The Hague Centre for Strategic Studies

Navigating the CBRN landscape of 2010 and beyond: towards a new policy paradigm

The Hague Centre for Strategic Studies Nº 01 | 01 | 10

The Hague Centre for Strategic Studies (HCSS) seeks to advance international security in an era defined by geopolitical, technological and doctrinal transformation and new security risks. HCSS provides strategic analysis and offers concrete policy solutions to decision makers. HCSS serves as a strategic planning partner to governments, international organisations and the business community.

Navigating the CBRN landscape of 2010 and beyond: towards a new policy paradigm
The Hague Centre for Strategic Studies N° 01 | 01 | 10

Erik Frinking, Tim Sweijs, Teun van Dongen and Aksel Ethembabaoglu

This report has been commissioned by TNO.

Graphic Design *Studio Maartje de Sonnaville, The Hague*

The Hague Centre
for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
www.hcss.nl

Navigating the CBRN landscape of 2010 and beyond: towards a new policy paradigm

The Hague Centre for Strategic Studies Nº 01 | 01 | 10

Table of Contents

Executive Summary

In times of tightening security budgets, the way in which countries prepare for Chemical, Biological, Radiological and Nuclear (CBRN) incidents, deserves renewed scrutiny.

The 'one percent doctrine' – prepare for the worst, even if the worst is highly unlikely – which is the current dominant paradigm, may have to be set aside in favour of a more realistic approach. This involves the prioritisation of capabilities against C, B, R, or N in the analysis, prevention and response (APR) phases. This will have to be done against the background of limited availability of data on the intentions and capabilities of actors to actually use CBRN weapons and uncertainty about scientific developments in the field of chemistry, biology and nanotechnology.

This report seeks to inform both policymakers and the CBRN industry by analysing the nature and size of present and future CBRN-threats as perceived by the policymaking and the expert community. It also compares policy approaches in six countries (Canada, France, Germany, the Netherlands, the United Kingdom (UK) and the United States (US)) and two international organisations (NATO and the EU).

Current CBRN-threats and hazards

An analysis of how current CBRN-threats and hazards are perceived by policymakers from the countries analysed shows the following:

- There is a consensus on the importance of CBRN-threats. All six countries list CBRN-terrorism or other CBRN-weapon use and the proliferation of CBRN-weapons among the most important security threats;
- The supporting analysis of these countries as well as NATO and the EU consider CBRN-incidents as necessarily catastrophic, high impact phenomena. They do not consider the possibility of smaller CBRN-incidents;

- The general perception is that state actors have the capacity to acquire CBRN but are restrained to deploy them. The opposite holds true for non-state actors. Only Al-Qaeda is considered a CBRN threat.

The expert community does not concur with these assessments. Most notably, this community disagrees with the probability of terrorist actors committing a CBRN attack (which it deems less probable). The experts also present a more in-depth understanding of the consequences of the release of CBRN agents with different delivery methods (impact).

Future CBRN threats and hazards

There is a consensus that in the next five to fifteen years, potential future CBRN threats and hazards depend on technological and geopolitical developments related to the proliferation and use of CBRN materials.

With respect to science and technology, experts expect:
- An increasing convergence of chemistry and biology;
- Tremendous advances in understanding and manipulating genes, cells, and organisms;
- Developments in the field of nanotechnology that may revolutionise dispersal methods.

With respect to materials:
- An increasing availability of CBRN materials;
- The potential to engineer (CB) materials from scratch;
- A growth in the number of dual-use materials and technology that pose major challenges to non-proliferation regimes.

With respect to intentions:
- A persistent intention on the part of state actors to acquire (new types of) CBRN capabilities;
- A persistent intention on the part of non-state actors to acquire (new types of) CBRN capabilities and in some cases an explicit desire to use these capabilities.

With respect to capabilities:
- Significantly fewer hurdles to state actor CBRN acquisition as a result of knowledge diffusion and economic globalisation;

- Fewer hurdles to non-state actor CBRN acquisition, although these will continue to exist;
- The emergence of a distinction between future and traditional BCW, with the former the prerogative of state actors while the latter may be within the reach of both state and non-state actors.

Overall, experts agree that in the 21st century, CBRN materials may be utilised and deployed as weapons in novel ways, both in the military and civil domain.

The CBRN-policy benchmark

The CBRN-policy benchmark, comparing the six countries mentioned above, reveals how countries formulate and execute their respective CBRN policies. Our analysis found that:

- Some countries deal with CBRN as a single policy issue in its own right; other countries approach CBRN as part of a larger security policy approach;
- CBRN crisis management has shifted from the military to the civil domain resulting in a duplication of efforts;
- While capabilities have been strategically identified along the analysis, prevention and response (APR) phases, few countries have dedicated CBRN strategies.

On the basis of the findings and conclusions of each of the chapters, the following eleven observations are made. These observations are intended to help policymakers and industry navigate the complex CBRN landscape of 2010 and beyond. They are formulated around the scope of risk consideration, the assessment of risks (including probabilities, impact, and vulnerability) and capability requirements.

Observation 1

The worst case-scenario approach, which is prevalent in CBRN assessment conducted by states, neglects attention to smaller or milder CBRN incidents.

Observation 2

The focus on CBRN as a whole ignores the distinct characteristics of each of these components.

Observation 3
While current proliferation prevention mechanisms seem to work, it is questionable whether they can keep pace with technological developments and remain future proof.

Observation 4
Focus on loss of life has dominated the impact discussion at the detriment of other potentially damaging impacts, ranging from political and social instability to economic and ecological costs.

Observation 5
Existing CBRN risk assessment capabilities within and outside governments are generally crude and lack a more calibrated analysis and an integrated understanding of the risk posed by CBRN incidents.

Observation 6
The current risk assessments approaches primarily focus on the threat and impact components of risk, and less so on vulnerability.

Observation 7
As with other investments in the field of security, a transparent method to evaluate budget allocation and investment in capabilities, against risk reduction and potential economic gain is lacking.

Observation 8
Risk reduction efforts do not focus sufficiently on getting more value for money.

Observation 9
The CBRN efforts by military and civilian actors are uncoordinated and overlap.

Observation 10
Responsibility for CBRN protection is partly shifting from the public to the private sector. But the associated knowledge flow (what to protect against, how to protect, how to respond?) is not always keeping up with this movement.

Observation 11
National security concerns prevent division of tasks across borders. This hampers a more efficient and effective CBRN policy.

1 Introduction

Security policy is increasingly subject to public scrutiny. Especially in the aftermath of the economic crisis, the demand for accountability of investments in security is growing. Measures to detect Chemical, Biological, Radiological and Nuclear (CBRN) activities, protect against harm or treat the effects of the production and use of CBRN materials are no exception. CBRN weapons pose a multi-faceted problem, as different actors are involved playing different roles. For instance, states can use or threaten to use nuclear weapons (NW), provide terrorist organisations with CBRN materials and technology, or be involved in espionage to obtain CBRN materials and know-how from other states. Terrorist organisations may be interested in acquiring, producing or using CBRN weapons, and illicit networks trade in CBRN technology and materials. Industrial sites constitute potential hazards as setting of an attack or accident or because others may attempt to acquire CBRN resources.

To complicate matters further, the impact of CBRN incidents is difficult to predict. The impact concerns not only casualties, but also mass panic, social disruption, economic loss and ecological damage. This report will analyses the nature and size of CBRN threats and compare policy options that are implemented by different states in the military, security and safety domains. This analysis will inform decision making in the allocation of resources to counter CBRN threats. The analysis will make a distinction between CBRN and its individual components. For purposes of this analysis the concept of risk comprises of the factors probability, impact, and vulnerability and the concept of the security chain contains elements of analysis, prevention and response. These concepts will be further elaborated in their respective chapters.

Chapter 2, 'CBRN: a primer', sketches some background to the build-up and use of CBRN weapons over the years. Chapter 3 looks at the way CBRN threats are perceived by policy makers from a group of selected countries (Canada, France, Germany, the Netherlands, the United Kingdom and the United States) and

international organisations, (NATO and the EU). How big are the CBRN risks and dangers? What will happen when a CBRN incident takes place? Who are the most likely culprits? These policy views are compared with expert views. Chapter 4 describes future trends that emerge from an analysis of 'foresight studies': expert studies that outline future developments regarding the use of CBRN weapons. These include expectations regarding the availability of CBRN materials, the size of CBRN incidents and incidence in the use of C, B, R and N weapons. Chapter 5 contains a strategic level CBRN policy benchmark, comparing the CBRN related policies of six selected countries, including how they spend R&D funds, the organisation of their crisis response and monitoring of (potentially) sensitive or hazardous locations. The reports concludes with a synthesis and observations on the scope of the risks we are facing, the ways these risks should be ascertained and how to adequately deal with them.

2 CBRN: a primer

2.1 Chemical weapons

Chemical weapons (CW) come in many shapes and forms, with most conventional weaponry also relying on chemical explosives. CW, however, are distinct in that they rely on their toxicity for their effects.[1]

Modern chemical weapons were first used on a large scale during World War I (WWI). Active Research and Development (R&D) continued through the interwar years and World War II (WWII), although actual use was rather sporadic. The Cold War saw the development of extensive stockpiles of CW on both sides and several developing countries successfully acquired CW capabilities. They were extensively used by the Iraqi forces under Saddam Hussein against Iran, as well as against parts of their own population. The introduction of the Chemical Weapon Convention (CWC) in 1997 has significantly reduced existing stockpiles. TA number of states have declared CW stockpiles and have started destruction of stockpiles under the rules of the convention, including the United States (U.S.), Russia, India, South Korea and Libya.[2] Despite the fact that all State Parties have committed to destroy their chemical weapon stockpiles by 2012, some countries are behind schedule - most notably the US and Russia - and it is unlikely that they will be able to meet the deadline. It is impossible for the OPCW to inspect every facility in the country to verify actual compliance and significant discrepancies

1 They are defined as 'non-living, manufactured chemical agents combined with a dispersal mechanism that, when activated, produce incapacitating, damaging or lethal effects on human beings, animals or plants. The chemical agents can be dispersed in four principal forms: as gas (or vapour), as aerosol (mist), as solid aerosol (smoke), or as a liquid. Chemical agents generally deliver their effect through inhalation, ingestion, or absorption by the skin. The effects (...) can appear very quickly (in a few seconds) or over the course of a couple of days. Lindstrom (2004), p. 25. The four most frequently cited types of chemical agents are blister, blood (cyanides), chocking (pulmonary), and nerve agents.' Ibid., p. 17.

2 Organization for the Prohibition of Chemical Weapons (2009).

exist in the depth and scope of implementation between different State Parties. Over half of the CWC States Parties (SP) have so far failed to adopt a legal framework to regulate the import and export of chemicals and related technology and in many countries no licensing regime is yet in place. Progress in the field of chemical materials and weapons disposal is behind schedule and (illegal) chemical weapon dumpsites, for instance at sea, pose an environmental hazard.[3] A large number of states have ratified the CWC (188 states by May 2009). Yet, some of the non-signatories as well as States Parties are suspected of retaining a clandestine CW capability, including China (SP), Iran (SP), Egypt (non-SP), Syria (non-SP), and Israel (non-SP).[4]

Although the fabrication of advanced and effective CW poses a technological challenge to non-state actors, the intent of non-state actors to use CW is certainly present. The Monterey Weapons of Mass Destruction (WMD) terrorism database reports both attacks and 'plot incidents', in which the perpetrators had been able to acquire CW agents, but failed to use them. In the period 1988-2004, 207 of the 316 CBRN incidents recorded in the Monterey WMD terrorism database involved CW.[5] Yet these incidents mostly involved conventional explosives mixed with openly available chemicals to make them more deadly, or were failed attempts to weaponise chemical agents. The only attack that involved a standard CW agent, the Tokyo Sarin gas attacks by Aum Shrinikyo in 1995, showed how difficult it is to mount an effective CW attack, even for an organisation with high levels of expertise and sufficient funding.

3 'Nuclear Threat Initiative, 'Chemical Weapons in Baltic Sea Remain a Threat, Lithuania Says.' Global Security Newswire, July 22, 2009.

4 James Martin Center for Nonproliferation Studies (2002).

5 Ivanova & Sandler (2006).

2.2 Biological weapons

Biological weapons (BW) are defined as combining 'a biological warfare agent with a means of dispersing it. Biological warfare agents are microorganisms such as viruses or bacteria that infect humans, livestock or crops and cause an incapacitating or fatal disease'.[6]

Primitive biological warfare has been waged by humans since ancient times.[7] However, only in the 20th century the advent of modern medicine and biology allowed for the systematic development of a range of biological warfare agents and their weaponisation. Several countries manufactured and used experimental BW during WWI and WWII, even though with rather limited success.[8] R&D of BW continued throughout the Cold War with the U.S. and the Soviet Union at the forefront, leading to the successful weaponisation of such deadly agents as anthrax or the smallpox virus.

The threat of BW was significantly reduced with the introduction of the Biological Weapons Convention (BWC) in 1972, which outlawed the development, use, and stockpiling of all BW and mandated their destruction.[9] Nonetheless, several countries, such as the Soviet Union and Iraq, are known to have continued extensive clandestine BW programs, sometimes until well into the 1990s.[10] Despite recent successes in dismantling BW programs (e.g. in Iraq or Libya), at least half a dozen countries around the world are suspected to retain at least some form of offensive BW capacity today. There are several countries that have not ratified or signed the treaty, including Israel, Egypt, and Syria (as of July 2008, 163 States have ratified or acceded to the BWC and 13 signed the treaty). The dangers from state-led BW programs have been reduced in recent years, but concerns remain over residual capabilities and possible clandestine BW programs. In recent years, the debate around BWs and non-proliferation has

6 'Biological agents are generally categorised on the basis of three forms of micro-organisms: bacteria; viruses; rickettsiae, fungi and toxins Symptoms of illness appear after a delay, or 'incubation period', that may last from days to weeks. By contrast, toxins – non-living poisons produced by living plants, insects and animals – are difficult to categorise. (...) Biological agents can enter the human body through the intestines (ingestion), lungs (inhalation) or skin (cutaneous).' Lindstrom (2004), p. 25.

7 Center for Infectious Disease Research & Policy (2009).

8 Tulliu & Schmalberger (2004).

9 Biological and Toxin Weapons Convention (1972).

10 See Purkitt (2005); Ainscough (2002).

increasingly focused on non-state actors and terrorist groups in particular. At least 25 'distinct sub-national actors' are known to have 'shown concerted interest' in acquiring BW, with at least eight of them known to have been successful.[11] The experiments of Aum Shrinikyo with Anthrax and Ebola, as well as the 2001 Anthrax attacks in the US are well-documented examples.

2.3 Radiological & nuclear weapons

Radiological weapons (RW) combine radioactive material with a means of dispersing it among a target population, resulting in the inhalation or ingestion of, or immersion with, radioactive material. The resulting exposure to alpha and beta particles, gamma rays and neutrons produces incapacitating or lethal effects through external and internal radiation.[12] Nuclear explosives are based on self-sustained nuclear reactions which transform the nuclear structure of atoms and in the process release great bursts of energy.[13] These processes are characterised by either fission reactions or (more powerful) fission and fusion reactions. Devastating damage accrues through a combination of effects comprising a powerful blast wave, thermal radiation, and initial and residual radiation. Whether based on fission only (atomic bomb), or fission and fusion (hydrogen bomb), the assembly of NW requires fissile material (typically highly-enriched uranium or plutonium) and substantial engineering expertise. It has been suggested that cruder 'Improvised Nuclear Devices' (INDs) might also be constructed. If successful, the latter might compare to a smaller 'conventional' nuclear bomb. If failing to reach a critical mass for a self-sustained nuclear reaction, the impact might nonetheless compare to a gigantic conventional explosion and would include dangerous radiological fall-out.[14] While some R&D towards RWs was conducted during the Cold War, state actors have rarely developed RWs[15]—presumably preferring to concentrate their efforts on acquiring much more powerful and deadly NWs. However, interest in RW has increased in recent years as they may constitute an attractive weapon for non-

11 Center for Counterproliferation Research (2003), p. 5.

12 Definition closely based on Lindstrom (2004), p. 33; Acton et al. (2007).

13 Tulliu & Schmalberger (2004).

14 Definition closely based on Ibid.

15 The most elaborate known attempt by a state to produce a RW was conducted by Iraq in the late 1980s. However the results were apparently disappointing and the program shelved, see United Nations Special Committee (1995),

state actors with limited capabilities and resources.[16] Far less destructive than a NW, an effective RW could cause considerable casualties, widespread panic and disruption, as well as sizable economic damage.[17]

Nuclear weapons, developed and deployed first by American forces during World War II, have become the epitome of WMD and symbol of their ultimate destructive power. Around the mid 20th century, only a handful countries had managed to develop their own NWs, but today it is estimated that between 35-40 countries possess the knowledge and capacity to attain a nuclear capability in a relatively short time span.[18] In 2009 nine states have a nuclear capability of some sort: U.S., Russia, UK, France, China, India, Israel, Pakistan and North Korea. Iran is suspected to develop a nuclear capability.

