our society against threats has to be actively raised.
- (4) Communication and cooperation of all stakeholders are key in webbing a strong web of prevention that honors the values of our democracy.
- (5) This web is not a theoretical construct but ought to be institutionalized in a hub that connects representatives of all stakeholders with each other.

Some threats to our society, such as attacks against critical infrastructure, are already combatted by means of joint centers, which involve the participation of multiple stakeholders, while other threats (including terrorist attacks using common-use toxins as weapons) have been overlooked. As researchers in the field of counter-terrorism, it is our moral responsibility to identify these gaps in our security architectures and to publicly raise awareness of their existence.



# References

## I. Legal Documents

### A International treaties and conventions

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Space Treaty). United Nations. 1967.

Treaty on the Non-Proliferation of Nuclear Weapons (NPT). United Nations. 1970.

Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Sea-Bed and the Ocean Floor and in the Subsoil thereof (Seabed Treaty). United Nations. 1972.

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (BWC). United Nations. 1975.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1). United Nation. 1979.

Strategic Arms Reduction Treaty (START). United States of America, Russian Federation. 1991.



Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC). United Nations, OPCW. 1997.

## **B European regulations and directives**

Council Directive 80/876/EEC of 15 July 1980 on the approximation of the laws of the Member States relating to straight ammonium nitrate fertilizers of high nitrogen content. European Council. 1980.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). European Parliament, European Council. 2002.

Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/ECC National legislation. European Parliament, European Council. 2006.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. European Parliament, European Council. 2006.

Regulation (EC) No 1272/2008 of the European Parliament and of the Council of 16 December 2008 on classification, labelling and packaging of substances and mixtures, amending and repealing Directives 67/548/EEC and 1999/45/EC, and amending Regulation (EC) No 1907/2006. European Parliament, European Council. 2008.

Directive 2009/128/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for Community action to achieve the sustainable use of pesticides. European Parliament, European Council. 2009.

2009/228/EC: Decision of the European Parliament of 22 April 2008 on the closure of the accounts of the European Network and Information Security Agency for the financial year 2006. European Parliament. 2009.

Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. European Council. 2009.

Regulation (EC) No 1107/2009 of the European Parliament and of the Council of 21 October 2009 concerning the placing of plant protection

products on the market and repealing Council Directives 79/117/EEC and 91/414/EEC. European Parliament, European Council. 2009.

Regulation (EU) No 305/2011 of the European Parliament and of the Council of 9 March 2011 laying down harmonised conditions for the marketing of construction products and repealing Council Directive 89/106/EEC. European Parliament, European Council. 2011.

Council Directive 2013/59/Euratom of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation, and repealing Directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom and 2003/122/Euratom. European Council. 2013.

Commission implementing Regulation (EU) No 1034/2013 of 24 October 2013 approving aluminium phosphide releasing phosphine as an active substance for use in biocidal products for product type 20. European Commission. 2013.

## **C National legislation (Germany)**

*Strafprozessordnung (StPO)* (Code of Criminal Procedure). 1952.

*Strafgesetzbuch (StGB)* (Criminal Code). 1953.

*Gesetz über die Kontrolle von Kriegswaffen (KrWaffKontrG)* (Military Weapon Control Act). 1961.

*Waffengesetz (WaffG)* (Weapons Act). 1972.

*Verordnung zum Schutz vor Gefahrstoffen (GefStoffV)* (Hazardous Substances Ordinance). 1993.

*Verordnung über Verbote und Beschränkungen des Inverkehrbringens und über die Abgabe bestimmter Stoffe, Gemische und Erzeugnisse nach dem Chemikaliengesetz (ChemVerbotsV)* (Chemical Ban Ordinance). 1993.

*Gesetz zum Schutz vor der schädlichen Wirkung ionisierender Strahlung (StrlSchG)* (Act on Protection against the Harmful Effects of Ionising Radiation). 2017.

## II. Literature

(START), N. C. for the S. of T. and R. to T. (2016). *Global Terrorism Database [Data file]*.

Abrahms, M. (2006). Why terrorism does not work. *International Security*, 31(2), 42–78.

Ackerman, G. (2014). “More bang for the buck”: examining the determinants of terrorist adoption of new weapons technologies. King’s College London (University of London).

Ackerman, G., & Jacome, M. (2018). WMD Terrorism. *PRISM*, 7(3), 22–37.

Ackerman, G A, & Pereira, R. (2014). Jihadists and WMD: a Re-evaluation of the Future Threat. *CBRNe World*, 27–34.

Ackerman, Gary A, & Pinson, L. E. (2014). An Army of One: Assessing CBRN Pursuit and Use by Lone Wolves and Autonomous Cells. *Terrorism and Political Violence*, 26(1), 226–245.  
<https://doi.org/10.1080/09546553.2014.849945>

Amazon. (2019a). *EU-US and Swiss-US Privacy Shield*. Amazon.Com.  
[https://www.amazon.com/gp/help/customer/display.html/ref=hp\\_left\\_v4\\_sib?ie=UTF8&nodeId=202135380](https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=202135380)

Amazon. (2019b). *Privacy Notice*. Amazon.Com.  
[https://www.amazon.com/gp/help/customer/display.html/ref=hp\\_left\\_v4\\_sib?ie=UTF8&nodeId=201909010#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3\\_\\_SECTION\\_87C837F9CCD84769B4AE2BEB14AF4F01](https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201909010#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_87C837F9CCD84769B4AE2BEB14AF4F01)

Amazon. (2019c). *Report a Security Issue*. Amazon.Com.  
[https://www.amazon.com/gp/help/customer/display.html/ref=hp\\_left\\_v4\\_sib?ie=UTF8&nodeId=201909140](https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201909140).

Anscombe, G. E. M. (2000). *Intention*. Harvard University Press.

Appleton, C. (2014). Lone wolf terrorism in Norway. *The International Journal of Human Rights*, 18(2), 127–142.

Arendt, H. (1987). Collective responsibility. In J. W. Bernauer (Ed.), *Amor Mundi: Explorations in the Faith and Thought of Hannah Arendt*. Distributors for the U.S. And Canada Kluwer Academic Publishers.

- Asal, V. H., Ackerman, G. A., & Rethemeyer, R. K. (2012). Connections Can Be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Weapons. *Studies in Conflict & Terrorism*, 35(3), 229–254.  
<https://doi.org/10.1080/1057610X.2012.648156>
- Atlas, R. M. (2009). Responsible Conduct by Life Scientists in an Age of Terrorism. *Science and Engineering Ethics*, 15(3), 293–301.  
<https://doi.org/10.1007/s11948-009-9124-7>
- Australian Government. (2016). *National Code of Practice For Chemicals of Security Concern*. Nationalsecurity.Gov.Au.  
<https://www.nationalsecurity.gov.au/Securityandyourcommunity/ChemicalSecurity/Documents/Code-of-practice.PDF>
- Auswärtiges Amt. (2017). *Terrorismusbekämpfung*.  
[http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/TerrorismusOK/Terrorismus\\_node.html](http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/TerrorismusOK/Terrorismus_node.html)
- Ayish, M. (2014). Employing of Media during Terrorism. In M. Eid (Ed.), *Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia* (pp. 157–172). IGI Global.
- Baer, W. (2011). Transnationaler Zugriff auf Computerdaten. *Zeitschrift Fuer Internationale Strafrechtsdogmatik*, 2, 53–59.
- Bale, J. (2004). *The Chechen Resistance and Radiological Terrorism*. Nuclear Threat Institute Website.  
<http://www.nti.org/analysis/articles/chechen-resistance-radiological-terror/>
- Bates, T. (1992). *Rads: The 1970 bombing of the Army Math Research*

- Center at the University of Wisconsin and its aftermath*. HarperCollins.
- Batson, C. D., Kennedy, C. L., Nord, L., Stocks, E. L., Fleming, D. A., Marzette, C. M., Lishner, D. A., Hayes, R. E., Kolchinsky, L. M., & Zerger, T. (2007). Anger at unfairness: Is it moral outrage? *European Journal of Social Psychology*, 37(6), 1272–1285.
- Baumanns, R. (2018). *Köln-Chorweiler: Gift-Anschlag geplant? Polizei nimmt Tunesier fest*. Express. <https://www.express.de/koeln/koeln-chorweiler-gift-anschlag-geplant--polizei-nimmt-tunesier-fest-30610914>
- BBC. (2006). *Al-Qaeda plotter jailed for life*. <http://news.bbc.co.uk/2/hi/uk/6123236.stm>
- BBC. (2018). *Ricin threat: Cologne anti-terror police search flats*. BBC News. <https://www.bbc.com/news/world-europe-44494010>
- BBK. (2019). *UP KRITIS*. [https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk\\_node.html](https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html)
- Bentley, M. (2012). The Long Goodbye: Beyond an Essentialist Construction of WMD. *Contemporary Security Policy*, 33(2), 384–406. <https://doi.org/10.1080/13523260.2012.693804>
- Bentley, M. (2014). *Weapons of Mass Destruction and US Foreign Policy the strategic use of a concept*. Taylor and Francis.
- Bernstein, M. (2017). *Untersuchungsbericht: Münchner Amokschütze war rechtsextrem gesinnt*. Sueddeutsche Zeitung. <https://www.sueddeutsche.de/muenchen/oez-untersuchungsbericht->

muenchner-amokschuetze-war-rechtsextrem-gesinnt-1.3480126

- Berntzen, L. E., & Sandberg, S. (2014). The collective nature of lone wolf terrorism: Anders Behring Breivik and the anti-Islamic social movement. *Terrorism and Political Violence*, 26(5), 759–779.
- Bezuidenhout, L. (2012). Research infrastructures, policies and the ‘web of prevention’: the ethical implications of inadequate research environments. *Medicine, Conflict and Survival*, 28(1), 19–30.  
<https://doi.org/10.1080/13623699.2012.658623>
- Bezuidenhout, L., & Rappert, B. (2012). The ethical issues of dual-use and the life sciences. *CORE Issues*, 1(1), 93–114.
- Binder, M. K., & Ackerman, G. A. (2019). Pick Your POICN: Introducing the Profiles of Incidents involving CBRN and Non-State Actors (POICN) Database. *Studies in Conflict & Terrorism*, 1–25.  
<https://doi.org/10.1080/1057610X.2019.1577541>
- Binder, M. K., & Quigley, J. M. (2019). *Profiles of Incidents Involving CBRN and Non-state Actors (POICN) Database*. START Consortium, University of Maryland.
- Binder, M. K., Quigley, J. M., & Tinsley, H. F. (2018). Islamic State Chemical Weapons: A Case Contained by its Context? *CTC Sentinel*, 27–31.
- Bogle, R. G., Theron, P., Brooks, P., Dargan, P. I., & Redhead, J. (2006). Aluminium phosphide poisoning. *Emerg Med J*, 23.  
<https://doi.org/10.1136/emj.2004.015941>
- Bolarinwa, I. F., Orfila, C., & Morgan, M. R. A. (2014). Amygdalin content



of seeds, kernels and food products commercially-available in the UK.  
*Food Chemistry*, 152, 133–139.

Bratman, M. (1997). The Two Faces of Intention. In A. R. Mele (Ed.), *The Philosophy of Action* (pp. 178–203). Oxford University Press.

Bratman, M. E. (1999). *Faces of Intention: Selected Essays on Intention and Agency*. Cambridge University Press.

<https://doi.org/10.1017/CBO9780511625190>

Breivik, A. B. (2011). 2083 – *A European Declaration of Independence*.

BUND.DE. (2017). *Zollkriminalamt*. BUND.DE - Behörden Und Institutionen Des Bundes.

<http://www.bund.de/Content/DE/DEBehoerden/XYZ/ZKA/Zollkriminalamt.html?nn=4641496&searchResult=true&templateQueryString=zollkriminalamt>

Bundesamt fuer Verfassungsschutz. (2017). *Gemeinsames Terrorismusabwehrzentrum (GTAZ)*.

<https://www.verfassungsschutz.de/de/arbeitsfelder/af-islamismus-und-islamistischer-terrorismus/gemeinsames-terrorismusabwehrzentrum-gtaz>

Bundesamt für Migration und Flüchtlinge. (2017). *Organigramm*.

Bundesamt Für Migration Und Flüchtlinge.

[http://www.bamf.de/DE/DasBAMF/Aufbau/Organigramm/organigramm-node.html;jsessionid=9877A28A093783324F3E20334D47F5D5.1\\_cid368](http://www.bamf.de/DE/DasBAMF/Aufbau/Organigramm/organigramm-node.html;jsessionid=9877A28A093783324F3E20334D47F5D5.1_cid368)

Bundesamt für Verfassungsschutz. (2017a). *Die Organisation des Amtes ist*

*kein Geheimnis*. Bundesamt Für Verfassungsschutz.

<https://www.verfassungsschutz.de/de/das-bfv/aufgaben/die-organisation-des-amtes-ist-kein-geheimnis>

Bundesamt für Verfassungsschutz. (2017b). *Gemeinsames Internetzentrum (GIZ)*. <https://www.verfassungsschutz.de/de/arbeitsfelder/af-islamismus-und-islamistischer-terrorismus/gemeinsames-internetzentrum-giz>

Bundesamt für Verfassungsschutz. (2017c). *Was genau macht der Verfassungsschutz?* Bundesamt Für Verfassungsschutz. <https://www.verfassungsschutz.de/de/das-bfv/aufgaben/was-genau-macht-der-verfassungsschutz>

Bundeskriminalamt. (2021). *Organigramm des BKA*. Bka.De. [https://www.bka.de/SharedDocs/Downloads/DE/DasBKA/Organisation\\_Aufbau/organigramm\\_neu.html](https://www.bka.de/SharedDocs/Downloads/DE/DasBKA/Organisation_Aufbau/organigramm_neu.html)

Bundesnachrichtendienst. (2017). *Aufgaben*. Bundesnachrichtendienst. [http://www.bnd.bund.de/DE/Auftrag/Aufgaben/aufgaben\\_node.html;jsessionid=B2B4AC8EE74ACF1D27D7C48A86620B7D.2\\_cid386](http://www.bnd.bund.de/DE/Auftrag/Aufgaben/aufgaben_node.html;jsessionid=B2B4AC8EE74ACF1D27D7C48A86620B7D.2_cid386)

Bundesnachrichtendienst. (2021). *Abteilungen des BND*. Bnd.De. [https://www.bnd.bund.de/DE/Der\\_BND/Abteilungen/abteilungen\\_node.html](https://www.bnd.bund.de/DE/Der_BND/Abteilungen/abteilungen_node.html)

Bundespolizei. (2017a). *GSG 9 der Bundespolizei*. [https://www.bundespolizei.de/Web/DE/05Die-Bundespolizei/04Einsatzkraefte/03\\_GSG9/GSG9\\_node.html](https://www.bundespolizei.de/Web/DE/05Die-Bundespolizei/04Einsatzkraefte/03_GSG9/GSG9_node.html)

Bundespolizei. (2017b). *Vorstellung der neuen Einheit "BFE+ der Bundespolizei" für besondere Gefährdungs- oder*

*Fahndungslagen*. Bundespolizei.

[https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2015/12/151216\\_bfe+.html](https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2015/12/151216_bfe+.html)

Bundeswehr. (2017). *Aktuelle Einsätze der Bundeswehr*.

[http://www.einsatz.bundeswehr.de/portal/a/einsatzbw/start/aktuelle\\_einsaetze!/ut/p/z1/04\\_Sj9CPykssy0xPLMnMz0vMAfIjo8zinSx8QnyMLI2MXEJCHQ08XU0N\\_IOdXYzdDczlwwkpiAJKG-AAjgb6wSmp-pFAM8xxmuFuqB-sH6UflZVYllihV5BfVJKTWqKXmAxyoX5kRmJeSk5qQH6yI0SgIDei3KDcUREAqeFHw](http://www.einsatz.bundeswehr.de/portal/a/einsatzbw/start/aktuelle_einsaetze!/ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zinSx8QnyMLI2MXEJCHQ08XU0N_IOdXYzdDczlwwkpiAJKG-AAjgb6wSmp-pFAM8xxmuFuqB-sH6UflZVYllihV5BfVJKTWqKXmAxyoX5kRmJeSk5qQH6yI0SgIDei3KDcUREAqeFHw)

Bunker, R. J. (2000). Weapons of mass disruption and terrorism. *Terrorism and Political Violence*, 12(1), 37–46.

<https://doi.org/10.1080/09546550008427548>

Bures, O. (2015). Political corporate social responsibility: Including high politics? *Journal of Business Ethics*, 129(3), 689–703.

Burke, P., & Feltes, J. (2017). *CT Overview: Germany*.