Across the globe, only four states are not party to the Nuclear Non-Proliferation Treaty (NPT) – India, Israel, North Korea, Pakistan, all of which are nuclear states.. The NPT is a treaty to limit the spread (proliferation) of nuclear weapons. Though almost universally ratified, the NPT is plagued by a number of weaknesses. A number of nuclear 'don't-haves', seem increasingly interested in acquiring NWs, especially since the nuclear 'haves' do little to fulfil one of the key tenets of the treaty: giving up NWs.[19] Furthermore, the mandate of the International Atomic Energy Agency (IAEA), the institution charged with the enforcement of the NPT, is limited. The IAEA is charged particularly with 'preventing diversion of nuclear energy from peaceful uses to NWs or other nuclear explosive devices.'[20] The IAEA has limited verification responsibilities and lacks authority to secure nuclear material, to install near-real-time surveillance devices at the sites it inspects, or to conduct the wide-area surveillance needed to monitor activities covered under the Additional Protocol to the NPT. Neither can the IAEA prevent the indigenous weaponisation of states that have not ratified the Treaty.[21] It is beyond the capacities of the IAEA to monitor the tremendous amount of fissile material worldwide. The NPT also contains a three-month withdrawal clause, allowing states to acquire technology

16 See Cornish, p16.
17 Zimmerman & Loeb (2004).
18 Mohamed el-Baradei, 'Towards a Safer World.' The Economist, October 16, 2003.
19 International Atomic Energy Agency (1970).
20 Ibid
21 Graham et al. (2008), pp. 45-46.

and nuclear material under the auspices of the IAEA and, having obtained this technology, withdraw from the Treaty. Additional non-proliferation agreements and organisations cover the trade in dual-use technologies, such as the Nuclear Suppliers Group.[22]

There are a number of reports of non-state actors intending and attempting to acquire NWs. Whether these attempts should be taken seriously is disputed but the threat of[23] so-called catastrophic terrorism, terrorists that intend to use nuclear weapons to wreak massive havoc on societies, is expected to be around for at least the next decade. While non-state actors would face significant obstacles in building a nuclear bomb, some experts stress that they might be able to build an improvised nuclear device, if they were able to obtain enough weapons-grade uranium or plutonium.[24] Much of the argument for RW as terrorists' 'weapon of choice' has concentrated on the fact that acquiring radioactive material in sizable quantities may be relatively easy: different suitable isotopes are used in large quantities in civilian applications around the globe, some of which lack strict monitoring or security arrangements.

22 Federation of American Scientists (2009).

23 Salama & Hansell (2005); cf. Bobbitt (2008).

24 Pluta & Zimmerman (2006).

3 Surveying contemporary risk perceptions

3.1 Introduction

This chapter provides an overview of the risks posed by CBRN weapons or CBRN related incidents. This analysis is based on a survey of key policy documents of six countries and two international organisations (IOs). The findings are compared with the prevailing views of experts.

For purposes of this analysis, a threat is defined as an event whereby a state, non-state or industrial actor either produces CBRN materials or uses a CBRN weapon. A risk is defined as: Risk (threat) = Probability (threat) x Impact (threat) x Vulnerability (threat)

The components 'probability', 'impact' and 'vulnerability' are defined as follows:

- Probability refers to the likelihood that a certain threat will manifest itself against the stakeholder. On the basis of expert opinion, intelligence reports or empirical evidence, one can roughly rank the threats from low (very unlikely) to high (very likely).
- Impact mainly concerns the question of what is affected when a threat manifests itself. Armed with knowledge of the probability and the impact, the stakeholder may decide on how to spend its resources. Even though stakeholders are likely to choose the options that cover the high probability/ high impact threats and dangers, this does not necessarily follow from the outcome of a risk assessment.
- Vulnerability is the third element of the risk assessment. It is the least commonly used element of the three, but finds increasing use, most notably by the U.S. Department of Homeland Security.[25] Vulnerability concerns the characteristics of a potential target that make it especially susceptible to manifestations of security and safety risks. Examples of vulnerabilities regarding the deployment of CBRN weapons include low levels of security

25 Masse et al. (2007), pp. 7-8.

and low awareness of the population of what to do in case of a CBRN incident. There is a relation between the impact and the vulnerability: when vulnerability is lower, the impact will be lower as well.

For our analysis, we examined key policy documents related to CBRN for the selected countries and IOs (US, UK, France, Germany, the Netherlands, Canada, EU and NATO). On a note of caution, the nature of the available documents differs from country to country, but they typically include national security strategies, counterterrorism strategies and other documents explaining national policies regarding security or safety. Where available, we included annual reports of secret services. For example, the Dutch intelligence and security services AIVD (*Algemene Inlichtingen- en Veiligheidsdienst*) and MIVD (*Militaire Inlichtingen- en Veiligheidsdienst*), the Canadian Security and Intelligence Service (CSIS) and the German security service BfV (*Bundesamt für Verfassungsschutz*) publish annual reports that describe various threats to national security in some detail, whereas the British secret services (MI5 and MI6) do not make their annual reports publicly available. As a result, we have more detailed information on security threats for the Netherlands, Canada and Germany than for the other countries. Not included in the analysis are policy or parliamentary debates in the respective countries.

3.2 Security and safety threats: state actors, non-state actors and accidents

The countries selected for our analysis distinguish three sources that may trigger CBRN events that are harmful to international and national security: state actors, non-state actors and accidents. To all, the most pressing threats to security do no longer come from states. From key policy documents, terrorist use of CBRN weapons emerges as one of the most imminent threats to security.[26] A worrying factor in this regard is the dual-use nature of many of the materials of which CBRN weapons are composed. This facilitates access to these types of weapons by terrorist organisations.

26 Ministry of Defence (2003).

OVERVIEW	STATE ACTORS	NON-STATE ACTORS	ACCIDENTS
CANADA	Iran, North Korea	Terrorism, notably Al-Qaeda	⚠
EUROPEAN UNION	Iran, North Korea, Middle-East region, South Asia region	Terrorism, notably Al-Qaeda	⚠
FRANCE	Iran, North Korea, India, Pakistan, East-Asia, Middle-East	Terrorism, notably Al-Qaeda	⚠
GERMANY	Iran, North Korea, Pakistan, Syria	Terrorism, notably Al-Qaeda	⚠
NATO	Iran, North Korea * NATO also mentions Russia as a potential source of proliferation	International Terrorism	⚠
THE NETHERLANDS	Iran, North Korea, Pakistan, Syria	Terrorism, notably Al-Qaeda	⚠
UNITED KINGDOM	Iran, North Korea	Terrorism, notably Al-Qaeda	⚠
UNITED STATES	Iran, North Korea, China, Russia, Pakistan, Syria	Terrorism, notably Al-Qaeda	⚠

⚠ = Recognised

Figure 1. OVERVIEW OF PERCEIVED STATE AND NON-STATE THREATS

This table shows the threats that countries perceive per category (state or non-state actor).[27] The table shows considerable consensus regarding the state and non-state actors that are considered as posing a threat. Most countries consider the 'usual suspects', like Al-Qaeda, Iran, North Korea and Pakistan to be potential threats. India and China are mentioned only once. The symbols in the column 'accidents' indicate that countries explicitly mention the dangers of CBRN accidents.

27 Since the information we used is exclusively open source and more detailed information is available for some countries, conclusions should be considered with caution.

3.3 Probability

Threats: state actors

The state actor threat is a traditional one, wherein state actors threaten another state with military CBRN weapons. For example, North Korea developed a nuclear weapon capability and recently threatened with nuclear retaliation in case it was attacked by the U.S.[28] The countries in our sample set assume that the state actors posing a CBRN threat have more resources for the development of CBRN capabilities. However, the willingness to actually use CBRN weapons is estimated to be relatively low because of high political costs that come with their use. For instance, the UK National Security Strategy states that 'a number of states retain the ability to produce chemical and biological weapons. However, they are not judged as posing a direct threat to the United Kingdom.[29]'

The countries analysed don't distinguish between strategic use of CBRN weapons, for example to improve a bargaining position, and actual use. There is a consensus that state use of CBRN weapons will lead to regional instability. For instance, North Korea poses a threat to the East Asian region, while Iran threatens the stability of the Middle East. This instability may have consequences for other regions, and international peace and security, but, unlike during the Cold War, the expectation of the surveyed countries is not that they themselves will be targeted by North Korea or Iran.[30] Regarding the distinction between C, B, R or N, the CBRN- threat posed by states is, unlike the CBRN threat posed by non-state actors, largely a nuclear one.

In the assessment of states with a CBRN weapons program there is consensus that the nuclear programs of Iran and North Korea are a threat to international peace and security. Because of their secrecy and defiance of United Nations Security Council (UNSC) resolutions, Iran and North Korea are viewed by the selected states as undermining the international non-proliferation regime. Iran because it continues its uranium enrichment program despite various UNSC resolutions and North Korea as it has withdrawn from the NPT, conducted illicit ballistic missile tests and recently restarted its nuclear program. Another

28 'North Korea Threatens Nuclear 'Fire Shower' if Attacked.' The Guardian, June 25, 2009.

29 Ministry of Defence (2003), p. 12.

30 See ibid.

country raising concern, although not mentioned as frequently, is Syria.[31] This threat is mostly linked to illicit nuclear activities. For example, Syria built a clandestine nuclear facility that was bombed, allegedly by Israel. Nonetheless, Syria still refuses to fully answer questions from the IAEA.

Generally, states that follow a geostrategic policy that threatens other states and have a nuclear capability, are perceived to pose a nuclear threat. The exception is Pakistan where it is not the state itself but the fear that Pakistan's nuclear weapons fall into the hands of non or sub-state actors. Pakistan is considered a threat because of its weaknesses rather than its strengths.

Threats: non-state actors

The second security threat with a CBRN component is terrorism. Some countries distinguish between international, global or transnational and home-grown terrorism. Of the surveyed countries, the Netherlands draws the sharpest distinction between home-grown and international terrorism. The Netherlands Intelligence Agency AIVD identifies a form of home-grown terrorism where persons operate without contact with Al-Qaeda. France and the UK admit that terrorist cells are being formed on their own soil, but they speak of international or global terrorism as a single actor.[32] Canada and the U.S. also blur the distinction, referring to "a transnational movement of extremist organisations, networks, and individuals".[33]

The inclusion of various forms of terrorism in key policy documents as a new major security threat, illustrates that non-state CBRN threats have become an increasing concern to states. The only organisation mentioned in the sources analysed is Al-Qaeda. Al-Qaeda is considered highly resourceful, which increases concerns that it might want to acquire and use CBRN weapons.[34]

The policy documents fail to specify which of the C, B, R, or N weapons non-state actors such as Al-Qaeda are likely to acquire, although nuclear weapons are

31 Algemene Inlichtingen- en Veiligheidsdienst (2009), p. 50.

32 Her Majesty's Government (2009), p. 141; Villepin (2006), p. 10.

33 United States Government (2006b), p. 5. For the Canadian perception of terrorism as an international phenomenon, not particularly spawned by Canada, see Government of Canada (2004), p. 6.

34 On the perceived strength of al Qaeda, see United States Government (2006b), p. 9.

considered to be too hard to acquire, at least on the short term. The assessment of the capabilities and intentions of non-state actors is that their resources to acquire a CBRN weapon are relatively low, but , contrary to states, they are eager to deploy such a weapon once acquired. According to the UK's National Security Strategy, 'terrorist networks have made no secret of their desire to acquire and use chemical, biological, radiological and nuclear (CBRN) weapons.'[35] However, this statement underestimates the technological complications that come with the production and use of CBRN weapons. As a result, terrorist organisations might stick with more conventional weapons.[36] This is illustrated by the Global Terrorism Database (GTD), which shows that terrorist organisations have not deployed CBRN weapons often and that the casualty rate of terrorist CBRN attacks has been low.[37]

Hazards: accidents

The third aspect of a CBRN event posing a danger is an accident or disaster with CBRN materials. This could be anything from a spill of CBRN materials during transport, a power failure in an industrial facility leading to the emission of toxic gases, or a broken test tube in a biological research centre, releasing bacteria that spread dangerous diseases. Notable examples of CBRN accidents are the accident at Three Mile Island in 1979, the 1984 Bhopal gas disaster in India and the explosion of the nuclear reactor in Chernobyl in 1986. No state rules out industrial CBRN accidents, but it is not framed as a national security threat.[38] Thus, it gets less attention than the threat of CBRN attacks. The key policy documents focus on intentional security threats.

3.4 Impact

What is the impact of a CBRN event? As a result of the lack of tools to differentiate between different degrees of impact, the impact is often described in terms of a worst-case scenario. For instance, the U.S. speaks of "catastrophic challenges involving the acquisition, possession, and use of WMD by state and non-state actors". Several countries use Weapons of Mass Destruction (WMD) as

35 Her Majesty's Government (2008), p. 29.

36 Parachini (2003).

37 The Global Terrorism Database allows for searches by weapon type. See http://www.start.umd.edu/gtd/search/BrowseBy.aspx?category=weapon.

38 However, the Dutch National Risk Assessment for 2010 will start considering NBC accidents within the realm of possible dangers to national security.

a synonym for CBRN weapons, which reflects the expectations of the impact that the deployment of such weapons will have.[39] The countries analysed show little awareness of the possibility of smaller CBRN attacks or incidents, which might require a different response.

The expected impact is frequently formulated in quite general terms. For example, the German National Strategy for Critical Infrastructure Protection notes that failure or degradation of critical infrastructure would result in sustained supply shortages or significant disruption of public safety and security.[40] Similarly, a Canadian policy document claims that disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence.[41] More concretely, the Dutch National Risk Assessment (*Nationale Risicobeoordeling*) specifies five types of impact that can be the result of the manifestation of a security or safety threat. These five types are related to territorial, physical, economic and ecological safety and security, and social and political stability. This explicit and structured approach suggests that a more comprehensive approach of assessing the impact of a CBRN incident is feasible.

The indications that are found in the policy documents on the impact of a CBRN incident assume that CBRN attacks or accidents will involve Critical National Infrastructure (CNI). None of the documents consider the impact of an attack on a soft or non-CNI target, such as the possibility of CBRN assassinations of influential national figures, which would gravely disrupt society.

3.5 Vulnerability

The policy documents analysed contain little information on vulnerability.[42] The documents concentrate on the threat (probability) and to a lesser extent the impact. The term 'vulnerability' is used, referring to assets a country considers essential for its functioning, in other words, its critical national infrastructure. CNI is defined differently by various countries, but generally describes a similar set of buildings and assets. It includes power and energy, IT and communications, (public) transportation, water supply, food, health, government buildings,

39 Villepin (2006), p. 65; Ministry of Defence (2003), pp. 11-12; Government of Canada (2004), p. 7.
40 Bundesministerium des Innern (2009), p. 4.
41 Bundesministerium des Innern (2008), p. 3.
42 Given the definition provided earlier.

banking and finance, military installations and units, iconic cultural objects and CBRN relevant industries. Some countries include other sectors as well. For example, Germany also refers to the media, law enforcement and public administration in its CNI.[43] The US includes the defence industrial base, postal and shipping services, cyber infrastructure and dams.[44] However, none of the countries explain why certain kinds of CNI are particularly vulnerable to CBRN attacks. Perhaps such documents exist but are not open-source.

3.6 Drivers of the CBRN threat: proliferation

The countries and IOs analysed are not only concerned about the actual deployment of CBRN weapons, but also focus on proliferation. Assessing the threat of proliferation is complicated by the dual-use nature of CBRN-materials which renders them useful for both peaceful and non-peaceful purposes. The threat of proliferation, much like the threat of the actual deployment of CBRN weapons, derives from both state and non-state actors. An example of a state constituting a proliferation risk is North Korea, which withdrew from the NPT in 2003. In international negotiations (the Six-Party Talks) North Korea now bargains with its nuclear program to receive economic and humanitarian aid.

It is allegedly undermining the international non-proliferation regime by secretly selling or trading nuclear technology and delivery vehicles. Recently, the US implicitly accused North Korea of assisting Burma in its attempts to acquire nuclear weapons.[45] Pakistan poses a particular type of proliferation risk: the chance that Pakistan's nuclear weapons fall into the hands of sub-state or non-state actors puts it high on the list of proliferation risks of most countries surveyed .