Counterterrorismethics.Com. <http://counterterrorismethics.com/the-counter-terrorism-landscape-in-germany/>

Cajani, F. (2018). “All Along the Watchtower”: Matters Not Yet Solved Regarding Communication Interception Systems and Electronic Data Retained on Foreign Servers. In M. A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci, & F. Turchi (Eds.), *Handling and Exchanging Electronic Evidence Across Europe* (pp. 59–71). Springer International Publishing. [https://doi.org/10.1007/978-3-319-74872-6\\_5](https://doi.org/10.1007/978-3-319-74872-6_5)

Callimachi, R., & Eddy, M. (2016). *Munich Killer Was Troubled, but Had*

- No Terrorist Ties, Germany Says*. The New York Times.  
<https://www.nytimes.com/2016/07/24/world/europe/munich-shooting-attack.html>
- Callimachi, R., Eddy, M., & Jacobs, A. (2016). *Gunman in Munich Kills 9, Then Himself, the Police Say*. The New York Times.  
[https://www.nytimes.com/2016/07/23/world/europe/munich-mall.html?\\_r=0](https://www.nytimes.com/2016/07/23/world/europe/munich-mall.html?_r=0)
- Capone, F. (2018). The EU Response to the CBRN Terrorism Threat: A Critical Overview of the Current Policy and Legal Framework. *Enhancing CBRNE Safety & Security: Proceedings of the SICC 2017 Conference*, 243–251.
- Cardash, M., & Johnston, A. (2014). That Mother of Satan is Highly Unstable! *CBRNe World*, 50–52.
- Carus, W. S. (2001). *Bioterrorism and biocrimes: the illicit use of biological agents since 1900*. NATIONAL DEFENSE UNIV WASHINGTON DC.
- Carus, W. S. (2012). *Defining weapons of mass destruction*. DTIC Document.
- Carus, W. S. (2017). *A Short History of Biological Warfare: From Pre-History to the 21st Century*.
- Caves Jr, J. P., & Carus, W. S. (2014). *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030*. DTIC Document.
- Chaussy, U. (1985). *Oktoberfest. Das Attentat: Wie die Verdrängung des Rechtsterrors begann*. Luchterhand.

- Coady, C. A. J. (1985). The morality of terrorism. *Philosophy*, 60(231), 47–69.
- Cohen-Almagor, R. (2015). *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway*. Cambridge University Press. <https://doi.org/DOI: 10.1017/CBO9781316226391>
- Conway, M., Parker, J., & Looney, S. (2017). Online jihadi instructional content: the role of magazines. In M. Conway, L. Jarvis, O. Lehané, S. Macdonald, & L. Nouri (Eds.), *Terrorists' Use of the Internet: Assessment and Response* (pp. 182–193). IOS Press.
- Copeland, S., Comes, T., Bach, S., Nagenborg, M., Schulte, Y., & Doorn, N. (2020). Measuring social resilience: Trade-offs, challenges and opportunities for indicator models in transforming societies. *International Journal of Disaster Risk Reduction*, 51, 101799.
- Cragin, K. (2007). *Sharing the dragon's teeth: Terrorist groups and the exchange of new technologies* (Vol. 485). Rand Corporation.
- Cragin, K., Daly, S. A., Everingham, S. S., Hoube, J., Kilburn, M. R., & Marcum, C. Y. (2004). *The dynamic terrorist threat: An assessment of group motivations and capabilities in a changing world*. Rand Corporation.
- Cronon, E. D., & Jenkins, J. W. (1999). *University of Wisconsin: Renewal to Revolution, 1945-1971* (Vol. 4). Univ of Wisconsin Press.
- Crowley, M. (2013). Exploring the Role of Life Scientists in Combating the Misuse of Incapacitating Chemical and Toxin Agents. In B. Rappert & M. Selgelid (Eds.), *On the Dual Uses of Science and Ethics: Principles, Practices and Prospects* (pp. 293–330). ANU Press.

- Daily Mail. (2012). *Anders Behring Breivik arrested over “holiday island massacre.”* Daily Mail Online.  
<http://www.dailymail.co.uk/news/article-2017709/Anders-Behring-Breivik-arrested-holiday-island-massacre.html>
- Daly, S., Parachini, J., & Rosenau, W. (2005). *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism*. DTIC Document.
- Danzig, R., Sageman, M., Leighton, T., Hough, L., Yuki, H., Kotani, R., & Hosford, Z. M. (2011). *Aum Shinrikyo. Insights into How Terrorists Develop Biological and Chemical Weapons*.
- Davidson, D. (1980). Agency (1971). In D. Davidson (Ed.), *Essays on actions and events: Philosophical essays* (pp. 43–62). Oxford University Press.
- de Graaf, B. (2003). *Why Communication and Performance are Key in Countering Terrorism*.
- de Graaff, B. (2012). *Op weg naar Armageddon: de evolutie van fanatisme*. Boom.
- de Graaff, B. (2016). IS and its Predecessors: Violent Extremism in Historical Perspective. *Perspectives on Terrorism*, 10(5), 96–103.
- Department of Homeland Security. (2017). *Chemical Sector-Specific Agency*. Cisa.Gov.  
<https://www.cisa.gov/sites/default/files/publications/chemical-ssa-fact-sheet-2017-508.pdf>
- Department of Homeland Security. (2018a). *Bomb-Making Materials*

- Awareness Program (BMAP)*. DHS. <https://www.dhs.gov/bmap>
- Department of Homeland Security. (2018b). *If You See Something, Say Something<sup>TM</sup>*. DHS. <https://www.dhs.gov/see-something-say-something>
- Department of Homeland Security. (2019). *Chemical Facility Anti-Terrorism Standards*. <https://www.dhs.gov/cisa/chemical-facility-anti-terrorism-standards>
- Department of Homeland Security. (2020). *Chemical Security Analysis Center*. Dhs.Gov. <https://www.dhs.gov/science-and-technology/csac>
- Deutsche Welle. (2014). *Man accused of plotting Bonn station bombing*. DW Online. <http://www.dw.com/en/man-accused-of-plotting-bonn-station-bombing/a-17498279>
- Deutsche Welle. (2016). *Man who stabbed mayor of Cologne sentenced to 14 years in jail*. DW Online. <http://www.dw.com/en/man-who-stabbed-mayor-of-cologne-sentenced-to-14-years-in-jail/a-19371698>
- Deutsche Welle. (2018). *Die neue Sorge vor der Bio-Bombe*. Dw.De. <https://www.dw.com/de/die-neue-sorge-vor-der-biobombe/a-44326086>
- Deutscher Presserat. (1997). *Pressekodex*. Presserat.De. <https://www.presserat.de/pressekodex.html>
- Dickstein, P., & Vanunu, S. (2016). *Nuclear Terror: The Essentials, Threats, Effects and Resilience*.
- Dinesen, P. T., & Jæger, M. M. (2013). The Effect of Terror on Institutional Trust: New Evidence from the 3/11 Madrid Terrorist Attack. *Political Psychology*, 34(6), 917–926.
- Dolnik, A. (2007). *Understanding terrorist innovation: Technology, tactics*

*and global trends*. Routledge.

- Doorn, N. (2017). Resilience indicators: Opportunities for including distributive justice concerns in disaster management. *Journal of Risk Research*, 20(6), 711–731.
- Doorn, N., Gardoni, P., & Murphy, C. (2019). A multidisciplinary definition and evaluation of resilience: The role of social justice in defining resilience. *Sustainable and Resilient Infrastructure*, 4(3), 112–123.
- Drake, C. J. M. (1998). The role of ideology in terrorists' target selection. *Terrorism and Political Violence*, 10(2), 53–85.
- Dukic, S. (2017). Islamic State's Weapons of Mass Destruction Capability: An Open Source Intelligence Approach. In M. Martellini & J. Rao (Eds.), *The Risk of Skilled Scientist Radicalization and Emerging Biological Warfare Threats* (Vol. 138, p. 30). IOS Press.
- Dunn, L. A., DeMarce, A., Givner-Forbes, R., Grosiak, A., Kovner, M., Lukasik, S. J., Moran, N., Skypek, T., Yengst, W., & Perry, J. L. (2008). *Next Generation Weapons of Mass Destruction and Weapons of Mass Effects Terrorism*.
- Early, B. R., Martin, E. G., Nussbaum, B., & Deloughery, K. (2017). Should conventional terrorist bombings be considered weapons of mass destruction terrorism? *Dynamics of Asymmetric Conflict*, 10(1), 54–73. <https://doi.org/10.1080/17467586.2017.1349327>
- ECHA. (2019). *Phosphine - Substance Information*. <https://echa.europa.eu/substance-information/-/substanceinfo/100.029.328>



- Ehni, H.-J. (2008). Dual use and the ethical responsibility of scientists. *Archivum Immunologiae et Therapiae Experimentalis*, 56(3), 147–152. <https://doi.org/10.1007/s00005-008-0020-7>
- Eid, M. (2014). *Exchanging terrorism oxygen for media airwaves: The age of terroredia: The age of terroredia*. IGI Global.
- Enemark, C. (2011). Farewell to WMD: The Language and Science of Mass Destruction. *Contemporary Security Policy*, 32(2), 382–400. <https://doi.org/10.1080/13523260.2011.590362>
- Enemark, C. (2012). The Unfinished Business of Abandoning WMD: A Reply to Bentley. *Contemporary Security Policy*, 33(2), 407–412. <https://doi.org/10.1080/13523260.2012.693806>
- English, R. (2016). *Does Terrorism Work?* Oxford University Press.
- Environmental Protection Agency. (2019). *Americium in Ionization Smoke Detectors*. <https://www.epa.gov/radtown/americium-ionization-smoke-detectors>
- Erlanger, S., & Shane, S. (2011). *Norway Shooting and Bomb Attack Leaves at Least 92 Dead*. The New York Times. <http://www.nytimes.com/2011/07/24/world/europe/24oslo.html>
- Etchegary, H., Lee, J. E. C., Lemyre, L., & Krewski, D. (2008). Canadians' Representation of Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Terrorism: A Content Analysis. *Human and Ecological Risk Assessment: An International Journal*, 14(3), 479–494. <https://doi.org/10.1080/10807030802073776>
- European Commission. (2006). *5th Report of the Standing Working Group*

*on Safe Transport of Radioactive Materials in the European Union.*

European Commission. (2018). *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document proposal for a Regulation of the European Parliament and of the Council on the marketing and use of explosives precursors, amending Annex XVII to Regulation (EC) No 1907/2006 an.*

[https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180417\\_regulation-proposal-eu-parl-council-marketing-use-explosive-precursors-cswd-ia\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180417_regulation-proposal-eu-parl-council-marketing-use-explosive-precursors-cswd-ia_en.pdf)

Europol. (2015). *Europol's Internet Referral Unit to combat terrorist and violent extremist propaganda / Europol.* Europol.