Non-state actors also play a significant role in proliferation. An example often referred to is the A.Q. Khan network, a clandestine group that sold nuclear technology to states and possibly non-state groups for financial gain. This network significantly and intentionally contributed to the proliferation of nuclear technology by, for example, providing nuclear capabilities to Pakistan. The Dutch AIVD states in its annual report that it conducts studies into the formation and modus operandi of so-called acquisition networks, in other

43 Bundesministerium des Innern (2009), p. 7.

44 Department of Homeland Security (2009a), p. 3.

45 'U.S. Concerned over N. Korea-Myanmar Tie.' CNN.com, July 22, 2009.

words, the nuclear black market, but there is no mention of concrete networks active on the nuclear black market.[46]

Non-state actors can also unintentionally contribute to proliferation. For example, foreign professionals, foreign exchange students, visiting professors as well as academic and research institutions can be used by states to illicitly acquire CBRN technologies and materials.[47] Governments of the countries in our sample set typically liaison with the relevant industries and appropriate institutions to prevent this kind of proliferation and warn them about the tricks and tactics of foreign powers conducting espionage. The risks of proliferation through espionage and weak export controls are illustrated by Iran. According to the AIVD, even under heavy international sanctions it still managed to acquire dual-use goods through espionage.[48]

3.7 Main policy findings

This chapter has given an overview of the information on the three components of risk (probability, impact and vulnerability) of CBRN threats. The main findings can be summarized as follows:

- The policy documents, that were analysed primarily address the threat and tell us less about the expected impact of manifestations of the threat and the vulnerabilities of the respective states;
- Countries and IOs think of CBRN incidents as necessarily catastrophic, high impact phenomena. The possibility of smaller CBRN incidents appears to have been overlooked;
- There is consensus on the importance of CBRN threats. All countries have listed CBRN terrorism, other CBRN weapon use and the proliferation of CBRN weapons among the most important security threats;
- States are considered to have more resources to acquire CBRN weapons than non-state actors;
- Non-state actors are perceived to be less restrained in the use of CBRN weapons by considerations of political backlash as a result of its use, than states. Except for Al-Qaeda, no other organisations are explicitly mentioned as posing a CBRN threat. Possibly, states do not wish to state these intentions for public

46 Algemene Inlichtingen- en Veiligheidsdienst (2009), p. 49.

47 See for example Ministerie van Defensie en Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2005); Bundesministerium des Innern (2008), pp. 284-285.

48 Algemene Inlichtingen- en Veiligheidsdienst (2009), p. 50.

consumption. However, even those services that can be considered as relatively transparent information providers, fail to provide detailed information on other non-state actors;[49]

- CBRN weapons are framed as a composite category, meaning that individual developments on the chemical or biological field are not specifically addressed. For example, key documents do not distinguish between the likely use of nuclear weapons by state and non-state actors.[50]

3.8 Expert views

To assess the assumptions on which the CBRN policies of the surveyed countries are based, we reviewed available expert literature to see whether it corroborates or contradicts the main findings above.

Countries and IOs think of CBRN incidents as necessarily catastrophic, high impact phenomena. The possibility of smaller CBRN incidents appears to have been overlooked.

Expert literature shows a similar tendency to assume that CBRN incidents will be inherently catastrophic. For example, the Commission on the Prevention of WMD Proliferation and Terrorism estimates that by the end of 2013 a weapon of mass destruction will be used by a terrorist group, most likely a nuclear device or a biological pathogen. It recommends to take measures to prevent biological attacks from inflicting mass casualties.[51] Other reports and testimonies also view the CBRN threat, usually coming from terrorist organisations, as inherently catastrophic. For example, Barnaby argues that 'terrorists need to move continually to higher levels of violence' and suggests that chemical weapons are most accessible to terrorists for such purposes.[52] Some researchers consider CBRN incidents on a smaller scale, not assuming high numbers of casualties or magnifying dangers. Neil Davison, for instance, refers to military research that

49 See the annual reports of the AIVD (https://www.aivd.nl/actueel/aivd-publicaties), BfV (http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/) and BVT (http://www.bmi.gv.at/cms/bmi_verfassungsschutz/).

50 Ongoing legislative developments in the US (specifically the Weapons of Mass Destruction Prevention and Preparedness Act of 2009 introduced in the Senate) do signal a preference for preparedness for biological attacks. See Lieberman (2009).

51 Graham et al. (2008), p. xviii.

52 See for example Barnaby (2001), p. 18.

focuses on a limited tactical role for chemical and biological weapons.[53] Similarly, some analysts of international think tanks, such as Chatham House, consider CBRN incidents on a more modest scale, arguing the probability of medium or small-scale terrorist CBRN attacks.[54] Nonetheless, in general, analysts and researchers assume disastrous intentions and consequences of CBRN events and programs.

There is a consensus on the importance of CBRN threats. All countries analysed have identified CBRN terrorism or other CBRN weapon use and the proliferation of CBRN weapons as the most important security threats.

There is little consensus on the probability of a terrorist CBRN attack. On the one hand, experts take the possibility of a CBRN attack quite serious. Many authors point out that the relevant knowledge and CBRN materials are widely available and that today's terrorist organisations have eschatological visions and non-negotiable goals, a rationale that goes well with the use of CBRN weapons.[55] On the other hand, some argue that there are good reasons not to overstate the threat of CBRN terrorism. Few terrorist organisations have the time, expertise and space to secretly produce CBRN weapons.[56] Several experts state that the attempts of terrorist CBRN attacks so far have not been particularly successful. For instance, the average number of casualties of CBRN attacks is less than half of the average casualty rate of attacks with conventional weapons.[57] Even organisations like Al-Qaeda, which has yet to commit its first CBRN-attack, and Aum Shinrikyo, which executed one CBRN attack, have had great difficulties in developing CBRN weapons, even though they both had extensive resources at their disposal.[58] The sarin attack in the Tokyo metro is, more because of the panic and chaos it caused than the number of deadly victims, one of the few examples of a successful terrorist CBRN attack. Therefore, some experts expect terrorist organisations to stick with more conventional weapons. According to experts, CBRN weapons are neither easy to acquire nor easy to use, an argument that some of the policy documents concur with.[59]

53 See for example Tenet (2004); Davison (2007b).
54 Cornish (2007).
55 See for example Pluta & Zimmerman (2006); Laqueur (1999), pp. 4-5.
56 Parachini (2003).
57 Ivanova and Sandler (2007).
58 Daly et al (2005), p. 69.
59 Jenkins (1975), p. 135.

States have more resources to acquire CBRN weapons than non-state actors.

Unsurprisingly, the literature confirms the estimation in policy documents that states have more resources than non-state actors. Frequently cited arguments for this assertion are a state's larger financial resources, logistical capabilities (e.g. storage), an R&D base with better access to technology (not just CBRN agents but also effective delivery methods) and better access to raw materials.[60] Given the increasing availability of CBRN knowledge and materials due to their dual-use nature, this does not mean that terrorists are unable to acquire CBRN weapons.[61] For instance, Barnaby notes that 'the ease of acquisition is one reason why terrorists are likely to find biological agents attractive'.[62] Although disparate formulations exist and implicit assumptions are present, analysts agree that states have more resources than non-state actors such as terrorist groups. This is also why states are more likely to acquire nuclear weapons, whereas terrorists would opt for chemical, biological, radiological weapons.

Non-state actors are less restrained than states by a political backlash as a result of the use of CBRN weapons.

Some experts argue that the nature of today's Islamist terrorist organisations makes it likely that they will engage in mass casualty terrorism, possibly by using CBRN terrorism. This view is held most prominently by Walter Laqueur and Bruce Hoffman, who stress the importance of the ideology of Islamist terrorists. They argue that these organisations see themselves as fighting an all-out war to destroy the existing order. Therefore, they will not be deterred from using CBRN-weapons.[63] As Islamist terrorists believe that martyrdom will take them to paradise, the threat of deadly retaliation will not have the desired effect.

Furthermore, unlike a state a terrorist organisation has no permanent location or basis that can be struck for retaliation.[64] These views have been challenged on a number of grounds, for such as that fanatics make up only a small part of a terrorist organisation and that other parts can be deterred, that the use of CBRN-weapons can be deterred by lowering the probability of success in using

60 Fangmark & Norlander (2005).
61 Kerr (2008).
62 Barnaby (2001).
63 Laqueur (1999), pp. 4-5.
64 See for example Betts (2002); Shultz & Vogt (2002); Feinstein & Slaughter (2004).

them and that Islamist terrorist organisations, like organisations of other ideological inclinations, need the support of a constituency, which they might lose when CBRN-weapons are used. Intentions of terrorist groups may fluctuate between minor disruptions and massive destruction. This may also depend on the capabilities of various terrorist groups. Yet, intentions of terrorist groups areare compatible with the modus operandi of CBRN weapons as a CBRN attack does not have to be on a massive scale. This renders a CBRN attack a viable means for terrorist organisations to achieve their goals.

Even though there is a willingness to name states that pose a CBRN-states are not naming non-state actors that pose a CBRN-threat. Al-Qaeda is the only organisation that is explicitly named.

The terrorist CBRN-threat proves hard to pin down. The lack of concrete instances of CBRN-weapons use by terrorists is not a gap that can be filled by examining the literature. The vast majority of the experts name only Al-Qaeda and aligned groups as possible perpetrators.[65] More eccentric suggestions include speculations on CBRN-weapon use by the Christian Identity movement and the environmental extremists.[66]

CBRN-weapons are framed as a composite category of threats.

The literature displays less inclination to speak of CBRN-weapons as a composite category than the reviewed policy documents. A number of publications draw a distinction between chemical, biological, radiological and nuclear components of CBRN weapons. Some argue that terrorist groups are more likely to use chemical, biological or radiological weapons, including the so-called dirty bombs, because of the ease of acquisition and the relatively low technological requirements.[67] Lindstrom, in his terrorist threat analysis for Europe, does not even include the nuclear dimension, indicating a clear distinction between CBRN subcomponents, particularly in the analysis of use by non-state actors.[68] Experts also assume that states are more likely to acquire nuclear weapons, since that requires more resources.'

65 Exceptions include Bruce Hoffman and Rob de Wijk, who describe specific terrorist plots to execute CBRN-attacks. See De Wijk (2006); Hoffman (2007), pp. 10-12.

66 Ferguson & Potter (2005) ; Ackerman (2003), pp. 160-161.

67 See for example Graham et al. (2008); Kerr (2008); Lindstrom (2004); Cordesman (2001).

68 Lindstrom (2004).

3.9 Conclusions

From a review of available literature and policy documents the following conclusions can be drawn:

- The threat of CBRN-terrorism may be overrated. For some, the low probability in combination with a possible high impact warrants the policy priority that is currently given to CBRN-terrorism. For others, the focus is on the low probability itself. A sounder argument on the impact and vulnerability is needed to balance this discussion. This could be done by providing a more elaborate explanation and justification of the two other components of impact and vulnerability, rather than the lopsided focus on probability (capabilities and intent) of terrorist use of CBRN-weapons. The two former factors tend to be undervalued in the analysis.
- The CBRN-policies of the countries analysed are not based on a complete risk assessment. Ideally, decisions on whether or not to adopt certain measures to counter CBRN-threats should be based on an exhaustive analysis.
- A well-founded decision requires in-depth knowledge about the actors that are posing the threat (probability), technological know-how about the consequences of the release of CBRN agents with different delivery methods (impact) and knowledge about the assets and locations that need to be protected (vulnerability). A framework to gather this knowledge and inform decision making, would be helpful to states.

4 The future of CBRN

4.1 Introduction

CBRN weapons are often lumped together under the header of weapons of mass destruction (WMD). This is odd, to say the least, given their different nature, both in terms of their make-up, ease by which they may be produced and potential for destruction. It may be the result of what they share in common: their effects do not rely on conventional explosives and CBRN weapons harness deadly, invisible forces (nuclear radiation, biological microorganisms, or poisonous compounds). As such, CBRN weapons invoke tremendous fear and abhorrence in people.

CBRN weapons are subject to continuing scrutiny and intense debate amongst policymakers, academics and military professionals. In the 21st century, CBRN materials may be utilised and deployed as weapons in novel ways, both militarily and in the civilian domain, in times of war as well as in times of peace.

This chapter looks at the potential future use of CBRN materials in the next five to fifteen years. It analyses the technological and geopolitical aspects of the production, proliferation and actual use of CBRN materials as weapons, and examines the capabilities and potential intentions of state and non-state actors. It discusses components of CBRN material individually, the political regimes that govern them, the production methods that may be developed and the new types of weapons that could be produced.

4.2 C, B, R, N materials and uses: key trends

Chemical weapons

The Chemical Weapon Convention (CWC) and challenges

The main challenge to the CWC arises from the huge amounts of chemical compounds that are continuously processed and transported around the globe for industrial applications. Some of these chemicals are toxic and generally

referred to in the literature as Toxic Industrial Chemicals (TICs).[69] The median lethal toxicity of TICS is between 10-100 times lower than that of CW agents, but compared to the approximately 70 existing CW agents there are about 70,000 different TICs, many of which are produced in great quantities and stored and transported around the world.[70]

The fact that large amounts of, in some cases extremely dangerous chemical agents are produced and stored in relatively poorly secured civilian industrial facilities and routinely transported over long distances, creates a considerable, threefold risk:

- TICs might be released accidentally during transport, handling or storage;
- TIC transports or production sites may become targets of attacks (particularly by non-state actors) aimed at releasing TICs into the environment;
- TICs constitute a proliferation risk as non-state actors may divert large amounts of dangerous chemical agents relatively easily and use the material as basis for a CW attack.

The dual-use nature of chemical materials and technology to weaponise these agents pose a challenge to the CWC regime. Whether the efforts to supplement the CWC with additional regimes, such as the European project REACH (Registration, Evaluation, Authorisation, Restriction of Chemicals) will strengthen governmental oversight, remains to be seen.[71]

The CWC was not designed as a counter-terrorist convention. As such, the CWC focuses on the production of militarily significant quantities of chemical agents and not on smaller quantities which might be useful to terrorist organisations. Within the current verification regime, it is impossible to guarantee that a diversion of relatively small quantities of key toxic chemicals will be detected. While the fabrication of CW will remain a technological challenge to non-state actors, they harbour the intent to use CW, and may be able to produce and deploy rudimentary CW.

69 Ibid., p. 21.
70 Hincal & Erkekoglu (2006), p. 220.
71 European Commission (2009b).

Technological developments and future use of chemical materials

Rapid developments in science and technology have complicated the nature of the work of the Organisation of the Prohibition of Chemical Weapons (OPCW). The globalisation of chemical industry, with thousands of facilities spread all over the world, and many 'multipurpose batch facilities that can be readily switched from one product to another,'[72] is a challenge to any inspection regime and provides an increased logistical burden to the OPWC. The introduction of micro-reactors allowing for safe, small-scale production of chemical agents, which are easy to hide and thus more difficult to detect, create additional difficulties.[73]

A key trend in science and technology that is likely to affect the future of CW is the increasing convergence of chemistry and biology. This may result, among other things, in different synthesis routes to existent toxics and the possibility of new, laboratory-designed toxics.[74] Discoveries in nanotechnology offer additional possibilities to assist in dispersal methods.[75] States with a relatively weak knowledge base will be able to produce and effectively deploy advanced CW. However, the production and effective deployment of advanced CW will likely remain a considerable technological challenge to non-state actors, although according to some analysts not an insurmountable one.[76] Cruder ways of chemical agents' dispersal– such as currently practiced by Iraqi insurgents, who combine chlorine with conventional explosives, to name only one known example – may belong to the realm of possibilities, especially within an asymmetric context.[77]

While usually discussed in the context of the future of BW, the biotech revolution may have similar implications for the future of CW. To understand this, one only has to think of the fact that most drugs that will result from advanced biotechnology are likely to be chemical agents. Similar to future BW, future CW will profit

72 Matoušek (2007).
73 Sweijs & Chehin (2007).
74 Matoušek (2007).
75 Sweijs & Chehin (2007).
76 Cornish (2007), p. 9.
77 Brodsky (2007).

from an advanced understanding of the biochemical processes in human bodies.[78]

This opens the possibility to develop advanced CW (ACW). This has led to renewed interest by state actors in developing a specific class of ACW, usually described as non-lethal, less-lethal, advanced riot-control, immobilizing, incapacitating agents, capabilities, technologies, techniques, devices, but never actually as ACW.[79] The reason for this diffuse and euphemistic labelling is to avoid the impression that these research programs constitute a violation of the CWC, which bans CW R&D but explicitly allows for the development and deployment of riot control agents for law enforcement purposes.[80] The most extensive known state-led research programs into ACWs are run by the US, Russia, and the Czech Republic. These programs are often funded by the military and include research into advanced means of dispersal (e.g. grenades, mortar shells, smoke, paintball-like bullets, sponge-like bullets etc.).[81]

What this type of ACWs have in common is that they aim to (a) incapacitate, immobilise or render the target unconscious within seconds after exposure to minor doses, (b) the effects last for at least a few minutes or longer, (c) aim to minimise the danger of lethal effects or permanent damage to the target, (d) typically rely on an advanced neuroscience which allows for an understanding and manipulation of complex chemical processes in the human brain.[82] In essence, law enforcement and military are looking for a powerful non-lethal 'knock-out' agent dispersed in different forms for wide-ranging application in 'peacekeeping missions; crowd control; embassy protection; rescue missions; and counter-terrorism', as well as 'hostage and barricade situations; crowd control; close proximity encounters, such as, domestic disturbances, bar fights and stopped motorists; to halt fleeing felons; and prison riots'.[83]

78 Kelle (2007), pp. 7-16
79 Davison (2009).
80 Ibid.
81 Davison (2007b), p. 15.
82 Dando (2002).
83 Department of Defense (1999) as cited in Davison (2007b), p. 17.