<https://www.europol.europa.eu/newsroom/news/europol's-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda>

Europol. (2016). *EU Internet Referral Unit. Year One Report. Highlights.*

<https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights>

Evans, N. (2013). Contrasting Dual-Use Issues in Biology and Nuclear Science. In M. J. Selgelid (Ed.), *On the Dual Uses of Science and Ethics: Principles, Practices and Prospects* (pp. 255–274). ANU E Press.

Evans, N. G. (2014). Dual-use decision making: relational and positional issues. *Monash Bioethics Review*, 32(3–4), 268–283.

Eyison, R. K., Pakdemirli, A., Aydin, E., Ozturk, A. S., Kilic, Z., Demirbag, B., Ortatatli, M., Sezigen, S., & Kenar, L. (2020). Evaluation of the Medical Chemical, Biological, Radiological, and Nuclear Awareness

- Level of Emergency Healthcare Professionals Serving on Different Centres. *Journal of Basic and Clinical Health Sciences*, 4(2), 174–179.
- Faulconbridge, G., & Holden, M. (2018). Explainer: The poisoning of former Russian double agent Sergei Skripal. *Reuters.Com*.
- Fellner, M. (1986). The Untold Story. After 15 Years, Dwight And Karl Armstrong Reveal The Drama Behind The Anti-Vietnam War Bombings in Madison Part 2. *The Milwaukee Journal*, 8–19.
- Feltes, J. (2015). *Semtex in the hand is worth two dirty bombs in the bush. The historical relation between explosive technology and terrorism*. Unpublished thesis, Utrecht University.
- Fisher, A. (2015). How Jihadist Networks Maintain a Persistent Online Presence. *Perspectives on Terrorism; Vol 9, No 3 (2015): Perspectives on Terrorism*.  
<http://www.terrorismanalysts.com/pt/index.php/pot/article/view/426>
- Flade, F. (2016). The Islamic State Threat to Germany: Evidence from the Investigations. *CTC Sentinel*, 9(7), 11–14.
- Flade, F. (2018). The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror. *CTC Sentinel*, 1–4.
- Forest, J. F. (2006). *Teaching terror: Strategic and tactical learning in the terrorist world*. Rowman & Littlefield Publishers.
- Forest, J. J. F. (2008). Knowledge Transfer and Shared Learning among Armed Groups. In J. H. Norwitz (Ed.), *Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency* (pp. 269–289). Dept. of the Navy.

- Forest, J. J. F. (2012). Framework for Analyzing the Future Threat of WMD Terrorism. *Journal of Strategic Security*, 5(4), 51.
- Forge, J. (2010). A Note on the Definition of “Dual Use”.” *Science and Engineering Ethics*, 16(1), 111–118. <https://doi.org/10.1007/s11948-009-9159-9>
- Frankfurter Rundschau. (2011). *Geigerzähler in Bürgerhand - sinnvoll oder nicht?* <https://www.fr.de/ratgeber/geld/geigerzaehler-buergerhand-sinnvoll-oder-nicht-11696313.html>
- French, P. A. (1979). The corporation as a moral person. *American Philosophical Quarterly*, 16(3), 207–215.
- French, P. A. (1987). *Collective and corporate responsibility*.
- Geys, B., & Qari, S. (2017). Will you still trust me tomorrow? The causal effect of terrorism on social trust. *Public Choice*, 173(3), 289–305.
- Gilbert, M. (2006). Who’s to blame? Collective moral responsibility and its implications for group members. *Midwest Studies in Philosophy*, 30(1), 94–114.
- Gould, E. D., & Klor, E. F. (2010). Does terrorism work? *The Quarterly Journal of Economics*, 125(4), 1459–1510.
- Gouweloos, J., Dückers, M., Te Brake, H., Kleber, R., & Drogendijk, A. (2014). Psychosocial care to affected citizens and communities in case of CBRN incidents: a systematic review. *Environment International*, 72, 46–65.
- Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*, 72(5), 1–8.

- Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, 3(1), 49–58.
- Grunwald, A. (2008). Nanoparticles: Risk Management and the Precautionary Principle. In F. Jotterand (Ed.), *Emerging Conceptual, Ethical and Policy Issues in Bionanotechnology* (pp. 85–102). Springer Netherlands. [https://doi.org/10.1007/978-1-4020-8649-6\\_6](https://doi.org/10.1007/978-1-4020-8649-6_6)
- Grunwald, A. (2015). Technology Assessment Technology Assessment and Design for Values. In *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains* (pp. 67–86).
- Gunn, D. (2016). *Does the MTA's 'If You See Something Say Something' Campaign Make Us Less Safe?* New York Magazine. <http://nymag.com/news/intelligencer/mta-anti-terrorism-2012-10/>
- Gurjar, M., Baronia, A. K., Azim, A., & Sharma, K. (2011). Managing aluminum phosphide poisonings. *Journal of Emergencies, Trauma and Shock*, 4(3), 378.
- Haensgen, M. (2017). *Internetfirmen gehen gegen Terrorpropaganda vor*. Schwaebische. [http://www.schwaebische.de/politik/ausland\\_artikel,-Internetfirmen-gehen-gegen-Terrorpropaganda-vor-\\_arid,10590647.html](http://www.schwaebische.de/politik/ausland_artikel,-Internetfirmen-gehen-gegen-Terrorpropaganda-vor-_arid,10590647.html)
- Harris, P. (2011). *Norway attacks: At least 80 feared dead in double attack on Oslo and Utoya*. Daily Mail Online. <http://www.dailymail.co.uk/news/article-2017902/Norway-attacks-At-80-feared-dead-double-attack-Oslo-Utoya.html>

- Hemmingby, C., & Bjørge, T. (2018). Terrorist Target Selection: The Case of Anders Behring Breivik. *Perspectives on Terrorism*, 12(6), 164–176.
- Hemphill, T. A. (2003). Corporate responsibility and the war on terrorism. *Business Horizons*, 46(3), 13.
- House, C. N. (2016). The Chemical, Biological, Radiological, and Nuclear Terrorism Threat from the Islamic State. *Military Review*, 96(5), 68–75.
- Hudson, A. (2014). *German Islamist charged over failed Bonn station attack in 2012*. Reuters. <http://www.reuters.com/article/us-germany-islamist-idUSBREA2D1BA20140314>
- Hummel, S. (2016). The Islamic State and WMD: assessing the future threat. *CTC Sentinel*, 9(13), 18–21.
- IAEA. (2016). *Radiation Safety for Consumer Products (Specific Safety Guide SSG-36)*.
- ICRC. (2016). *Principle of Proportionality in the Rules Governing the Conduct of Hostilities Under International Humanitarian Law*.
- International Atomic Energy Agency. (1998). *The Radiological Accident in Goiania*.
- Ivanova, K., & Sandler, T. (2006). CBRN incidents: Political regimes, perpetrators, and targets. *Terrorism and Political Violence*, 18(3), 423–448.
- Ivanova, K., & Sandler, T. (2007). CBRN Attack Perpetrators: An Empirical Study. *Foreign Policy Analysis*, 3(4), 273–294.

<https://doi.org/10.1111/j.1743-8594.2007.00051.x>

- Jackson, B. A. (2001). Technology acquisition by terrorist groups: threat assessment informed by lessons from private sector technology adoption. *Studies in Conflict and Terrorism*, 24(3), 183–213.
- Jackson, B. A., & Frelinger, D. R. (2008). Rifling Through the Terrorists' Arsenal: Exploring Groups' Weapon Choices and Technology Strategies. *Studies in Conflict & Terrorism*, 31(7), 583–604.
- James, L. C., & Oroszi, T. L. (2015). *Weapons of Mass Psychological Destruction and the People Who Use Them*. Praeger.
- Jaspers, K. (1946). *Die Schuldfrage: Ein Beitrag zur deutschen Frage* (Vol. 11). Artemis-verlag.
- Johansen, M.-L., Sandrup, T., & Weiss, N. (2018). Introduction: the generative power of political emotions. *Conflict and Society*, 4(1), 1–8.
- Kaati, L., & Johansson, F. (2016). Countering lone actor terrorism: weak signals and online activities. *Understanding Lone Actor Terrorism: Past Experience, Future Outlook, and Response Strategies*. Abingdon, UK: Routledge, 266–279.
- Kamm, F. M. (2011). *Ethics for Enemies: Terror, Torture, and War*. Oxford University Press.
- Kant, L., & Mourya, D. T. (2010). Managing Dual Use Technology: It Takes Two to Tango. *Science and Engineering Ethics*, 16(1), 77–83.  
<https://doi.org/10.1007/s11948-008-9062-9>
- Kenney, M. (2010). Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists. *Terrorism and Political*

- Violence*, 22(2), 177–197. <https://doi.org/10.1080/09546550903554760>
- Khripunov, I. (2006). The social and psychological impact of radiological terrorism. *Nonproliferation Review*, 13(2), 275–316.
- Kock, P. de. (2014). *Anticipating criminal behaviour : using the narrative in crime-related data*. Wolf Legal Publishers (WLP).
- Koehler-Derrick, G., & Milton, D. J. (2017). Choose Your Weapon: The Impact of Strategic Considerations and Resource Constraints on Terrorist Group Weapon Selection. *Terrorism and Political Violence*, 1–20. <https://doi.org/10.1080/09546553.2017.1293533>
- Koehler, D., & Popella, P. (2018). Mapping Far-right Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism Efforts in the West: Characteristics of Plots and Perpetrators for Future Threat Assessment. *Terrorism and Political Violence*, 1–25.
- Kuhlau, F., Eriksson, S., Evers, K., & Höglund, A. T. (2008). Taking due care: moral obligations in dual use research. *Bioethics*, 22(9), 477–487.
- Kuhlau, F., Höglund, A. T., Eriksson, S., & Evers, K. (2013). The ethics of disseminating dual-use knowledge. *Research Ethics*, 9(1), 6–19.
- LaFree, G., Dugan, L., & Miller, E. (2014). *Putting terrorism in context: Lessons from the Global Terrorism Database*. Routledge.
- Lakoff, A. (2007). Preparing for the next emergency. *Public Culture*, 19(2), 247.
- Larsson, S. (2017). A First Line of Defence? Vigilant surveillance, participatory policing, and the reporting of “suspicious” activity. *Surveillance and Society*, 15(1), 94–107.



- Lemyre, L., Clément, M., Corneil, W., Craig, L., Boutette, P., Tyshenko, M., Karyakina, N., Clarke, R., & Krewski, D. (2005). A psychosocial risk assessment and management framework to enhance response to CBRN terrorism threats and attacks. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 3(4), 316–330.
- Lévy, P., & Bononno, R. (1997). *Collective intelligence: Mankind's emerging world in cyberspace*. Perseus books.
- Lewis, H. D. (1948). Collective responsibility. *Philosophy*, 23(84), 3–18.
- Louis, R. (2018). Straddling the Liminal Space Section 810.01 3 Recognizance: Preventative Justice Or Preventing Justice. *WJ Legal Stud.*, 8, 1.
- Madeira, J. L. (2012). *Killing McVeigh: The death penalty and the myth of closure*. NYU Press.
- Madison Capital Times. (1970, September 3). Text of FBI affidavit in UW bombing. *Madison Capital Times*.
- Mäkelä, P. (2013). *Collective Responsibility: Against Collectivism* (Vol. 24).
- Mala, E., & Goodman, J. D. (2011). *At Least 80 Dead in Norway Shooting*. The New York Times.  
<http://www.nytimes.com/2011/07/23/world/europe/23oslo.html>
- Malone, T. W., Laubacher, R., & Dellarocas, C. (2009). *Harnessing crowds: Mapping the genome of collective intelligence*.
- Marchant, G. E., & Pope, L. L. (2009). The Problems with Forbidding Science. *Science and Engineering Ethics*, 15(3), 375–394.

<https://doi.org/10.1007/s11948-009-9130-9>

Marris, C., Jefferson, C., & Lentzos, F. (2014). Negotiating the dynamics of uncomfortable knowledge: The case of dual use and synthetic biology. *BioSocieties*, 9(4), 393–420.

McMahan, J. (2009). Intention, permissibility, terrorism, and war. *Philosophical Perspectives*, 23(1), 345–372.

Mele, A. R. (1992). *Springs of action: Understanding intentional behavior*. Oxford University Press.

Mele, A. R., & Moser, P. (1997). Intentional Action. In A. R. Mele (Ed.), *The Philosophy of Action* (pp. 223–255). Oxford University Press.

Mendel, T. (2003). Freedom of information as an internationally protected human right. *Comparative Media Law Journal*, 1(1), 39–70.

Meyer, B. (2004). Fighting Terrorism—A Narrow Path between Saving Security and Losing Liberty. *Globalization, Armed Conflicts and Security*.

Mihr, A. (2017). Shrinking Space. In A. Mihr (Ed.), *Cyber Justice: Human Rights and Good Governance for the Internet* (pp. 45–56). Springer.

Mika, O. J., & Fiserova, L. (2011). Brief overview of chemical terrorism and its consequences. *Toxin Reviews*, 30(4), 115–121.  
<https://doi.org/10.3109/15569543.2011.594784>

Militärischer Abschirmdienst (MAD). (2017). *Über uns*. Dienststellen Der Streitkräftebasis.  
[http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/start/weitdstst/mad/ueberuns/!ut/p/z1/04\\_Sj9CPykssy0xPLMnMz0vMAfIjo8zinS](http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/start/weitdstst/mad/ueberuns/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zinS)

x8QnyMLI2MXAJcjQw8jT3CTIOc\_A18zY31wwkpiAJKG-  
AAjgb6wSmp-pFAM8xxmuFnph-  
sH6UflZVYllihV5BfVJKTWqKXmAxyoX5kRmJeSk5qQH6yI0SgID  
ei3KD

Miller, S. (in press). Moral Injury, Moral Identity and ‘Dirty Hands’ in War Fighting and Police Work. *Journal of Medicine and Philosophy*.

Miller, S. (1995). Intentions, Ends, and Joint Action. *Philosophical Papers*, 24(1), 51–66.

Miller, S. (2001). *Social action: A teleological account*. Cambridge University Press.

Miller, S. (2006). Collective Moral Responsibility: An Individualist Account. *Midwest Studies In Philosophy*, 30(1), 176–193.

Miller, S. (2008). *Terrorism and counter-terrorism: Ethics and liberal democracy*. Blackwell Publishing Ltd.

Miller, S. (2012). F. M. Kamm, Ethics for Enemies: Terror, Torture and War. In *Notre Dame Philosophical Reviews*.

Miller, S. (2013). Moral Responsibility, Collective-Action Problems and the Dual-Use Dilemma in Science and Technology. In M. J. Selgelid & B. Rappert (Eds.), *On the Dual Uses of Science and Ethics: Principles, Practices and Prospects* (pp. 185–206). ANU E Press.

Miller, S. (2014). Police Detectives, Criminal Investigations and Collective Moral Responsibility. *Criminal Justice Ethics*, 33(1), 21–39.  
<https://doi.org/10.1080/0731129X.2014.906094>

Miller, S. (2015). Design for values in institutions. In *Handbook of Ethics*,

- Values, and Technological Design: Sources, Theory, Values and Application Domains* (pp. 1–11). Springer.
- Miller, S. (2016). *Shooting to Kill: The Ethics of Police and Military Use of Lethal Force*. Oxford University Press.
- Miller, S. (2018). *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Springer Science & Business Media.
- Miller, S., & Feltes, J. (2018). Chemical Industry. In *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction* (pp. 55–71). Springer Science & Business Media.
- Miller, S., & Mäkelä, P. (2005). The collectivist approach to collective moral responsibility. *Metaphilosophy*, 634–651.
- Miller, S., & Selgelid, M. J. (2007). Ethical and philosophical consideration of the dual-use dilemma in the biological sciences. *Science and Engineering Ethics*, 13(4), 523–580.
- Molotch, H. (2014). *Against security: How we go wrong at airports, subways, and other sites of ambiguous danger*. Princeton University Press.
- Moser-Knierim, A. (2013). *Vorratsdatenspeicherung: Zwischen Überwachungsstaat und Terrorabwehr*. Springer-Verlag.
- Motzkus, K.-H., Häusler, U., & Dollan, R. (2012). *Wissenswertes über hochradioaktive Strahlenquellen*.  
[http://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-2012112610240/3/BfS\\_2012\\_SG-17-12.pdf](http://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-2012112610240/3/BfS_2012_SG-17-12.pdf)
- Mueller, J., & Stewart, M. G. (2015). Terrorism, counterterrorism, and the