Biological weapons

The Biological Weapon Convention (BWC) and challenges

Concerns about future proliferation of biological weapons focus mainly on non-state actors and the growth of advanced biotechnology in an increasingly important part of the global economy, also in developing countries. The fundamental 'dual-use' character and accelerating diffusion of biotechnology leads to a mushrooming of actors with potential access to material, infrastructure and expertise to develop BW and even advanced BW (ABW).[84] This includes many developing countries and potentially sub-national actors. Non-proliferation efforts will be challenged by the fact that potential BW programs may be difficult to distinguish from legitimate biotechnology enterprises. These developments pose a challenge to the existing non-proliferation regimes for BWs.[85]

If successfully deployed, a terrorist attack with BW could have devastating consequences. Ten grams of anthrax spores can theoretically kill as many people as a ton of the nerve gas sarin, and 30 kg as many people as a nuclear bomb of the size used in Hiroshima.[86] Handling BW agents is obviously hazardous but obtaining them is relatively easy and cheap in comparison to chemical or nuclear weapons. However, the key challenge to a non-state actor would be to effectively weaponise and deploy an agent, which demands extensive scientific and technological know-how. In most cases, this will make the use of BW by terrorist groups 'more difficult or less effective than most people realise'.[87]

Technological developments and future use of biological materials

Experts stress that development in biotechnology will be the dominant influence on the future development of BW. Advances in understanding and manipulating genes, cells, and organisms are reinforced through parallel revolutions in information and nanotechnology, as well as neurosciences. While many of these developments are aimed at benign applications, biotechnology may also lead to dangerous new BWs.[88]

84 Purkitt (2005); Aincough (2002).
85 Shea (2007).
86 Barnaby (2001), p. 21.
87 Ackerman & Moran (2005), p. 11.
88 Wheelis & Dando (2003), pp. 52-56.

At present, some biological agents are readily available in the natural environment, whereas others may be ordered through facilities that supply the market for civilian research. The capacity to manufacture old and new biological agents will become more prevalent over the next decade. In the last decade, American scientists managed to recreate the 'Spanish Flu' influenza virus in this manner, but new –and more advanced- agents are expected to appear in due course.[89] The impact of biotechnological advances on future BWs will take place in three principal phases:[90]

- Enhanced countermeasures will become available against the limited number of existing 'traditional' BW agents;
- 'Traditional' BW agents will be enhanced into more stable, more easily delivered, more contagious, and/or more lethal variants. As for now, possibilities for manipulating 'traditional' BW agents are limited and countermeasures against these enhanced BWs will also eventually become available;
- Continuing advancements in biotechnology will make it eventually possible to design a large variety of 'advanced' BW (ABW) agents. These highly effective ABWs may target a wide range of different biological processes and be designed to create a very wide range of different effects.

The possibility of creating ABWs is particularly worrisome. Such ABWs may consist of binary BW (where a second agent must be deployed to trigger the effects of the BW), malign gen therapy (where harmful genes are inserted into a target organisms), or designer diseases (where a disease and its pathogen are engineered from scratch).[91] The effects of such weapons could be tailored very precisely to the wishes of a user and target specific ethnicities, mask the source of the attack, etc.[92] ABWs may also target plants or animals.[93] This threatens to

89 'Lethal Virus from 1918 Genetically Reconstructed: US Army scientists create "Spanish Flu" virus in laboratory - medical benefit questionable.' The Sunshine Project News Release, October 9, 2003.

90 Nixdorff et al. (2004), p. 1.

91 Ainscough (2002), p. 20.

92 Ibid.

93 Wheelis (2000).

create a 'diffuse and fundamentally unknowable'[94] range of potential BW agents and hence a 'diverse and elusive threat spectrum'.[95]

It is and will be within the reach of the majority of state actors, even those with less developed economies, to produce BWs. However, it is less clear whether all states will partake in the revolution in the biotechnology and nanosciences and create and produce ABWs. Similar to CWs, the effective weaponisation of biological agents may pose a problem for non-state actors, depending on how widespread the fruits of the nanotechnology revolution will be reaped. Cruder and more traditional forms of dispersion of biological agents – such as the poisoning of a well or through an infected individual, or other unforeseen ways – should not be ruled out.

Radiological weapons

While some R&D towards RWs was conducted during the Cold War, states have rarely developed RWs[96]–presumably preferring to concentrate their efforts on acquiring more powerful and deadly nuclear weapons (NW). However, interest in RW has increased in recent years as they may constitute an attractive weapon for non-state actors with limited capabilities and resources.[97] Far less destructive than a NW, an effective RW could nonetheless cause considerable casualties, widespread panic and disruption, as well as sizable economic damage.[98]

Availability of radioactive material

Radiological materials are used in large quantities in civilian facilities around the globe, some of which lack strict monitoring or security arrangements as will be discussed more in depth in the section on NWs.[99] Radioactive material may also be obtained from the civilian nuclear fuel cycle, e.g. by harvesting it from widely used mixed oxide fuel (MOX), which is a relatively simple technical procedure.[100]

94 Nixdorff et al (2004), p. 1.
95 CIA Office of Transnational Issues (2003).
96 The most elaborate known attempt by a state to produce a RW was conducted by Iraq in the late 1980s. However the results were apparently disappointing and the program shelved, see United Nations Special Committee (1995).
97 See Cornish (2007), p. 16.
98 Zimmerman & Loeb (2004).
99 Cornish (2007), p. 16.
100 Barnaby (2001), p. 27.

The more potent the material and the greater the quantities acquired, the more hazardous it becomes to transport and handle the material. However, terrorist groups with a fanatical following with little regard for their own life might be willing to accept their own exposure to harmful radiation while preparing and executing an attack.[101]

Weaponising radioactive material

The typical example discussed in the literature for dispersing radioactive material in order to harm a target population is the so-called 'dirty bomb'. A dirty bomb packs the radioactive material together with powerful conventional explosives. The explosion of the dirty bomb disperses particles of radioactive material over a large area. There are divergent opinions on the effectiveness of a dirty bomb and much of it will depend on the force of the explosion, the type of radioactive material used, the particle-size of the dispersed material, weather conditions, countermeasures etc. However, there is a consensus that the amount of casualties would be relatively low and probably not reaching more than a hundred.[102] Nonetheless, the repercussions of a RW are likely to be severe due to the large scale disruption of public life, stress on the health care system, extremely expensive clean-up operations, and the probability of a sizable psychological impact.[103] While it isn't trivial to produce a dirty bomb with optimal particle size and dispersion pattern to maximise casualties, it is considerably simpler than constructing a nuclear device, as no fission or fusion reactions have to be triggered.

Experts have drawn attention to alternatives to dirty bombs in dispersing radioactive material. A variety of approaches could be used to disperse fine particles amongst a target population, provoking it to inhale, ingest or to become immersed with radioactive matter. This could be achieved by, for example, radioactively contaminating water or food supplies, aerosolizing radioactive material or dissolving it in water which could be used to soak victims with it.[104] Such an approach could be considerably more dangerous than a dirty bomb if it is success-ful in getting victims to absorb radioactive material into their bodies,

101 Zimmerman & Loeb (2004), p. 5.
102 Acton et al. (2007), p. 152.
103 Cornish (2007), p. 17.
104 Acton et al. (2007).

as miniscule amounts of radioactive material are likely to be lethal if ingested or inhaled.

In the aftermath of 9/11, a fervent discussion has taken place on the prospects of terrorist groups attacking civilian nuclear reactors in order to seize dangerous radioactive material for the purpose of assembling a 'dirty bomb' or to sabotage a nuclear plant in order to cause the hazardous leakage of radioactive material. Experts agree that the threat from using spend fuel rods in a RW is relatively minor, paradoxically because of the fact that they are so dangerous: Unshielded exposure to fuel rods is likely to cause a lethal radioactive dose in a very short time span and the extremely hot and heavy rods are difficult to manipulate, let alone to transport to a suitable target for detonation.[105]

A particular focus of the research has been the likely consequence of a commercial airplane being crashed into a nuclear power plant in an attack modelled after the 9/11 attacks.[106] It is relatively difficult to draw clear conclusions from these debates, as they involve intricate technical detail and are highly politicised. Stakes are high as many experts are intimately connected to the nuclear industry and additional security measures can be immensely costly. Opponents of nuclear energy have used the debate to underline their argument that nuclear power plants constitute an incalculable security risk. It should not be surprising that the key findings have been controversial. Positions range from those who argue that even the impact of a fully fuelled commercial airliner on basic reactor security would be negligible,[107] to those who claim that it might result in a reactor meltdown and the release of radioactive material on a scale that could exceed that of Chernobyl.[108]

Nuclear weapons

Non-Proliferation Treaty (NPT) and challenges

Recent years have provided ample evidence of the existence of a thriving black market in nuclear materials and technology.[109] Materials traded are dual-use goods and subcomponents for example for gas centrifuges, reactors, computer-

105 Cravens (2002), pp. 40-44.
106 Behrens & Holt (2005).
107 Rossin (2005).
108 Hirsch (2001).
109 As illustrated by interviews with Abdulkeer Khan on the scope and dealings of his network, see Fitzpatrick (2007).

numerically controlled machine tools, laser alignment systems and hot cell technology.[110] Concealing such technologies will be easier in the future.[111] The existence of poorly guarded nuclear facilities in the former Soviet Union constitutes a particular source of proliferation concern.[112]

Highly enriched uranium is not only found in military facilities, but is stored in civilian facilities in over 40 countries worldwide, where it is used for research purposes. Estimates of civilian HEU reactor material are in the range of 50 tons, which would be sufficient to produce 2,000 NWs.[113] Recent history is rife with examples of nuclear material that has gone missing and is unaccounted for until today.[114]

NWs are seen by many states as playing a key role in the international balance of power and as a valuable instrument in the promotion of national security. The advent of one new nuclear state may create a momentum towards further proliferation, as neighbouring states are confronted with a worsened security situation that will drive them to attain a nuclear capability of their own.[115] Amongst potential proliferators are Egypt, Jordan, Saudi Arabia and Turkey, in the event that Iran goes nuclear, Japan and South Korea if North Korea goes nuclear, Syria to counter Israel and possibly Burma.[116]

The US nuclear umbrella has dissuaded many allies from attaining a nuclear capability of their own. This is seen as a major factor in stemming proliferation.[117] If, for whatever reason – e.g. US isolationism or ruptures in US bilateral relations – states would lose their faith in the US protective umbrella, it may motivate them to go nuclear.[118] In the face of proliferation, existing nuclear powers may also resume nuclear testing to ensure the reliability of new weapon systems,

110 Ibid.
111 Bernstein et al (2007), pp. 12-14.
112 Pluta & Zimmerman (2006).
113 NATO (2008).
114 International Atomic Energy Agency (2007).
115 Department of Defense (2006), p. 3.
116 Cetron & Davies (2005); el-Baradei (2009), pp. 4-5.; Institute for Science and International Security (2009), pp. 4-5.
117 Department of Defense (2006), p. 3; Dunn (2009), pp. 144-145; Sagan (1996), pp. 57-62; Waltz (1981).
118 Hughes (2007); Campbell et al. (2004).

further undermining the spirit of the NPT and the CTBT, with ample opportunities for international crises to erupt.[119]

Nuclear terrorism

As described previously in the chapter 'CBRN – a primer', non-state actors would face significant obstacles in building a nuclear bomb. Yet, some experts stress that they are able to build an improvised nuclear device, if not an actual NW, once they are in the possession of enough weapons-grade uranium or plutonium.[120]

Alternatively, state actors may hand over a NW to a non-state actor.[121] States that would be afraid to use the NWs themselves would share the weapons with a non-state group that wouldn't have to fear for annihilation. This scenario is not very realistic since it would be possible to trace the source of the weapon with a fair degree of accuracy.[122] Still, radical elements within a state apparatus may be inclined to share a nuclear device.[123] Some analysts consider this to be a risk in the former Soviet Union and Pakistan, as they express doubts about the level of security of their NWs facilities (although other analysts disagree with this assessment).[124] In a worst-case scenario, these weapons may fall in the hands of non-state actors in case of state failure, which is at present a concern with respect to Pakistan, but may apply to other nuclear state actors of the future.[125]

Technological developments and future nuclear weapons

Nuclear materials, technology and knowledge will continue to proliferate as a result of increasing mobility of information and people, and a diminished capacity on the part of states to monitor and control these flows. The globalisation of education opens up possibilities to gain the necessary scientific

119 Schneider (2004).
120 Pluta & Zimmerman (2006).
121 Bobbitt (2002).
122 Allison (2008); Joint Working Group of the American Physical Society and the American Association for the Advancement of Science (2008).
123 Cetron & Davies (2005), pp. c12-13
124 For Pakistan, see Gregory (2009); for the former Soviet Union, see Langewiesche (2006); Albright et al. (2001); Allison (2004).
125 Lee (2005), p. 1-3.

expertise, both in the field of nuclear enrichment and in weapons design.[126] Mastering the production of the key materials – enriched uranium or plutonium is the main challenge. The weaponisation of these materials, although still requiring substantial technological expertise, is a slightly lesser challenge – especially for state actors – with rough drawings for the construction of fission and fusion devices available in the open literature.[127]

Experts also discuss the development of new types of NWs and alternative uses. Specifically, they describe the development of low yield tactical weapons such as nuclear bunker busters and Robust Nuclear Earth Penetrators (RNEP),[128] as well as electromagnetic pulse-effect bombs and high-altitude nuclear blasts designed to disrupt an enemy's information networks and systems through a powerful electromagnetic impulse.

4.3 Findings and conclusions

This chapter has analysed the potential future use of CBRN materials as weapons in the next five to fifteen years. Five key observations can be made:

- Expert discourse focuses predominantly on the future of biological weapons. This can be explained by technological developments in this domain and by the nature of present and future biological.
- Experts debate the consequences of a CBRN attack perpetrated by actors with malicious intent, rather than the consequences of a CBRN disaster caused by a manmade or natural hazard.
- There is a bias towards describing worst-case scenarios. CBRN events with a lesser impact tend not to be considered.
- Within the CBRN domain, a significant gap exists between the scientific and the policymaking community. Except for some literature on the threat posed by nuclear materials, there is little authoritative work that incorporates both geopolitical and scientific/technological dimensions of the debate on the future of CBRN weapons. While scientists tend to focus narrowly on technological details, policymakers tend to discuss the broader picture

126 Knowledge diffusion has been one of the drivers of past proliferation with Abdulkeer Khan, the father of the Pakistani nuclear bomb, receiving university diplomas in Germany and the Netherlands and being employed in nuclear facilities in the latter before returning to Pakistan. See The Hague Centre for Strategic Studies (2009).

127 See for example Morland (1999).

128 Medalia, Jonathan (2004), p. 24.

without having a real understanding of the technological fundamentals underlying it.
This may produce unrealistic projections of capabilities.
- Some experts extrapolate from the present when talking about actor's intentions, the proliferation of materials and the future of dual-use technology. Yet, there is a significant degree of uncertainty on the impact of the revolutions in the field of bio- and nanotechnology, and how these may affect types of agents, ease of production and magnitude of effects.

Within this context and given the aforementioned caveats, a number of conclusions may be drawn with respect to future developments in the field of science and technology, materials, intentions and capabilities.

Science and technology

- An increasing convergence of chemistry and biology;
- Tremendous advances in understanding and manipulating genes, cells, and organisms;
- Developments in the field of nanotechnology that may revolutionise dispersal methods.

Materials

- An increasing availability of CBRN materials;
- The potential to engineer (CB) materials from scratch;
- A growth in the number of dual-use materials and technology that may pose major challenges to non proliferation regimes.

Intentions

- A persistent intention on the part of state actors to acquire (new types of) CBN capabilities;
- A persistent intention on the part of non-state actors to acquire (new types of) CBRN capabilities and in some cases an explicit desire to use these capabilities.

Capabilities

- Significantly fewer hurdles to state actor CBRN acquisition as a result of knowledge diffusion and economic globalisation;
- Fewer hurdles to non-state actor CBRN acquisition, although these will continue to exist;

- The emergence of a distinction between future and traditional BCW, with the former the prerogative of state-actors while the latter may be within the reach of both state and non-state actors.

Overall, in the 21st century, CBRN materials may be utilised and deployed as weapons in novel ways, both militarily and in the civil domain, in times of war as well as in times of peace.

5 Examining national capabilities

5.1 Introduction

This chapter provides a broad overview of the CBRN-policies and capabilities[129] of six countries: the US, the UK, France, Germany, the Netherlands and Canada. We also look at how NATO and the EU, two important international organisations, consider the issue of CBRN. The main purpose of this chapter is to inform stakeholders how these countries deal with the risk of CBRN-attacks and accidents. To this end, this chapter analyses the key documents describing CBRN policies and capabilities for the respective countries surveyed. Although the nature of the documents examined differs from country to country, they typically include national security strategies, antiterrorism strategies and documents detailing national policies regarding security and safety, as well as websites of the relevant organisations and departments.

Not all countries have spelled out their security policies in the same level of detail. The US government, and especially the Department of Homeland Security (DHS), has published many policy documents outlining strategies, crisis management arrangements and budgets concerning security, including preparation for CBRN-incidents. The same is true for the UK. For Germany and France, this kind of information is considerably harder to come by, possibly because this information is classified. The Netherlands and Canada fall somewhere between the US and the UK on the one hand and Germany and France on the other. On a note of caution, there are obviously more detailed organisational arrangements and substantive elaborations in each of these countries that have not been considered in the present analysis. This chapter will analyse the policies of the selected countries at the strategic level; that is, we will

129 Capabilities can be defined as the ability (expressed in, for example, required people, processes and equipment) to perform certain tasks.

compare the countries as regards general policy characteristics, as opposed to doing a full-fledged benchmark.

In the first section, we consider whether these countries deal with the issue of CBRN as a distinct policy issue or as part of a larger policy issue. We will also provide an overview of the actors involved in CBRN policies. The second section discusses and evaluates CBRN capabilities along the analysis-prevent-response (APR) chain. The APR chain provides an analytical framework to identify and determine capabilities to counter security threats. This framework will also be described in more detail in this section. The concluding section provides a comparative assessment of the national CBRN policies and capabilities.

5.2 National policies and institutional frameworks

Countries take different approaches towards the threat of a CBRN attack or disaster. Some countries formulate specific counter CBRN-strategies at the national level, while other states address CBRN risks within the context of a counter terrorist strategy or within the domain of defence policy. Although most CBRN policies have a substantial counter-terrorism dimension, CBRN threats by states remain part of the contingencies anticipated by policymakers. This chapter focuses primarily on capabilities along the APR-chain in a domestic context. The emphasis is on the security dimension rather than on safety (health, environment). The role of the military is addressed in this context.

National security and CBRN policies

Canada

Canada has formulated a national CBRN strategy with a strong focus on the risk of terrorist CBRN incidents. The CBRN Strategy complements the *Government of Canada's National Security Policy*. The Minister for Public Safety and Emergency Preparedness is responsible for the implementation of Canada's *National Security Policy*. This Minister has formal authority in a CBRN crisis situation. All response actions take place within the framework of the National Emergency Response System that includes crisis and consequence management with actors across government. The Canadian Forces assist the civilian response and provide operational support with forces and assets, in addition to being involved in the support of international counter-proliferation efforts and the gathering of CBRN-related intelligence.

France

France has no CBRN strategy but has outlined most of its CBRN policy in *Prevailing Against Terrorism: White Paper on Domestic Security Against Terrorism* and, to a lesser extent, in *The French White Paper on Defence and National Security*. The Secretariat-General for National Defence (SGDN) serves as an advisory body to the head-of-government. France has a designated body to lead its efforts to counter threats and dangers. The Inter-Ministerial Coordination Committee for the fight against CBRN threats is the national governmental body that is installed to ensure consistency in CBRN threat-protection capabilities and a satisfactory execution of research and equipment programs. It also sets high-level policies for a coordinated interdepartmental and comprehensive approach in addressing CBRN threats.

At a lower organisational level, governmental bodies and emergency services have specialised (and dedicated) CBRN units, (e.g. specialised medical units and fire fighting units), illustrating a distinctive CBRN approach. Relevant bodies in case of an incident, such as the Centre Operationnel de Gestion Interministerielle des Crises (COGIC) of the Ministry of Interior, are activated in a crisis regardless of its nature. Although these civilian actors are leading in responding to CBRN threats, the role of the military is relatively important in France. For example, in the Vigipirate contingency plan, a military presence can quickly be summoned to guard Critical National Infrastructure.

Germany

On the strategic level, Germany has incorporated its CBRN-policies in its civil protection plans, as outlined in the *Neue Strategie zum Schutz der Bevölkerung in Deutschland* (New Strategy for the Protection of the Population in Germany) and the *Nationale Strategie zum Schutz Kritischer Infrastrukturen* (National Strategy for the Protection of Critical Infrastructure). The planning and coordination of these policies are the prerogative of the Federal Office of Civil Protection and Disaster Assistance (BBK), part of the Federal Ministry of Interior, created in May 2004. It does not focus specifically on a terrorist threat but has a broad interdisciplinary mandate in the domain of civil protection and advises other Federal and Land authorities in their missions. Civil protection from CBRN threats falls within the mandate of the BBK. Civilian emergency units throughout the country receive some CBRN training. The BBK is the civilian lead in a CBRN incident and is also responsible for the coordination of civil-police-military cooperation. The Bundeswehr has an NBC Defence Corps to provide a military NBC defence

capability but can also be called upon by civil actors in case of a non-state actor incident.

The Netherlands

The Netherlands has not formulated a CBRN strategy that is similar in nature to the strategies of other countries. The National Security Strategy (*Strategie Nationale Veiligheid*, SNV) outlines the process to formulate policy priorities rather than the policy priorities themselves. Also, the Netherlands has not assigned the responsibility to counter CBRN to a specialised bureaucratic unit. The National Coordinator for the Fighting of Terrorism (NCTb) covers some elements of a CBRN policy, especially the (terrorist) threat analysis. The NCTb is a post-9/11 central civilian agency in charge of national efforts to counter terrorism and related (CBRN) threats. It receives and analyses information from across government. In addition, there is an interdepartmental CBRN working group. The Minister of Interior is the coordinating minister in all crises and disasters. The National Crisis Centre coordinates and assists the provinces that, in turn, direct the local emergency services during a crisis. Specialised CBRN units assist emergency services. In case of a terrorist threat or incident, the NCTb leads this coordination. The Dutch military has a specialised CBRN unit that is able to assist civilian actors in case of an incident. The primary purpose of the military is to provide a military operational capability in CBRN threat deployment areas that focus primarily on state threats.

United Kingdom

The United Kingdom has implemented a national civilian counter-terrorism programme (CONTEST) led by the Office for Security and Counter Terrorism of the British Home Office. This strategy contains most of the principles guiding CBRN-related policies and measures in the UK. Further guidelines for CBRN policies are laid out in the national security strategy of the UK and, for the military domain, in *Delivering Security in a Changing World: Defence White Paper*. The CBRN terrorist threat is mostly addressed within the CONTEST programme. Civilian actors, coordinated by the Home Office, have the lead in the response phase, while military actors focus primarily on threats from other states. The emergency services in the UK all receive CBRN training. The police forces host the Police National Centre for specific CBRN training. The Jt. CBRN Regiment of the UK Army, supplies similar CBRN response capabilities to British military forces at home and abroad and can assist civilian units if necessary.

United States

Like Canada, the United States has a separate strategy CBRN-strategy, the 2002 *National Strategy for Combating Weapons of Mass Destruction*. Institutionally, however, CBRN is integrated in a broader crisis management structure, which serves to arrange the US prevention of and response to both manmade and natural disasters. The *National Security Strategy of the United States of America*, the *Homeland Security Strategy* and the *National Strategy for Combating Terrorism* are the documents that provide the strategic guidance on CBRN-policies. The DHS, largely founded in reaction to the 9/11 attacks, is the most important player in the execution of the CBRN-related elements in these documents, as it is in charge of the efforts to protect the population and the critical national infrastructure and to enhance the US's emergency preparedness. Crises are dealt with on the lowest possible administrative level. Only when a crisis exceeds the resources of that level, will responsibility shift to the higher (state or federal) level. The National Guard has WMD Civil Response Teams, which can be called on to assist civilian actors in case of a CBRN incident. Otherwise, the efforts to deal with CBRN threats in the military sphere are largely separate from the ones in the civilian sphere. The *National Defense Strategy* and the *National Military Strategy to Combat Weapons of Mass Destruction* provide the strategic framework for preparation of the US military for the use CBRN-weapons.

NATO

NATO also devised a strategy for CBRN threats, NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending against Chemical, Biological, Radiological and Nuclear (CBRN) Threats. NATO established a WMD Centre and a Joint CBRN Defence Centre of Excellence (JCBRN Defence COE). As a military alliance, NATO focuses primarily on the involvement of military capabilities to counter CBRN threats presented in the strategy.

European Union

The European Union (EU) does not have a designated actor for CBRN in Europe but a a facilitating role towards Member States. In this capacity, the EU has developed the EU CBRN Action Plan that facilitates and streamlines a concerted EU response to assist Member States in countering and responding to CBRN incidents.

Assessment of national policies and institutional frameworks

The national policies of the surveyed countries are very similar. Yet, some distinctions can be identified. First, a difference exists between countries that treat CBRN as a single threat entity or within a larger threat framework. The German Civil Safety mandate of the BBK and the French Inter-Ministerial Coordination Committee for the fight against CBRN are an example of the latter, the Canadian stand alone CBRN strategy is an example of the former. While this difference may reflect on the relative importance these countries attach to the topic of CBRN, it certainly illuminates the degree to which CBRN policies are bureaucratically anchored. This may affect both the budgets and the nature of the CBRN policies in the years to come.

Second, in some countries a single department determines the formulation and execution of a national CBRN strategy, whereas in other countries CBRN policies are coordinated by interdepartmental bodies at different levels of authority. For example, the Inter-Ministerial Coordination Committee for the fight against CBRN threats in France represents a cross-governmental decision-making body at the level of the prime-minister. The NCTb in the Netherlands, on the other hand, is active at the sub-ministerial level and executes parts of CBRN policies. In contrast, in Canada the Ministry for Public Safety and Emergency Preparedness determines most high-level decision-making.

Third, and closely related to the second point, countries opt for different bureaucratic solutions in dealing with a potential CBRN threat. Some countries, like France and the United Kingdom, do not add an additional bureaucratic layer, but focus on improved cooperation and communication within existing frameworks. Other countries, like Germany, the US and the Netherlands opt for the establishment of new institutions to solidify the analysis, prevention and response chain. These two different approaches have implications for the unity of the formulation and the execution of CBRN policies, and for the consistency of a whole-of-government approach.

Fourth, the role of the military is different from country to country. Various levels of military participation and civil-military integration exist. In some countries, the military is strongly involved in the CBRN analysis, prevention and response stages; in other countries its role is limited. Although sometimes hard to assess, the analysis shows that the military forces of the US and France are strongly involved, while the german military play a more minor role.

These models of integration of the civilian and military responses have implications forloci and modi of R&D, unity of policies and duplication of efforts. These analytical dimensions are depicted in Figure 2.

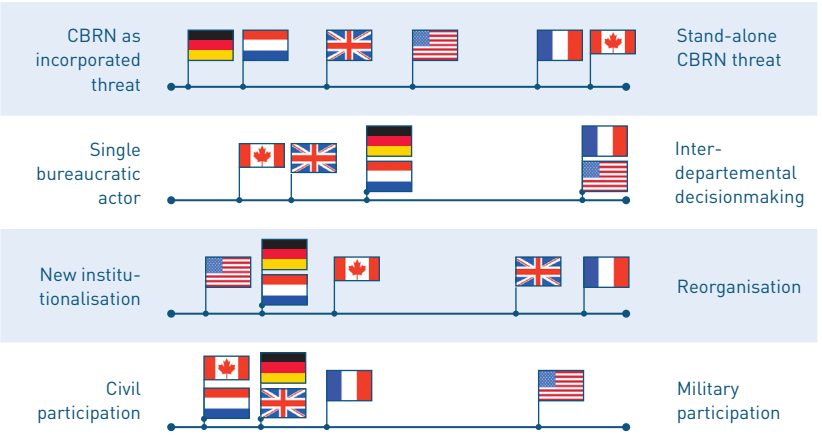


Figure 2. NATIONAL POLICY ANALYSIS ON FOUR DIMENSIONS

CBRN policies in the military domain

This section addresses the military CBRN policies of the surveyed countries. CBRN protection is not only a matter of civilian crisis management, but also of force protection. The ability to sustain military operations in CBRN-environments widens the range of arenas in which the armed forces can operate and thus its ability to conduct expeditionary missions. The following section discusses the arrangements that have been made to prepare the armed forces for CBRN-environments, drawing on defence white papers and military doctrines.

Canada

The Canadian Forces (CF) want to be able to provide CBRN-protection for all military operations, missions or tasks, but there is an element of conditionality: the need will be established on a case by case basis. To save resources, the CF do not include CBRN protection in the standard repertoire of all units. Canada has a separate CBRN defence doctrine to support operations. In CBRN defence operations, specialised units provide various levels of support to regular troops

operating in CBRN environments. Integral Support (IS) represents the lowest level of CBRN security, Close Support (CS) the intermediate level and General Support (GS) the highest. All units have access to IS, CS and GS. CBRN defence is regularly evaluated to ensure that units are not overqualified in CBRN training and to optimise the use of resources.

France

The *2e Regiment de Dragons* is the main actor for French military CBRN defence. It fulfils a variety of tasks, including reconnaissance of sites and zones, risk assessment and management and decontamination. This battalion provides French armed forces, anywhere in the world, with specialists on CBRN in order to sustain military operations in CBRN environments. The French CBRN doctrine focuses on two types of CBRN protection: collective (protection of an entire vehicle) and individual protection (protection of individuals in a vehicle). France is gravitating towards individual protection. This suggests that CBRN training is increasingly incorporated in French basic military training and that every unit should have at least some capability to deal with CBRN environments. This is not a move towards the abolishment of specialised CBRN-assistance, but rather towards a higher degree of self-reliance.

Germany

While there is a general inclination on the part of Germany to deploy the Bundeswehr for stabilisation missions, there is a reluctance to provide troops to high-spectrum missions abroad, which also applies to CBRN units. The Bundeswehr has NBC Defence Units to provide CBRN operational support to deployed forces, and not just German forces. For example, during Operation Freedom German NBC Units assisted American troops in Kuwait. Furthermore, the NBC- and Self-Protection School provides NBC training to specialised CBRN-units. These are also supposed to assist civil crisis management units, as the German security strategy explicitly mentions the role of the armed forces in domestic, civilian crisis management.

The Netherlands

The Netherlands has specially equipped the 101 NBC Defence Company, a unit that can be deployed domestically and abroad, to provide specialised support to operational or forward deployed units. The Netherlands considers CBRN-support as the ability to provide for all potential arenas and does not single out a certain setting or region. Although it can bolster its regular forces, the Dutch military

does not have CBRN units that act as a 'quick entry team'. Therefore, it is relatively limited in its expeditionary capabilities compared to, e.g. the UK or the US.

United Kingdom

The British armed forces operate across the entire force spectrum, including CBRN, with a full expeditionary military force. The UK's Joint CBRN Regiment, consisting of Army and RAF units with specialised equipment (e.g. Fuch trucks), provides a strategic enabling capability to sustain a military effort anywhere in the world, including on British soil, where the unit can assist in CBRN crisis management. The CBRN regiment operates alongside regular military units to provide specialised operational support, as opposed to fully equipping all units with CBRN gear. Moreover, the Light Role Team, part of the CBRN regiment, is an early entry team that can pave the way for regular expeditionary forces. Thus, the British CBRN policy in this field is one of employing specialised units as well as equipping and supporting regular forces.