- Internet: The American cases. *Dynamics of Asymmetric Conflict*, 8(2), 176–190.
- Mythen, G., & Walklate, S. (2006). Communicating the terrorist risk: Harnessing a culture of fear? *Crime, Media, Culture*, 2(2), 123–142.  
<https://doi.org/10.1177/1741659006065399>
- Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2018). *Precursoren voor explosieven*. NCTV.  
[https://www.nctv.nl/onderwerpen\\_a\\_z/precursoren\\_voor\\_explosieven/index.aspx](https://www.nctv.nl/onderwerpen_a_z/precursoren_voor_explosieven/index.aspx)
- National Center for Biotechnology Information. (2019). *Phosphine*, CID=24404. PubChem Database.  
<https://pubchem.ncbi.nlm.nih.gov/compound/Phosphine>
- National Research, C., Division on, E., Life, S., Forrest, S., & Lange, M. (2014). *An all-of-government approach to increase resilience for international chemical, biological, radiological, nuclear, and explosive (CBRNE) events : workshop summary*.  
[http://www.nap.edu/catalog.php?record\\_id=18814](http://www.nap.edu/catalog.php?record_id=18814)
- Nesser, P., Stenersen, A., & Oftedal, E. (2016). Jihadi Terrorism in Europe: The IS-Effect. *Perspectives on Terrorism*, 10(6).
- New Year's Gang. (1970). Statement concerning UW bombing. *Kaleidoscope*, 2(17), 1.
- Ni Loideain, N. (2015). EU law and mass internet metadata surveillance in the post-Snowden era. *A Revised Version of This Paper Will Be in Media and Communications-Special Issue on Surveillance: Critical Analysis and Current Challenges (2015), Forthcoming*.

- Nixdorff, K. (2013). Education for Life Scientists on the Dual-Use Implications of Their Research. *Science and Engineering Ethics*, 19(4), 1487–1490.
- North Atlantic Treaty Organization. (2014). *AAP-6 NATO Glossary of Terms and Definitions*.
- NTI. (2021). *National Threat Initiative*. Nti.Org. <https://www.nti.org/>
- O'Connor, T., & Sandis, C. (2011). *A Companion to the Philosophy of Action*. John Wiley & Sons.
- O'Haver, H. (2016). *How 'if you see something, say something' became our national motto*. The Washington Post. [https://www.washingtonpost.com/posteverything/wp/2016/09/23/how-if-you-see-something-say-something-became-our-national-motto/?utm\\_term=.16b02f1c7fb5](https://www.washingtonpost.com/posteverything/wp/2016/09/23/how-if-you-see-something-say-something-became-our-national-motto/?utm_term=.16b02f1c7fb5)
- O'Mara, E. M., Jackson, L. E., Batson, C. D., & Gaertner, L. (2011). Will moral outrage stand up?: Distinguishing among emotional reactions to a moral violation. *European Journal of Social Psychology*, 41(2), 173–179.
- OPCW. (2016). *Third report of the Organization for the Prohibition of Chemical Weapons-United Nations Joint Investigative Mechanism 3/98 16-14788*.
- OPCW. (2021). *Organisation for the Prohibition of Chemical Weapons*. Opcw.Org. <https://www.opcw.org/>
- Organisation for the Prohibition of Chemical Weapons. (1992). *Convention on the Prohibition of the Development, Production, Stockpiling and*

*Use of Chemical Weapons and on their Destruction.*

- Pabst, S. (2015). *BFE plus: Deutschlands neue Anti-Terror-Einheit / Deutschland*. Deutsche Welle. <http://www.dw.com/de/bfe-plus-deutschlands-neue-anti-terror-einheit/a-18921189>
- Palmer, I. (2004). The psychological dimension of chemical, biological, radiological and nuclear (CBRN) terrorism. *Journal of the Royal Army Medical Corps*, 150(1), 3–9.
- Parachini, J. (2003). Putting WMD terrorism into perspective. *The Washington Quarterly*, 26(4), 37–50.  
<https://doi.org/10.1162/016366003322387091>
- Parachini, J. V. (2001). Comparing motives and outcomes of mass casualty terrorism involving conventional and unconventional weapons. *Studies in Conflict and Terrorism*, 24(5), 389–406.
- Parakrama 'gura 'gurusinghe. (2014). *FUMIGANTS: PHOSPHINE AND PHOSPHINE-GENERATING COMPOUNDS RISK CHARACTERIZATION DOCUMENT* Environmental Fate.  
<http://www.cdpr.ca.gov/docs/emon/pubs/fatememo/phosphine.pdf>
- Pearce, J. M., Rubin, G. J., Selke, P., Amlôt, R., Mowbray, F., & Rogers, M. B. (2013). Communicating with the public following radiological terrorism: results from a series of focus groups and national surveys in Britain and Germany. *Prehospital and Disaster Medicine*, 28(02), 110–119.
- Petersen, K. L. (2008). Risk, responsibility and roles redefined: is counterterrorism a corporate responsibility? *Cambridge Review of International Affairs*, 21(3), 403–420.

- Pettit, P. (2007). Responsibility incorporated. *Ethics*, 117(2), 171–201.
- Pichtel, J. (2011). *Terrorism and WMDs. Awareness and Response*. CRC Press.
- Pillar, P. R. (2006). Intelligence, policy, and the war in Iraq. *Foreign Affairs*, 15–27.
- Pita Pita, R., Domingo Álvarez, J., Aizpurua Sánchez, C., González Domínguez, S., Cique Moya, A., Sopesen Veramendi, J. L., Gil García, M., Pérez, J., del Valle, M., & Ybarra de Villavicencio, C. (2004). Extracción de ricina por procedimientos incluidos en publicaciones paramilitares y manuales relacionados con la red terrorista Al Qaeda. *Med. Mil*, 60(3), 172–175.
- Primoratz, I. (1997). The Morality of Terrorism. *Journal of Applied Philosophy*, 14(3), 221–233. <https://doi.org/10.1111/1468-5930.00059>
- Quandt, T., Frischlich, L., Boberg, S., & Schatto-Eckrodt, T. (2019). Fake news. *The International Encyclopedia of Journalism Studies*, 1–6.
- Quillen, C. (2016). The Islamic State’s Evolving Chemical Arsenal. *Studies in Conflict & Terrorism*, 39(11), 1019–1030. <https://doi.org/10.1080/1057610X.2016.1154364>
- Quinn, W. S. (1989). Actions, intentions, and consequences: The doctrine of doing and allowing. *The Philosophical Review*, 98(3), 287–312.
- Ranstorp, M., & Normark, M. (2009). *Unconventional weapons and international terrorism: challenges and new approaches*. Routledge.
- Rappert, B., & McLeish, C. (2012). *A web of prevention: Biological weapons, life sciences and the governance of research*. Routledge.



- Rath, C. (2015). Ermittlungen nach Reker-Attentat: „Gefahr für das Ansehen der Bundesrepublik im Ausland“. *Koelner Stadtanzeiger*. <http://www.ksta.de/koeln/gefahr-fuer-das-ansehen-der-bundesrepublik-im-ausland-sote-23078416>
- Ravndal, J. A. (2015). Thugs or Terrorists? A Typology of Right-Wing Terrorism and Violence in Western Europe. *Journal for Deradicalization*, 3, 1–38.
- Rebera, A. P., & Rafalowski, C. (2014). On the Spot Ethical Decision-Making in CBRN (Chemical, Biological, Radiological or Nuclear Event) Response. *Science and Engineering Ethics*, 20(3), 735–752. <https://doi.org/10.1007/s11948-014-9520-5>
- Reed, A., & Ingram, H. (2019). *Towards a Framework for Post-Terrorist Incident Communications Strategies*.
- Reeves, J. (2012). If you see something, say something: Lateral surveillance and the uses of responsibility. *Surveillance & Society*, 10(3/4), 235.
- Revill, J. (2016). *Improvised Explosive Devices: the paradigmatic weapon of new wars*. Springer.
- Rheinische Post. (2019). *Düsseldorf: Rizin-Anschlagspläne waren weit fortgeschritten*. Rheinische Post. [https://rp-online.de/nrw/staedte/koeln/duesseldorf-rizin-anschlagsplaene-waren-weit-fortgeschritten\\_aid-39751823](https://rp-online.de/nrw/staedte/koeln/duesseldorf-rizin-anschlagsplaene-waren-weit-fortgeschritten_aid-39751823)
- Rodin, D. (2004). Terrorism without intention. *Ethics*, 114(4), 752–771.
- Roeser, S., Hillerbrand, R., Sandin, P., & Peterson, M. (Eds.). (2012). *Handbook of risk theory: Epistemology, decision theory, ethics, and*

*social implications of risk* (Vol. 1). Springer Science & Business Media.