United States

The US leaves little doubt as to the geographic scope of its ambitions and has a full expeditionary military capability. The National Defense Strategy stresses the severity of the dangers posed by weapons of mass destruction and states the American ambition to sustain operations in CBRN environments around the world. The US Field Manual 3-0 allows for a certain flexibility regarding the role of specialised CBRN-units in the operations of the US Army, as there are several ways to organise this cooperation. CBRN-units can be integrated in a regular force to support these forces in CBRN-protection, or can operate more independently from the regular forces, for instance as a 'first entry team'. The US approach can thus be adjusted to the situation at hand.

As part of NATO a multinational CBRN battalion, the Combined Joint CBRN Defence Task Force, provides an operational capability to maintain freedom of operation in a CBRN threat environment. The battalion is under direct command of the Supreme Allied Commander Europe and has the following operational capabilities: (1) provide identification of CBRN substances, (2) biological detection and monitoring operations, (3) provide CBRN assessments and advice to NATO commanders and (4) CBRN decontamination operations. Although the battalion can be deployed relatively quickly, it does not provide a rapid entry capability similar to the British or American forces.

Assessment of military policies

The countries surveyed are among the most expeditionary forces in the world. Their willingness to be deployed globally ranks high in their defence strategies and policies. Although all surveyed countries are committed to international peace and stability and stress the importance of CBRN threats, there are some striking differences in their military CBRN policies. We will discuss the level of ambition (do the countries want to be able to deploy CBRN-units worldwide or primarily for home defence?) and the way in which CBRN-expertise is disseminated throughout the armed forces (is CBRN expertise concentrated in a few specialised units or is it part of the skills and equipment of all units?).
Not all militaries share the same level of international operating ambitions. In this context, the CBRN units in France, the Netherlands and Germany are more specifically focused on domestic deployment and maintain a relatively low expeditionary organisation, particularly in comparison to the US and the UK. The latter countries, through their availability of rapid entry units, display a higher readiness to intervene in foreign CBRN-environments. A good illustration of the willingness to deploy CBRN-units abroad is the British Light Role Team, which provides a rapid entry capability. By contrast, Germany notes the CBRN capability as a vital asset for protecting the national territory. All surveyed countries allow for the possibility of military assistance in civilian crisis management.

There are also differences in the way CBRN-expertise is incorporated in the armed forces. CBRN-expertise can be a part of the training and preparation of all units or of specialised units. France is moving towards an army wherein all units receive extensive CBRN training and equipment, to promote CBRN autonomy for all units in any theatre. Other countries seem to concentrate their CBRN-expertise in some designated units. This is the case in the UK, Canada, the US and the Netherlands. In these countries, specialised CBRN units are tasked to deal with CBRN environments and threats or assist regular forces in doing so. This strategy results in a decreased robustness for CBRN threats over the entire military spectrum. However, it saves resources and reduces individual unit burdens, for example of heavy equipment. The differences between countries are depicted in figure 3.

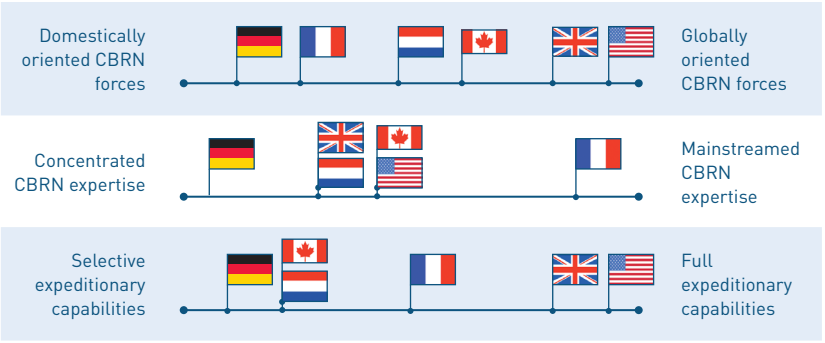


Figure 3. CBRN POLICIES IN THE MILITARY ON THREE DIMENSIONS

5.3 National capabilities

The aforementioned national policies provide the framework within which countries set their CBRN priorities and allocate resources for capabilities to counter CBRN threats. NATO and the EU do not have the full set of resources or capabilities as the sample countries, and therefore these entities are only sporadically referred to in this section. This section compares the national capabilities along the analysis-prevent-response (APR) chain on the basis of a list used in the Netherlands' national capabilities planning process. The three APR categories suggest that CBRN-policies move along a chain that starts with identifying threats and dangers (analysis) to avoiding manifestations of these threats and dangers (prevention) to being able to respond adequately to when a CBRN-incident occurs (response).

The A-category comprises efforts to monitor the CBRN threats and dangers, the collection, analysis and dissemination among the relevant players of CBRN-related intelligence and information, and research into new ways of detecting and protecting against CBRN-agents as well as technological developments that impact on the future use of CBRN-weapons. The P-category covers protective measures, ranging from target hardening and registering CBRN materials to monitoring and auditing CBRN facilities. The R-category includes measures to enhance a country's preparedness for a CBRN-incident, such as stockpiling of vaccines, detection and early warning capability, a CBRN clearing house, and CBRN decontamination and quarantine equipment. The response phase covers more than just the actions taken in case of a CBRN-incident. All efforts to make

sure that the response is adequate fall in the response-category, even though they obviously take place before the actual CBRN-incident takes place.

CBRN capabilities: analysis

An analysis capability is instrumental in determining risks and vulnerabilities and setting policy priorities accordingly. This report distinguishes between Intelligence and a Research & Development (R&D) capability. The first refers to an intelligence capability to monitor CBRN developments in addition to serving as a central dissemination unit for timely CBRN briefs. An R&D base covers the national capability to conduct research into protection against CBRN.

Intelligence

Canada

In Canada, the Integrated Threat Assessment Centre (ITAC) coordinates the security intelligence effort from the Canadian Security Intelligence Service (CSIS), Canada Border Services Agency, Transport Canada, and the Royal Canadian Mounted Police (RCMP), and produces central CBRN threat assessments.

France

In France, there is appears to be no designated CBRN or contra-proliferation unit for intelligence collection and dissemination, not publicly nor as a unit within the secret services. The French intelligence community has no organisation similar to the British JTAC or the US NCTC (see below). However, the French secret services are notoriously closed which possibly explains the absence of information.

Germany

In Germany, the Bundesnachrichtendienst (BND) provides the federal government with foreign intelligence on CBRN threats, the Bundesamt für Verfassungsgeschutz (BfV) and the Militärischen Abschirmdienst (MAD) deliver internal and military intelligence, respectively, concerning CBRN threats and activities. Although a number of agencies are involved in CBRN-related analysis tasks, coordination of these activities by a central (public) CBRN expert or intelligence centre is lacking.

The Netherlands

The Netherlands brings together its CBRN intelligence and expertise within the NCTb, which receives CBRN intelligence from the intelligence services: the General Intelligence and Security Service (AIVD) and the General Military Intelligence and Secret Service (MIVD). Additional analysis of the CBRN threat is conducted by a specialised CBRN unit comprising both intelligence services (civil and military).

United Kingdom

In the UK, the Joint Terrorism Analysis Centre (JTAC), established in 2003, produces analyses and assessments of international terrorism from a various government departments and agencies. JTAC is not specifically directed at the analysis of CBRN threats, but does encompass CBRN threats from terrorists. JTAC is based at MI5 and its Head is accountable to the Director of MI5 (British Secret Service) that is part of the Home Office.

United States

The US Office of Intelligence and Analysis of the Department of Homeland Security is tasked with the collection and analysis of information about CBRN threats. Gathering intelligence about the CBRN threat is also a priority for both the FBI and the CIA who have specialised WMD units. The NCTC is the organisation where all terrorism-related US intelligence is brought together for an overall analysis and dissemination among the relevant partners. The focus of the NCTC's analysis work is not exclusively on CBRN-terrorism, but as the use of CBRN-weapons is cause of concern to US policy makers, the NCTC was specifically tasked to 'provide a clearer picture of terrorist capabilities and intentions, including with respect to WMD'.

NATO

NATO has an analysis capability with the NATO WMD Centre. The WMD Centre works on improving the quality and quantity of military intelligence received by its members, and on improving information on proliferation issues. It also contributes in enhancing military readiness to counter WMD threats by facilitating international exercises and information exchange.

European Union

The EU has a fragmented analysis capability. EUROPOL is an EU institution for information exchange on criminal offences and terrorism with a specialised

Counter Proliferation Programme. On a more strategic level, the EU Joint Situation Centre provides strategic assessments for Member States on internal security issues, including terrorism and CBRN.

Research and development (R&D) base

Canada

Research and development is provided for in Canada with the so-called CBRN Research and Technology Initiative (RTI), which provides funding for research projects and specific funding for fellowships, bursaries and university research chairs. Within government, the Defence Research and Development Canada (DRDC) coordinates governmental CBRN research and supports response capabilities. Outside government, extensive cooperation exists with academia and private institutions through the RTI.

France

France has a comprehensive interdepartmental CBRN R&D programme which is coordinated by the Atomic Energy Commission (CEA). The National Research Agency (ANR) supports civilian technological research and has a special programme dealing with security issues including research on terrorism, organised crime, protection of vital infrastructure, crisis management and border security. The General Delegation for Armament has a similar task for the defence sector.

Germany

The German Bundesamt für Bevölkerungschutz und Katastrophenhilfe (BBK) is responsible for the promotion of civil research activities. In addition it conducts research on behalf of the Ministry of Interior (BMI) as a contractor. With the BMI the BBK determines priorities for research and funds research contracts to research proposals. Closely affiliated with the BBK, the AKNZ (Academy of Crisis Management, Emergency Planning and Civil Protection), organises workshops, meetings, information exchanges and expert meetings on current subjects.

The Netherlands

In the Netherlands various research institutes such as the National Institute for Public Health and the Environment (RIVM), Netherlands Forensic Institute (NFI) and TNO conduct research in the CBRN realm. There is also cooperation with academia. In addition, various ministries support the development of their own CBRN detection equipment. The Ministry of Defence has its own research

programme. Some departments, such as the Ministry of Public Health, Welfare and Sport (VWS) have reserved funding for CBRN research and activities.

United Kingdom

In the UK, the Science and Innovation section in the Home Office provides a scientific basis for research of the CBRN threat by terrorists. Through collaboration with the private sector, industries, academia and other scientific institutions it advances research and development in the most urgent areas. Examples of collaborative partners are the Defence Science and Technology Laboratory (DSTL), the Health Protection Agency (HPA) and the Atomic Weapon's Establishment (AWE). The Home Office' Scientific Development Branch is the general research centre.

United States

In the US, the DHS is involved in R&D for CBRN-agents detection and mitigation of their impact. Research takes place in-house, coordinated by the Office of National Laboratories (ONL), as well as through funding of external research institutes. For instance, the Domestic Nuclear Detection Office DNDO sponsors research by private companies to develop detection tools and devices.

Assessment analysis

Obviously, all countries have an intelligence capability; yet, significant differences exist in terms of where this capability is located within the bureaucracy and the extent to which this capability has specialised CBRN knowledge. Some countries operate specialised CBRN intelligence units that are integrated and coordinated by a single actor, as illustrated by the NCTB in the Netherlands that integrates and disseminates the intelligence of the joint civil and military services. Other countries have decentralised intelligence units that report to different authorities, such as in Germany and France.

These different modes of organisation not only indicate the degree to which intelligence is shared within these bureaucracies (to what extent are these services stove piped?), but may have implications for the way in which R&D funding for intelligence capabilities is allocated.

With respect to R&D, investment is not always earmarked as CBRN R&D. The role of the government in supporting and encouraging CBRN R&D varies from country to country. In Germany, research is heavily directed by the government

with the BBK and BMI prioritising and funding research proposals. In the Netherlands and Canada academia and research institutions conduct most research, funded by the government. Similar to intelligence capabilities, all countries fund and direct research to some degree and distinctions are gradual rather than absolute. The involvement of governments in funding and directing CBRN research is relevant since the penultimate rationale of the role of governments is to provide the common security good. It is unclear whether the CBRN R&D market will be comprehensively catered by private initiatives. In the absence of a clear market demand, it is crucial that the direction of research is informed by substantial knowledge of the entire CBRN domain.
The differences in national analysis capabilities are depicted in figure 4.

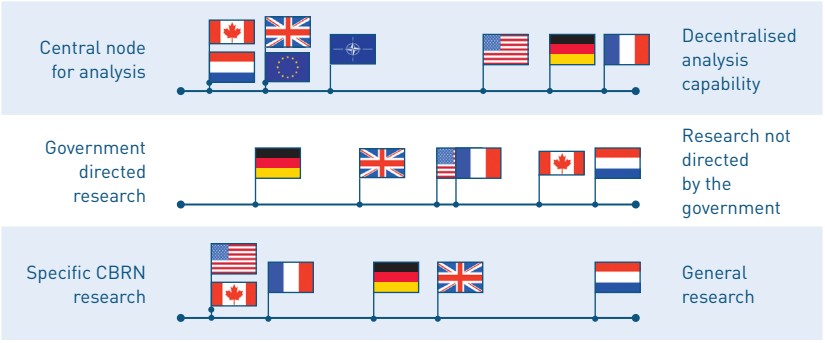


Figure 4. NATIONAL ANALYSIS CAPABILITIES ON THREE DIMENSIONS

CBRN capabilities: prevention

In addition to analysing and anticipating the threat of a CBRN incident, countries also seek to reduce the probability and impact of a CBRN incident in a variety of ways. In the context of prevention, the most important policy measures relate to the implementation of international non-proliferation agreements, the protection of critical national infrastructure (CNI) through the monitoring and auditing of facilities, and the safeguarding of CBRN- materials and CBRN-facilities (e.g. nuclear power reactors or chemical plants, but also biological research centres).

With respect to the support for and implementation of international non-proliferation agreements, the six countries exhibit a great deal of similarity.

All countries are staunch political supporters of the various non-proliferation regimes including the Non-Proliferation Treaty (NPT), Chemical Weapons Convention (CWC), the Biological Weapons Convention (BWC), the Missile Technology Control Regime (MTCR), and the Proliferation Security Initiative (PSI). Regarding the monitoring and auditing of CNI and the safeguarding of CBRN-facilities and materials, the countries have different policies and capabilities in place, which is further explored in the next two sections.

Securing critical national infrastructure

Canada

In Canada, the Department of Public Safety and Emergency Preparedness (PSEP) is responsible for the safety of Canadians, yet private industries are responsible for the safety of their infrastructure. The PSEP supports partnerships with critical infrastructure stakeholders to ensure their protection. The Department produced a National Strategy for Critical Infrastructure and an Action Plan which guide the identification of risks, implementation of protective measures and effective response to disruptions of critical infrastructure.

France

In France, the Act 2004-811 designates French citizens as the primary actors in civil defence. The government, through the General Secretariat of National Defence (SGDN), has responsibilities for planning and contingency response. The Civil Defence and Protection Directorate (DDSC) of the Ministry of Interior is the central national institution for risk management, both for every day accidents and major catastrophes. The sub directorate Risk Assessment assesses risks, including natural, technological, nuclear and marine pollution-related, and defines the framework for relief operations and civil defence measures. In the Vigipirate national contingency plan, the French SGDN is tasked to preserve critical national infrastructure.

Germany

In Germany, the Federal Ministry of Interior (BMI) developed a National Strategy for Critical Infrastructure Protection (CIP). In Germany the Federal Office of Civil Protection and Disaster Assistance of the (BMI) is involved in safety measures. Similar to other countries, the German CIP makes clear that as a result of widespread private ownership of CNI facilities, the responsibility for the security, reliability, and availability of such infrastructure increasingly passes to the private sector or, at least, becomes a shared responsibility.' The government

provides risk assessments analyses and protection concepts. It relies on voluntary commitments to regulations from intensive cooperation but reserves the right to amend and enact new legislation.

The Netherlands

In the Netherlands, the National Advisory Centre on Vital Infrastructure (NAVI) is the agency that advises industries on risk identification and structural safety measures. The NAVI works extensively with the NCTb and with the intelligence services to support the private industries to minimise proliferation and security risks. However, the NAVI has only an advisory role. The actual implementation of measures is left to private industry.

United Kingdom

The UK protects its CNI by extensively cooperating with the Centre for the Protection of National Infrastructure (CPNI). It provides integrated security advice regarding national infrastructure on physical, personnel and electronic security. Despite its mere advisory role, the CPNI, similar to the Dutch NAVI, has special access to restricted information to provide advice and set priorities.

United States

In the US the protection of CNI falls under the jurisdiction of the Department of Homeland Security (DHS). DHS developed a risk assessment tool to decide on the allocation of resources for the protection of its so-called Critical Infrastructure and Key Resources (CIKR). The ambitions of the US efforts, the ways of prioritising certain locations and security measures over others and the responsibilities of the different administrative levels are laid out in the National Infrastructure Protection Plan (NIPP). As the majority of CIKR is in private hands, the NIPP contains arrangements for public-private cooperation. Even though private companies are responsible for the security of their own assets, the plan provides for the exchange of threat assessments and best-practices among governments and companies, for example in fora like the Sector Coordinating Councils (SCCs).

Safety regimes: registration of CBRN materials

Canada

A signatory to all CBRN treaties, Canada has an extensive export control regime, enforced by the Export Controls Bureau of the Ministry of Foreign Affairs and International Trade. Registration of CBRN-related materials takes place within the export controls of military and strategic goods. Domestically, CBRN related materials are monitored and controlled by Public Works and Government Services Canada and any transport of materials is the responsibility of the Department of Transport, Infrastructure and Communities.

France

In France, the Ministry of Economics, Finance and Industry (MEFI) safeguards, controls and audits CBRN materials, supported by the Department of Radioactive Materials Safety (DSMR) and the Institute for Radiation Protection and Nuclear Safety (ISRN). By law, any import, export, production, possession, transfer, use or transport of nuclear materials is subject to prior authorisation by the Senior Nuclear Control Official, acting on the authority of the MEFI. The MEFI is also responsible for controls on chemical and biological materials in accordance with the various treaties (e.g. BWC, CWC).

Germany

In Germany, the Federal Office for Economics and Export Control (BAFA) is the main licensing authority. A license is also required for the domestic handling or transport of controlled goods. Furthermore, the BAFA is responsible for the administrative implementation of export control policies. It cooperates with customs and monitoring agencies to manage a complex export control system. In some cases, the Federal Ministry of Economics and Technology and the Federal Foreign Office are consulted for political advice on granting licenses.

The Netherlands

In the Netherlands the Ministry of Economic Affairs (MEA) and the Ministry of Foreign Affairs (MFA) are responsible for export controls. The MEA is responsible for the actual export controls and the MFA provides political advice. The Dutch customs' Central Unit for Import and Export (CDIU) of the Ministry of Finance is tasked with the administrative implementation and with the provision of information on the implementation of export controls of treaties. The CDIU keeps the mandatory reports of goods at companies in industry and is the main point of contact for businesses.

United Kingdom

In the UK, the Department for Business, Innovation and Skills (BIS) oversees the registration and monitoring of CBRN materials in accordance with the CWC and BWC. The Export Control Organisation (ECO) within the BIS is responsible for legislating, assessing and issuing export licences for specific categories of "controlled" goods. Also, the Office for Civil Nuclear Security (OCNS), as part of the BIS, monitors British nuclear materials. To improve security of legally stored CBRN materials, the government seeks to enhance safeguards of these materials by cooperating extensively with the CPNI, OSCT, National Counter Terrorism Security Office (NCTSO) and the UK BIS.

United States

The US imposes obligations on companies that are involved in the import and export of CBRN materials. The central actor in these efforts, which largely follow from international agreements, is the Bureau for Security and Industry (BSI), a part of the Department of Commerce. The BSI oversees the import and export of CBRN materials, grants export licenses and advises private companies on how to comply with the import and export requirements. The US regulations regarding chemicals go further than solely export controls and constitute an internal verification regime, as they oblige companies to 'submit declarations on production, consumption, processing, imports and exports, and reports on imports and exports to BIS'.

Assessment prevention

Countries have largely similar oversight regimes. Governmental or semi-governmental bodies conduct risk assessments of vulnerable CBRN facilities leaving it up to private actors to act and reduce the identified vulnerabilities. It would go beyond the scope of the present report to evaluate the nature and effectiveness of the respective national oversight regimes. Still, a clear trend exists towards responsibility of the private sector in the execution of preventive policies.

The national CBRN materials registration systems are similar in nature as well. Although the selected countries have registration systems in place (in order to abide by the obligations they assumed under the BWC and the CWC), the strictness of these systems merits further analysis Challenges posed by scientific revolutions (e.g., dual-use) will have significant ramifications for these

registration systems. These challenges will be discussed more in depth in the conclusion.

CBRN capabilities: response

Response capabilities determine the extent to which countries are able and capable to respond to and recover from a CBRN incident. They consist of a wide variety of capabilities, of which the most important are: the presence of an early detection and warning system, a crisis management centre, decontamination and quarantine equipment, stockpiles of vaccines, and restoration plans and capabilities. The next sections explore the national response capabilities of the surveyed countries.

Detection, early warning and public incident alert

Canada

The Canadian detection capability consists of specialised CBRN training and equipment for local first responders. Early warning capabilities are advanced (detection) equipment for laboratories for the provision of timely information sharing of disease incidents, and a Global Public Health Intelligence Network, which is currently being developed. In addition, the Defence R&D Canada (DRDC) agency, part of the Department of National Defence, possesses extensive CB expertise to help assess a CB incident. A nation-wide public incident alert system, CanAlert, which allows the government to deliver public alerts via radio, television, cell phones and the Internet, reaching 99% of the Canadian population, is also being developed.

France

In France, detection of fire, explosives attacks or other incidents is conducted by the Laboratoire Central de la Prefecture de Police (LCPP). For identifying and characterising the most dangerous biological contaminants or chemical substances, France has a system of laboratories with different capabilities that are integrated across the defence zones of the national territory, the network of BIOTOX/PIRATOX laboratories. In early warning, the Lyon Biopole also plays a role in the identification of pathogens. The sub directorate Risk Management of the DDSC informs the population and increases threat and risk awareness by using a national alarm system (including alarms and message vehicles in case of an incident).

Germany

In Germany, the Länder are tasked with detection of CBRN incidents. They have special "ABC-Erkundungskraftwagens" (around 370 in total) for detection on disaster sites, during fires, or at other incidents. They belong to the local emergency services of the Länder but are procured by the Federal Office for Civil Protection and Disaster Management (BBK). For early warning in public health, the Robert Koch Institute (RKI) is the central federal institution responsible for disease control and prevention. It is tasked with medical monitoring, particularly on biological agents, and it maintains an Outbreak Investigation Team that assists and coordinates the work of the Länder. The BBK created a system which warns the population about dangers in times of crises and defence, the Deutschen Notfallvorsorge-Informationssystem (deNis).

The Netherlands

Due to relative modest resources, the Netherlands has a decentralised detection and early warning capability. Besides special governmental CBRN emergency units (i.e., six strategically located CBRN detection and support centres, and the specialised units of the fire service, Hazard Dangerous Substance group (OGS)), the research institutes TNO, NFI, RIVM and the National Laboratory Network provide additional detection and early warning capabilities can be called upon for fast communication in case of an emergency through the NCTb. Through the use of television, radio and internet, the government is able to communicate with the population in an emergency, in addition to the existence of a national acoustic alarm system.

United Kingdom

Emergency services in the UK are trained to initially detect and identify CBRN materials and the Home Office works extensively with the emergency services to continuously improve equipment. In addition, the National Network of Laboratories is a laboratory network dispersed across the UK providing specialist forensic analysis of CB material for the police to provide an early warning capability. The UK government published a leaflet, 'Preparing for Emergencies, What You Need to Know', to inform the public on how to respond during crises. In addition, the government works with the media and has a central news coordination centre to alert the public.

United States

In the US, to make sure that all actors have access to all relevant information about a crisis in an early stage, the US has integrated a number of detection systems into a single point where all detection information is collected. This Integrated Public Alert Warning System (IPAWS), which integrates a number of detection systems, includes information about the spread of CBRN-agents, and allows the authorities, particularly the president, to inform the public about the crisis through various channels, including e-mail and cell phones. The US has the ambition to also include alert systems from private industries in IPAWS. Early warning systems regarding biological agents are integrated in the National Biosurveillance Integration Center (NBIC), which collects all information that could indicate the release of a biological agent. There have been efforts at the integration of detection mechanisms in the military sphere as well. Since early 2003, when the DHS became operational, the US has invested many resources in the creation of a system to adequately respond to CBRN incidents. Project BioShield and the BioWatch Program are examples of measures to detect threats in an early stage and be medically prepared for the consequences.

CBRN crisis centre

Canada

In the event of an actual attack, the Canadian Government Operations Centre coordinates the national response, provinces and territories are responsible for operational and logistical issues, while municipal authorities make the tactical decisions.

France

In France, an interdepartmental crisis centre, Centre Operationnel de Gestion Interministerielle des Crises (COGIC) is part of the Ministry of Interior's Civil Defence and Protection Directorate (DDSC). This centre is activated during crises regardless of the nature of the crisis (including CBRN) and prepares and coordinates the actions of the government. France is subdivided in various defence zones to coordinate between the national and regional levels of government. In case of an emergency, the COGIC cooperates with local emergency actors and defence zone actors.

Germany

The German GMLZ (Joint Information and Situation Centre) foresees in an integrated assistance system in the context of a new strategy of civil protection

in Germany to ensure efficient crisis management with the participation of all establishments and organisations, especially in the event of damage to large areas or events of national importance.

The Netherlands

In the Netherlands, a response to a CBRN incident is either coordinated by the NCTb (terrorist attack) or the Ministry of Internal Affairs (disaster). The National Operational Coordination Centre (LOCC) is the national operational coordinating body of the Ministry. The LOCC coordinates the capabilities required to respond to disasters and CBRN incidents. In addition, the National Crisis Centre (NCC) is a designated unit that also assists in the formulation of a post-CBRN incident response. The NCC is the contact for the regional Landelijk Laboratorium Netwerk - terreur aanslagen (LLN). Relevant actors in an emergency CBRN response, e.g. law enforcement, emergency services, intelligence services receive updates from a central source, the NCTb, which streamlines the national effort.

United Kingdom

In the UK, a crisis committee within the Home Office leads a coordinated response to a terrorist incident and includes a specialised CBRN centre of the police. Furthermore, a government liaison team (GLT) functions as a single point of contact and is headed by a government liaison officer (GLO).

United States

In the US, the coordination of the actors involved in the management of a crisis is the Federal Emergency Management Agency (FEMA). In case of a crisis that requires capabilities beyond those of the individual states, FEMA takes the lead in the federal efforts to respond to and recover from crisis situations. FEMA's mandate encompasses all kinds of crisis situations, and thus includes CBRN incidents. To fulfil this role adequately, FEMA makes inventories of the crisis response capabilities on the state and federal level to identify gaps that need to be plugged and to have full situational awareness in crisis situations regarding the resources that can be deployed.

CBRN protective equipment, decontamination and quarantine

Canada

The Canadian CBRN Strategy trains over 60,000 local first responders with investments being made to acquire new and upgrade old first responder CBRN protective and decontamination equipment. Additionally, the Joint Nuclear,

Biological, Chemical Defence (JNBCD) Company from the Canadian military forces assists in federal decontamination operations. Furthermore, various departments have technical resources readily available, including Environment Canada, Transport Canada, the Canadian Food Inspection Agency, the Canadian Nuclear Safety Commission, and Health Canada. A quarantine response capability relating to public health and welfare is provided by the Department Health Canada (HC) under the Quarantine Act.

France

In France, the civil authorities have SAMU (Emergency Medical Assistance Services) units with specialised CBRN equipment, chemical or radiological intervention cells of the departmental fire and emergency services (SDIS), decontamination processes, national reinforcements from the Civil Security Intervention and Training Units, or UIISC, and hospitals with special capabilities. The Central Inter-Ministerial Technological Intervention Unit can also be mobilised at any time. If necessary, the Ministry of Defence can make available its decontamination, treatment and rehabilitation capabilities for the affected areas.

Germany

In Germany, the Länder civil protection units provide specialised CBRN response units using personal protective equipment. This is conducted in cooperation with the Federal Office for Civil Protection and Disaster Assistance (BBK). In addition, their equipment contains decontamination trucks and CBRN reconnaissance vehicles, so called "ABC-Erkundungskraftwagens". They are assisted by the (voluntary) Federal Agency for Technical Relief (THW) of the Ministry of Interior. THW has established local NBC Rescue Units (SEB-ABC), whose task is to ensure that THW is able to carry out its duties, such as rescuing victims or the evacuation of large areas in a contaminated environment. Furthermore, the Länder, provide hospital access and quarantine capabilities. However, the exact regulations vary per Länder. The BBK coordinates with the Länder on hospital incident planning with the BBK's Centre for Disaster Medicine. This centre concentrates on health issues (e.g., providing protective equipment and public health service).

The Netherlands

In the Netherlands, specialised civilian and military CBRN units have protective CBRN equipment. For example, each region has a small specialised Hazard

Dangerous Substance group (OGS) with special training and small-scale equipment. In addition, there are six strategic CBRN centres that have specialised CBRN personnel. These CBRN centres provide first responders with a decontamination and quarantine capability. When people are quarantined, the Ministry of Public Health, Welfare and Sports is involved. The Central Military Hospital provides additional quarantine units.

United Kingdom

In the UK, ambulance personnel, key health workers and police receive specific CBRN training and special protective equipment (e.g. tailored response suits). Rather than specialised CBRN units, all emergency services are trained for a CBRN response and have special protective equipment. For example, the Police National CBRN Centre trains its law enforcement personnel in responding to CBRN and provides special CBRN suits. In a CBRN event, the Department of Health is the lead actor and coordinates decontamination and quarantine assets. The emergency services, however, first assess the need for decontamination and quarantine.

United States

In the US, the DHS coordinated the investments in CBRN capabilities of first responders throughout the country, enabling them to operate in and decontaminate CBRN environments. In doing so, DHS's approach is clearly one of spreading CBRN expertise over the regular units, rather than concentrating it in a smaller number of specialised units. Decontamination is one of the four major strands of the CBRN Defense Modernization Plan. The goal is to acquire the ability to quickly decontaminate people, equipment and fixed sites.

Stockpiling vaccines

Canada

In Canada, preparation for a large scale CBRN attack is extensive: stockpiles of pharmaceutical and medical supplies exist in warehouses strategically located around the country. Through the National Emergency Services Stockpile System they are replenished and updated. To assist efforts in health protection, a Public Health Agency of Canada and Chief Public Health Officer were established. Through the private pharmaceutical company Glaxo-Smith-Kline (GSK), Canada is able to produce vaccines domestically.

France

In France, the Lyon Biopole aims to gain a comprehensive understanding of human and animal infectious diseases as a specialist of vaccines and viruses. This expertise ranges from diagnostics and prevention to treatment to the development of delivery systems. This 'integrated' approach aims to build a 'healthcare shield' in order to protect populations against these diseases in the fight against bioterrorism. With the capability that Lyon Biopole provides, France is able to indigenously produce vaccines and stockpiles.

Germany

In Germany, so-called "Notfalldepots" (medicinal stockpiles) are organised on a state level but are not specifically targeted towards CBRN incidents. The Federal Office for Civil Protection and Disaster Assistance (BBK) started a pilot project 'Federal stockpiling of pharmaceuticals and medical devices – cooperative resource utilisation and emergency supplies at pilot locations' as part of the New Strategy to Protect the Population. This project is currently being implemented and evaluated. For example, the Paul Ehrlich Institute (PEI) evaluates and approves the annual influenza vaccine on the national level and assesses the requirements and options for manufacturing a vaccine against avian influenza, in close cooperation with the Robert Koch Institute and the Friedrich Loeffler Institute (FLI). Germany also has private vaccine production capabilities through, amongst others, the Bayer concern.

The Netherlands stockpiles vaccines for a variety of diseases. A smallpox vaccine is available for the entire population. For the stockpiled vaccines, contingency plans exist for quick distribution among the population. In addition, the Ministry of Agriculture, Nature and Food Quality also has vaccines for 'terrorist sensitive' cattle. In specific cases, the powers of the Ministry of Public Health, Welfare and Sport are expanded to increase the effectiveness in addressing medical threats. For domestic production, the Dutch Vaccine Institute supplies vaccines for national vaccination programmes.

United Kingdom

In cooperation with the Department of Health, the UK has national medical stockpiles of various vaccines although little information is available on type or quantity. The UK has a framework for stockpiling, distributing and using antiviral medicines in the event of pandemic influenza. The UK Vaccine Industry

Group (UVIG) is an umbrella group that represents the major vaccine companies investing in research, development and manufacturing of vaccines for the UK.

United States

In the US, the Homeland Security Strategy stresses the need to establish appropriate levels of medical stockpiles and systems that can rapidly distribute medical countermeasures to large, at-risk populations. This intention has materialised in the Strategic National Stockpile (SNS), managed by the DHS and the Centers for Disease Control and Prevention (CDCP), which contains medications that can be used for all kinds of disasters, including CBRN incidents, that require more medication than individual states have readily available. The SNS is distributed in such a way that the necessary medication can be flown to all US states in a short period of time.