- Rogers, M. B., Amlôt, R., & Rubin, G. J. (2013). The impact of communication materials on public responses to a radiological dispersal device (RDD) attack. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 11(1), 49–58.
- Rubin, G. J., Chowdhury, A. K., & Amlôt, R. (2012). How to communicate with the public about chemical, biological, radiological, or nuclear terrorism: a systematic review of the literature. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 10(4), 383–395.
- Ruggiero, A., & Vos, M. (2015a). Communication challenges in CBRN terrorism crises: Expert perceptions. *Journal of Contingencies and Crisis Management*, 23(3), 138–148.
- Ruggiero, A., & Vos, M. (2015b). Communication Challenges in CBRN Terrorism Crises: Expert Perceptions. *Journal of Contingencies and Crisis Management*, 23(3), 138–148. <https://doi.org/10.1111/1468-5973.12065>
- Ryan, J. (2007). *Countering militant Islamist radicalisation on the Internet: A user driven strategy to recover the Web*. IIEA.
- Rychnovská, D. (2016). Governing dual-use knowledge: From the politics of responsible science to the ethicalization of security. *Security Dialogue*, 47(4), 310–328.
- Sand, M. (2018). *Futures, Visions, and Responsibility. An Ethics of Innovation*. Springer.

- Satterfield, J. (2011). *When terrorists fight dirty: the likely magnitude of a terrorist radiological attack in the United States*. Georgetown University.
- Schmid, A. P. (2012). The revised academic consensus definition of terrorism. *Perspectives on Terrorism*, 6(2).
- Schmid, D. (2018). *Household internet access in the European Union (EU28) 2007-2017*.  
<https://www.statista.com/statistics/377585/household-internet-access-in-eu28/>
- Schwenkenbecher, A. (2014). Collateral Damage and the Principle of Due Care. *Journal of Military Ethics*, 13(1), 94–105.  
<https://doi.org/10.1080/15027570.2014.910015>
- Schwartz, M. (2019). *A Year After Skripal Poisoning, Russia Offers Defiant Face to Britain and the West*. The New York Times.  
<https://www.nytimes.com/2019/03/04/world/europe/russia-skripal-poisoning-britain.html>
- Selgelid, M. J., & Rappert, B. (Eds.). (2013). *On the dual uses of science and ethics: principles, practices, and prospects*. ANU E Press.
- Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber terrorism and public support for retaliation—a multi-country survey experiment. *British Journal of Political Science*, 1–19.
- Sidell, F. R., Takafuji, E. T., & Franz, D. R. (1997). *Medical aspects of chemical and biological warfare*. DTIC Document.
- Smiley, M. (2017). Collective Responsibility. In *Stanford Encyclopedia of*

*Philosophy.*

- Smithson, A., & Levy, L.-A. (2000). *Ataxia: The Chemical and Biological Terrorism Threat and the US Response*.
- Spencer, M. L., Kindt, M. T., & Stans, M. P. (2012). *Public Resilience in CBRN Events: Lessons Learned from Seven Cases*. DTIC Document.
- Spilcker, A. (2018). *Köln: Tunesier festgenommen: Wollte offenbar mit Giftanschlag Ungläubige töten*. Focus.  
[https://www.focus.de/politik/deutschland/koeln-er-wollte-offenbar-mit-einem-giftanschlag-die-unglaeubigen-toeten\\_id\\_9092406.html](https://www.focus.de/politik/deutschland/koeln-er-wollte-offenbar-mit-einem-giftanschlag-die-unglaeubigen-toeten_id_9092406.html)
- Staudenmaier, R. (2018). *German police carry out more raids in Cologne after charging man with making biological weapon*. Deutsche Welle.  
<https://www.dw.com/en/german-police-carry-out-more-raids-in-cologne-after-charging-man-with-making-biological-weapon/a-44236311>
- Steele, D. F., & Enemark, R. B. (1975). *Optical smoke detector*. Google Patents.
- Stenersen, A. (2009). Al-Qaeda's thinking on CBRN: A case study. In *Unconventional Weapons and International Terrorism* (pp. 62–76). Routledge.
- Strack, C. (2017). The Evolution of the Islamic State's Chemical Weapons Efforts. *CTC Sentinel*, 10(9), 19–23.
- Sullivan, G. R., & Bongar, B. (2007). Psychological consequences of actual or threatened CBRNE terrorism. In *Psychology of terrorism* (pp. 153–163).

- Szinicz, L. (2005). History of chemical and biological warfare agents. *Toxicology*, 214(3), 167–181.
- Taillard, M.-O. (2000). Persuasive communication: the case of marketing. *Working Papers in Linguistics*, 12, 145–174.
- Taillard, M.-O. (2002). Beyond communicative intention. *UCL Working Papers in Linguistics*, 14, 189–206.
- Taylor, M. (2011). *Breivik sent “manifesto” to 250 UK contacts hours before Norway killings*. The Guardian.  
<https://www.theguardian.com/world/2011/jul/26/breivik-manifesto-email-uk-contacts>
- The Irish Times. (2015). *Cologne mayor candidate stabbed and severely injured - police*. The Irish Times.  
<http://www.irishtimes.com/news/world/europe/cologne-mayor-candidate-stabbed-and-severely-injured-police-1.2396010>
- The Times of Israel. (2015). *Israel tests “dirty bombs,” finds they pose no substantial danger*. The Times of Israel.  
<http://www.timesofisrael.com/israeli-tests-find-dirty-bombs-pose-no-substantial-danger/>
- Theobalt, C. (2011). *Mit Geigerzählern und Jod gegen die Angst*.  
<https://www.dw.com/de/mit-geigerzählern-und-jod-gegen-die-angst/a-14915453>
- TRADOC. (2007). *Terrorism and WMD in the Contemporary Operational Environment* (T. I. S. A.-T. F. L. KS (Ed.)).
- U.S. Agency for Toxic Substances and Disease Registry. (2004).

- Toxicological Profile for Americium.*  
<https://www.atsdr.cdc.gov/toxprofiles/tp156.pdf>
- U.S. Congress Office of Technology Assessment. (1993). *Technologies Underlying Weapons of Mass Destruction (OTA-BP-ISC-115).*
- U.S. Department of Defense. (2010). *Joint Pub 3-07.2, Antiterrorism.*
- U.S. Department of State. (2004). *Patterns of Global Terrorism 2003.*
- U.S. Fire Administration. (2020). *USFA position on home smoke alarms.*  
 Usfa.Fema.Gov.  
[https://www.usfa.fema.gov/about/smoke\\_alarms\\_position.html](https://www.usfa.fema.gov/about/smoke_alarms_position.html)
- UK National Counter Terrorism Security Office. (2016). *Recognising the terrorist threat.*  
<https://www.gov.uk/government/publications/recognising-the-terrorist-threat/recognising-the-terrorist-threat>
- Unger, C. (2018). *Wie groß ist die neue Bedrohung durch Bioterrorismus?*  
 WAZ. <https://www.waz.de/politik/wie-gross-ist-die-neue-bedrohung-durch-bioterrorismus-id214690269.html>
- United Nation Office of Disarmament Affairs. (1975). The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction. In *un.org*.
- United Nations Office on Drugs and Crime. (2016). *The International Legal Framework against Chemical, Biological, Radiological and Nuclear Terrorism.* [https://www.unodc.org/documents/terrorism/for web stories/1-WS CBRN 6 modules/CBRN\\_module\\_-\\_E.pdf](https://www.unodc.org/documents/terrorism/for_web_stories/1-WS_CBRN_6_modules/CBRN_module_-_E.pdf)

- Valkanova, E., Kostadinov, R., Etova, R., & Georgieva, M. (2019). Healthcare providers' readiness for management of incidents with weapons of mass destruction. *Journal of IMAB–Annual Proceeding Scientific Papers*, 25(3), 2640–2643.
- van de Poel, I., Royakkers, L., & Zwart, S. D. (2015). *Moral responsibility and the problem of many hands* (Vol. 29). Routledge.
- van den Hoven, J., Vermaas, P. E., & van de Poel, I. (2015). Design for Values: An Introduction. In J. van den Hoven, P. E. Vermaas, & I. van de Poel (Eds.), *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains* (pp. 1–7). Springer Netherlands. [https://doi.org/10.1007/978-94-007-6970-0\\_40](https://doi.org/10.1007/978-94-007-6970-0_40)
- Van den Hoven, J., Vermaas, P., & Van de Poel, I. (2015). *Handbook of ethics, values and technological design*. Springer.
- Van Der Does, R., Kantorowicz, J., Kuipers, S., & Liem, M. (2019). Does Terrorism Dominate Citizens' Hearts or Minds? The Relationship between Fear of Terrorism and Trust in Government. *Terrorism and Political Violence*, 1–19.
- Van Der Veer, R., Bos, W., & Van Der Heide, L. (2019). *Fusion Centres in Six European Countries: Emergence, Roles and Challenges*. <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST 12168 2005 REV 3>.
- Varon, J. (2004). *Bringing the war home : the Weather Underground, the Red Army Faction, and revolutionary violence in the sixties and seventies*. University of California Press.
- Ward, M. (2014). *Exploratory Analysis of Cultural Factors and the Impact*

*They May Have on Terrorist Views about CBRN Weapons*. George Mason University.

Watanabe, M. (1998). Religion and violence in Japan today: A chronological and doctrinal analysis of Aum Shinrikyo. *Terrorism and Political Violence*, 10(4), 80–100.

Weber, M. (1914). *Economy and society: An outline of interpretive sociology* (Vol. 1). Univ of California Press.

Weimann, G. (2008). The Psychology of Mass-Mediated Terrorism. *American Behavioral Scientist*, 52(69), 69–86.  
<https://doi.org/10.1177/0002764208321342>

Wessely, S. (2005). Don't panic! Short and long term psychological reactions to the new terrorism: The role of information and the authorities. *Journal of Mental Health*, 14(1), 1–6.  
<https://doi.org/10.1080/09638230500048099>

Westdeutscher Rundfunk. (2018). *Rizin-Fund in Köln: Tunesier mischte Bio-Waffen zusammen*. WDR.De.  
<https://www1.wdr.de/nachrichten/rheinland/koeln-chorweiler-toxische-substanzen-100.html>

Whitby, S. M., Novossiolova, T., Walther, G., & Dando, M. R. (2015). *Preventing Biological Threats: What You Can Do*.

Wikipedia. (2007). *Ricin* (edited 5 January, 2007). Wikipedia.  
<https://en.wikipedia.org/w/index.php?title=Ricin&direction=next&oldid=98613417>

Wikipedia. (2019a). *Talk:Ricin*. Wikipedia.Org.



- <https://en.wikipedia.org/wiki/Talk:Ricin>
- Wikipedia. (2019b). *Wikipedia*. Wikipedia.  
<https://en.wikipedia.org/wiki/Wikipedia>
- Wikipedia. (2020a). *Ricin*. Wikipedia. <https://en.wikipedia.org/wiki/Ricin>
- Wikipedia. (2020b). *Wikipedia:Risk Disclaimer*. Wikipedia.Org.  
[https://en.wikipedia.org/wiki/Wikipedia:Risk\\_disclaimer](https://en.wikipedia.org/wiki/Wikipedia:Risk_disclaimer)
- Wikipedia. (2020c). *Wikipedia Help:Censorship*. Wikipedia.Org.  
<https://en.wikipedia.org/wiki/Help:Censorship>
- Wikipedia. (2021). *Wikipedia:What Wikipedia is not*. Wikipedia.Org.  
[https://en.wikipedia.org/wiki/Wikipedia:What\\_Wikipedia\\_is\\_not#Wikipedia\\_is\\_not\\_an\\_indiscriminate\\_collection\\_of\\_information](https://en.wikipedia.org/wiki/Wikipedia:What_Wikipedia_is_not#Wikipedia_is_not_an_indiscriminate_collection_of_information)
- Williamson, H., Fay, S., & Miles-Johnson, T. (2019). Fear of terrorism: media exposure and subjective fear of attack. *Global Crime*, 20(1), 1–25.
- Woodside, S. N. (2013). Unintentional Terrorism? An Objection to David Rodin’s ‘Terrorism without Intention.’ *Journal of Military Ethics*, 12(3), 252–262. <https://doi.org/10.1080/15027570.2013.847537>
- World Institute For Nuclear Security. (2017). *Considerations for the Adoption of Alternative Technologies to Replace Radioactive Sources*. [https://wins.org/wp-content/uploads/2017/12/2017\\_04\\_14\\_Special-Report-Considerations-for-the-Adoption-of-Alternative-Technolgies\\_Rev2.1-EN\\_WEB.pdf](https://wins.org/wp-content/uploads/2017/12/2017_04_14_Special-Report-Considerations-for-the-Adoption-of-Alternative-Technolgies_Rev2.1-EN_WEB.pdf)
- Youtube. (2021). *Youtube*. Youtube.Com. [youtube.com](https://www.youtube.com)

# Acknowledgements

To me, the quote at the very beginning of this thesis refers to a quality that is as important in liberal democratic counter-terrorism infrastructures as it is in life. It is about the necessity to sometimes let go off the illusion of control. If only half of the world is fire resistant, than the other half must be inflammable, uncontrollable. We spend too much time trying to prepare for this second half and attempting to work on strategies to control the uncontrollable variables in life. That does not only waste energy on a pointless endeavor. Trying to control or avoid every possible threat or pain (making the inflammable fire-resistant) can also hurt us to even greater extent. The history of Asbestos is a case in point here.

Obviously, a Ph.D. is never the product of just one person. Hence, it is not surprising that I would like to thank other people for their support and contribution to this work. First of all, I would like to thank my supervisors Seumas Miller and Ibo van de Poel. Seumas, thank you very much for the opportunity to conduct my research independently, to explore new topics, and to visit and engage with researchers around the globe. I deeply appreciate your trust in my capabilities and I enjoyed working with you in the ERC project. Ibo, thank you for assisting me with the administrative tasks leading to my defense. Without your in-depth knowledge of the Dutch academic world and your availability for spontaneous meetings, I would probably still plan my defense. Furthermore, I would like to extent my gratitude to the independent members of my doctoral committee Professor

Neelke Doorn, Dr. Michael Skerker, Professor Christian Enemark, Professor Michael Gross, and Professor Jeroen van den Hoven. Thank you for taking the time to engage with my research and to participate in my defense.

This Ph.D. thesis is part of the Advanced Grant awarded by the European Research Council (ERC) to Professor Seumas Miller. I would like to thank the members of the ERC project "Global Terrorism and Collective Moral Responsibility". Paul, Adam, Mitt, Michael, Do'aa, Scott, Alastair, Barbara, and Tony - thank you for feedback and support during countless meetings, workshops, and conferences. Of course, also the section for Ethics/Philosophy of Technology at the TPM faculty supported my research to a great extent during my time at TU Delft. I found valued colleagues and friends that provided a lot of feedback on my thesis. Particularly, I would like to thank Taylor and Martin for their support, advice, and friendship. I bet it did not come as a surprise to you when I asked you to be my paranymphs. Furthermore, thank you to Aimee, Georgy, Christine, Lieke, Anna, Sabine, Behnam, and Nathalie for the help and discussions during my Ph.D. life in Delft.

Obviously, this thesis would not have been possible without my wonderful parents, who raised me to be a curious adult and who taught me to always follow my interests without spending too many thoughts on what to do after university. Thank you for always being there for me. Thank you to my brother for countless stimulating discussions about the world, politics, and funny Internet memes.

Thank you to my friends Christof (for the beers and the amazing book

cover), Hanno, Rainer, Inga (for the weekends and the beers), Domi (for the advice, support, and the beers), Navina, Liv, Laya, Carina, Caro (for the beers), Katrin, Martin, and to my goddaughter Hannah.

Finally, I would like to thank Anna for all the love, support, and optimism during the last phase of this thesis. Without you, I would have never had the courage to hand in this thesis. Thank you for always believing in me and for making me feel loved and understood. I am so much looking forward to the wonderful years ahead of us and our small family. Ich liebe dich.

## About the author

Jonas Feltes is a security analyst working for the German state of Northrhine-Westfalia. Between the years 2016 and 2021, Jonas completed his Ph.D. in the ERC Advanced Grant project “Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies” of Delft University of Technology, Charles Sturt University, Georgetown Law Center, and Oxford University. His main research interests include the relation between weapon technologies and terrorism as well as concepts of collective responsibility as starting point for security research.

Jonas holds an M.Sc. degree in History and Philosophy of Science at Utrecht University (with distinction) and a B.A. degree in History and Philosophy at the University of Cologne. In his master thesis, he investigated the relation between selected explosive technologies and terrorism and described both patterns in the selection of specific explosives by different violent groups as well as complex knowledge networks to distribute technical expertise on explosive manufacturing beyond the borders of groups and ideologies. During his studies in Delft, Utrecht, and Cologne, Jonas worked on topics such as bioterrorism & biological warfare, the role of media in terrorism and disasters, industrial espionage, ethical dimensions of asteroid mining and space exploration as well as ethical issues with unmanned weapon systems.

## List of publications

- Feltes, J. (forthcoming). Collective moral responsibility and chemical, biological, radiological and nuclear terrorism: the case of phosphine. Miller, S., Henschke, A. & Feltes, J. *Counter-Terrorism: The Ethical Issues*. Edward Elgar Publishing Ltd.
- Miller, S. & Feltes, J. (2018). Chemical Industry. Miller, Seumas. *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction*. Springer, Cham, pp. 55-71.
- Miller, S. & Feltes, J. (forthcoming). The definition of terrorism. In: Miller, S., Henschke, A. & Feltes, J. *Counter-Terrorism: The Ethical Issues*. Edward Elgar Publishing Ltd.
- Miller, S. & Feltes, J. (forthcoming). Collective responsibility and counter-terrorism. In: Miller, Seumas, Henschke, Adam & Feltes, Jonas. *Counter-Terrorism: The Ethical Issues*. Edward Elgar Publishing Ltd.