Recovery

Canada

Canada acknowledges the importance of the restore phase in its CBRN strategy, and provides some more detail in An Emergency Management Framework for Canada. This indicates that Canada is well aware of the long-term impact that crisis situations may have on public health and economic growth.

France

The ORSEC Plan (Organisation des Sécours, Emergency Relief Organisation) is France's all-hazard crisis response plan. The plan distinguishes the mapping of the risks and the operational response as its two separate phases and appears to have no strategic principle suggesting the importance of the various forms of restoration and aftercare.

Germany

Germany's strategic principles regarding crisis management are formulated in the *Strategie für einen modernen Bevölkerungsschutz* [Strategy for modern protection of the people]. This document addresses the common issues that are important during crisis situation themselves, like coordination, equipment and international cooperation. Little attention is paid to the aftermath of the crisis.

The Netherlands

After the initial response to a CBRN incident, the Netherlands has a particular focus on minimising casualties and restoring the normal situation. The NCTb

progress reports indicate some measures that take place in the aftermath of a CBRN incident, but there is no reference to strategic recovery and restore efforts as integral part of a crisis response framework.

United Kingdom

Like Canada, the UK has incorporated business continuity into its crisis manage-ment arrangements. 'Resilience', the ability to recover from crisis situations, is one of the key elements of the British crisis response efforts and applies to more than solely CBRN-incidents. The Civil Contingencies Secretariat (CCS) of the Cabinet Office, in its role as lead agency regarding crisis management, issued a guidance document, Emergency Response and Recovery, to inform lower level governments on how to deal with the aftermath of a crisis.

United States

US crisis response appears to extend beyond business continuity. It aims to address the long-term effects on sites, people and the environment rather than merely getting organisations to function again. The clearest example is DHS' Universal Task List, where recovery is a separate strand of work, following the response phase. The Universal Task List calls for capabilities to treat post-traumatic stress, providing medium-term housing for victims, execute site restoration and restore environmental balance. The National Response Framework also addresses efforts along these lines. The various policy ocu-ments emphasise the importance of the recovery phase, which is aimed at returning people, physical infrastructure and organisations to their pre-incident level of functioning.

Assessment response

The national response capabilities countries vary in several respects. First, detection & early warning systems are organised differently. Whereas some countries deploy decentralised detection units scattered throughout the country, other countries place that capability partly in the hands of the emergency services (UK), or rely on non-governmental detection capabilities, which can be called upon in times of emergency (the Netherlands). Second, different actors are equipped with decontamination & quarantine capabilities. In the UK, Canada and Germany emergency services receive additional CBRN training. In the Netherlands and France, the government has established specialised CBRN units. These different approaches have significant budgetary implications in addition to potential impacts on the effectiveness of the response force.

Third, most countries stockpile some vaccine reserves, albeit in different quantities and for different diseases. In addition, to stockpiling, they have different capabilities with respect to the development of (new) vaccines. Although publicly accessible information on these matters is slim, this is an important marker for the level-of-preparedness in case of a large scale attack or disaster. The response to the Mexican flu and the scramble for the acquisition of Tamil Flu serving as a vivid illustration.

Fourth, some countries have a framework in place in which they address the follow-up phase after the initial crisis response. The Anglo-Saxon countries have a broader perception of crisis response than their peers. The impact of CBRN incidents may well extend far beyond their first-order effects. CBRN agents can, for instance, lead to chronic diseases and can make incident sites uninhabitable for a longer period of time. Restoration plans and capabilities are therefore relevant as they determine the impact duration of a large-scale CBRN incident, the second order effects of which may be significant both in terms of monetary units and human losses.

The different response capabilities are depicted in figure 5.

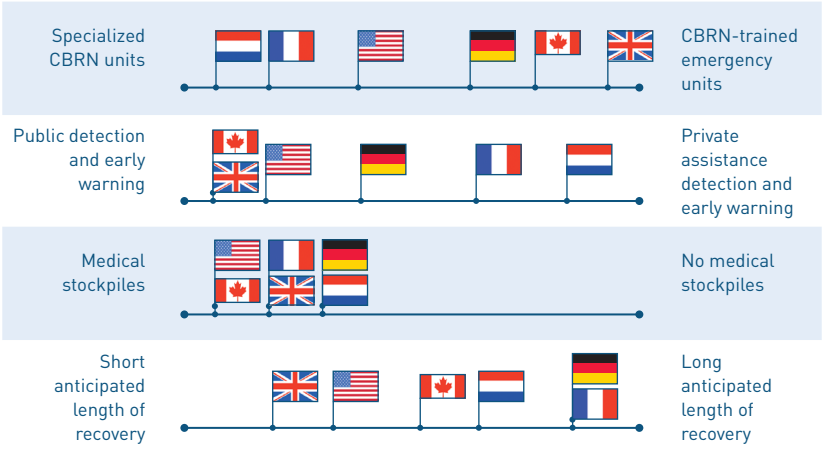


Figure 5. NATIONAL RESPONSE CAPABILITIES ON FOUR DIMENSIONS

5.4 Conclusion

This chapter examined the CBRN-policies and capabilities of the six countries US, UK, France, Germany, the Netherlands and Canada. To this end, key documents and websites describing CBRN policies and capabilities for all countries were analysed. The first section of this chapter described whether and how countries deal with the issue of CBRN incidents and which actors are involved in the formulation and execution of their respective CBRN policies. The second section discussed the actual CBRN capabilities of these countries along the analysis-prevent-response (APR) chain. The findings have been summarised in each section. On the basis of these findings, a number of themes emerge with respect to policies and capabilities along the military – civil dimension, the prevention – response dimension and the single issue vs. comprehensive security dimension. These are further explored below.

The military – civil dimension

CBRN crisis management has shifted from the military to the civilian domain. The surveyed countries have built up significant civilian CBRN capabilities after 9/11. This is in line with the broadening of the threat universe and the fading of boundaries between external and internal threats. The shift has had consequences for military capability development. Although all surveyed countries have explicitly recognised the possibility of using military CBRN units in civilian crisis management, the two spheres are now largely separated. Military CBRN force protection now serves predominantly as a means to improve the sustain-ability of military operations abroad in a wide range of arenas, whereas civilian CBRN crisis management will only use the military as a last resort.

The division of civil-military capabilities needs further consideration in light of the question of duplication of efforts. The same could be argued for the division between security and safety, especially with respect to response and recovery phases. A more efficient allocation and division of capabilities is obscured by the increase of the number of actors, existing under-capacity (see ICMS) and legal issues (e.g. *posse comitatus* in the United States).

The prevention – response dimension

Capabilities can be strategically chosen along the APR chain. No country focuses specifically on CBRN intelligence. In contrast, in terms of research capabilities more dedicated CBRN capabilities exist. In Canada there is a specific CBRN

strategy. In France or the US these capabilities have developed withn a military context.

The capability development in the recovery phase remains relatively underdeveloped in all countries surveyed. For the moment, this limits the possibilities to rely on a unique resilience only approach, which would depend on capabilities in the recovery phase. The question remains whether the relatively marginal position of recovery capabilities is due to under-investments, the relative high investment in analysis and prevention in general, or whether there is not enough understanding about the requirements and needs for recovery after CBRN attacks.

Single issue – comprehensive security dimension

The increased, perceived threat of terrorism has pushed CBRN up the political agenda, especially after 9/11. As a result, both areas have profited from increased budgets. Now, with attention to terrorism waning again, dedicated CBRN budgets are under pressure. In those countries with a significant military role, this change might have milder consequences for the potential of CBRN capability development.

6 Synthesis

6.1 Introduction

The end of the post 9/11 spree in security investments is amplified by tightening government budgets. Governments around the world seek to balance their budgets in the aftermath of the economic crisis. Naturally, this will have implications for the amount of resources allocated to the protection against CBRN threats and hazards. The actual risk posed by CBRN threats will – once more – receive extra scrutiny, as will the ways in which societies receive more value for money in mitigating such risks.

In the preceding chapters, we have reviewed a number of assessments by countries, international organisations and non-governmental entities of the risk posed by CBRN threats and hazards at present, specifically looking at probability, impact and vulnerability. We have also analysed the debate on potential CBRN threats and hazards in the next five to fifteen years, looking at technological and geopolitical aspects of proliferation and the actual use of CBRN materials as weapons. Finally, we have examined the CBRN-policies and capabilities of six countries to examine how countries deal with CBRN incidents and how they formulate and execute their respective CBRN policies along the analysis-prevent-response (APR) chain.

These research endeavours have yielded some significant findings which form the basis for eleven observations presented below. These observations are intended to help policymakers and industry executives navigate the complex CBRN landscape of 2010 and beyond.

The eleven observations are formulated around:

- the scope of risk consideration,
- assessment of risks (including probabilities, impact, and vulnerability), and
- capability requirements.

6.2 Eleven observations

Scope of risk consideration

Observation 1

The worst case-scenario approach, which is prevalent in CBRN assessment conducted by states, neglects attention to smaller or milder CBRN incidents.

- CBRN-incidents are generally though of as high impact and with catastrophic consequences. This is not necessarily justified by empirical evidence, or by logical reasoning. While non-state actors may have the intention, but lack the capability to carry out a CBRN attack due to technological constraints, state actors have the capacity but generally lack the intention to launch a CBRN attack for reasons of political expediency and deterrence.
- This does not mean that the probability of a high impact CBRN incident is zero or should be ignored. However, it draws attention to the narrow scope of CBRN assessments which focus excessively on high impact-low probability incidents, overlooking the possibility of smaller CBRN-incidents.
- The fall-out of smaller CBRN incidents may be considerable. For instance, if a CBRN incident takes place in a port, the port may become inaccessible for a number of days to sea traffic, with perhaps limited loss of human life, but tremendous costs to the economy.

Observation 2

The focus on CBRN as a whole ignores the distinct characteristics of each of the CBRN components.

- The probability of the use of nuclear weapons in the near term against the home territories of Western countries has receded with the end of the Cold War. Nuclear weapons pose a threat to regional stability in the Middle East, South Asia and the Korean peninsula. The devastating effect of nuclear weapons is enormous, but their actual use by both state and non-state actors unlikely.
- The impact of biological weapons may be significant, but the likelihood of their military deployment by state actors limited.
- While state and non-state actors may be able and willing to deploy chemical weapons, these weapons mainly pose a disruptive risk, with effects of a different order of magnitude than BN weapons.

Assessment of risks

Observation 3

While current proliferation prevention mechanisms seem to work, it is questionable whether they can keep up with technological developments and remain future proof.

- The anticipated revolutions in the field of field of chemistry, bio- and nano-technology may affect the types of agents, ease of production and magnitude of effects and may have significant effects for non proliferation efforts in the mid-term.
- Although there is a significant degree of uncertainty as to the timing and nature of developments in a number of scientific fields, the increasing convergence of chemistry and biology Advances in 'manipulating genes, cells, and organisms may result in an unprecedented increase in the number of dual-use materials (both with respect to agents and production and delivery technologies).

Observation 4

Focus on loss of life has dominated the impact discussion at the detriment of other potential damaging impacts, ranging from political and social instability to economic and ecological costs.

- The CBRN discussion has a considerable human fear dimension. This obscures a rationale analysis of potential impact and puts a heavy emphasis on prevention. Given technological developments, the assurance of absolute prevention is a fallacy. While there remain significant obstacles for stable and effective application, the list of potential target areas or groups is unpredictable and substantial.
- As a result, the discussion about impact and impact reduction needs to be developed further. Impact has focused on loss of life. Given the low incidence of CBRN-attacks and the relatively low number of casualties, this fixation does not cover the spectrum of potential impacts sufficiently. Significant economic loss and (related) ecological damage might prove to be more relevant for both major and milder incidents (see also observation 1).

Observation 5

Existing CBRN risk assessment capabilities within and outside governments are generally crude and lack a more calibrated analysis and an integrated understanding of the risk posed by CBRN incidents.

- The divide between the scientific and policy communities is great with few experts able to capture both geopolitical and scientific/technological dimensions of CBRN risks.
- This divide may lead to uninformed assessments. We need to cross this divide, if not at the level of policymakers, then at least among experts advising the policymakers.
- The Dutch Nationale Risicobeoordeling (National Risk Assessment [NRA]) is a significant development to introduce a scientifically sound risk assessment approach in the domain of policymaking. However, it has not yet considered CBRN attacks or incidents (see observation 7).

Observation 6

The current risk assessments approaches primarily focus on the threat and impact components of risk, and less so on vulnerability.

- While threat assessments are generally uninformed, and impact assessments are informed by worst case scenario assumptions (see observation 1), vulnerability tends to receive less attention. Vulnerability is a key component of risk and its role in determining both the impact of CBRN incidents and, if intentional, their probability, is greatly underappreciated.

Observation 7

As with other investments in the field of security, a transparent method to evaluate budget allocation and investment in capabilities, against risk reduction and potential economic gain is lacking.

- In the coming year, the Dutch National Risk Assessment will incorporate the impact and probability of (large scale) nuclear and chemical accidents. This will fill a part of the gaps identified in chapter 3. The assessment will allow for a well substantiated comparison of these types of risks with other types, such as pandemics, terrorism, and loss of energy. However, in this stage of development of the NRA, it will not yet provide sufficient indication as to how best to decrease the risks associated with CBRN-attacks and incidents.
- Security and economic considerations should inform allocation of R&D budgets. Funding an independent R&D CBRN base is costly but may have

substantial economic pay offs. Budgetary cuts may result in a quickly deteriorating CBRN knowledge base which is difficult to (re)build.

Observation 8

Risk reduction efforts do not focus sufficiently on getting more value for money

- When it comes to CBRN capabilities, countries have built up diverse capabilities-portfolios based on limited strategic analysis.
- Capabilities in the recovery/restoration phase generally receive scant attention and even scanter budgetary resources.
- In the light of the fact that small scale CBRN incidents may have significant consequences, this may need reconsideration.

Capability requirements

Observation 9

The CBRN efforts by military and civilian actors are uncoordinated and overlap.

- After the events of /11, a significant build-up of CBRN capabilities took place in the civilian domain, resulting in a duplication of efforts between military and civilian actors in some countries.
- The duplication of civil-military efforts and capabilities merits renewed scrutiny in terms of legal issues (e.g. posse comitatus in the United States), increased civil-military cooperation between military and civil establishments in general (e.g., Intensivering Civiel Militaire Samenwerking (ICMS) in the Netherlands) and the attention for the comprehensive approach in the wider Western world.
- However, military CRBN protection and detection capabilities serve as a force enabler for the armed forces. Possession of these capabilities allows the military to operate in CBRN risk environments and thereby contribute to the broader foreign policy objectives outlined in national security strategies.

Observation 10

Responsibility for CBRN protection is partly shifting from the public to the private sector. But the associated knowledge flow (what to protect against, how to protect, how to respond?) is not always keeping up with this movement.

- Although governments in the reviewed countries continue to play a salient role in CBRN protection, private actors are increasingly expected to make significant contributions to efforts along the analysis-prevention-response chain.

- Public-private partnerships will gain renewed attention to facilitate cooperation between the public and private sector in the protection against CBRN.

Observation 11

National security concerns prevent division of tasks across borders. This hampers a more efficient and effective CBRN policy.

- Strong partnerships with a (limited) set of countries may facilitate national specialisation in a particular subfield, increase returns-on-investment of R&D funding while continuing to guarantee security and safety of populations (e.g., country X specialises in C detection and protection versus country Y in B protection, agreeing to come to each other's aid in case of an emergency).
- Options for multinational capabilities such as outlined in the EU CBRN Action Plan (June 2009) deserve further exploration.
- The extent to which it is possible for countries to retain a reserve capacity – that can be called upon in emergency situations and that allow for a quick build-up of capabilities deserves further examination.

6.3 Conclusion

Policymakers, policy advisers and the population at large should distinguish facts from fiction prompted by fear when debating CBRN. In times of tightening security budgets, the 'one percent doctrine' –prepare for the worst, even if the worst is highly unlikely –may be set aside in favour of a more realistic approach. This approach will prioritise capabilities against C, B, R, or N in the analysis, prevention and response phases. This will (have to) be done against the background of scant data on the intent of actors to actually use CBRN weapons and uncertainty about scientific developments in the field of chemistry, biology and nanotechnology.

References

Ackerman, G. A. (2003), 'Beyond Arson? A Threat Assessment of the Earth Liberation Front.' *Terrorism and Political Violence*, Vol. 15, No. 4.

Ackerman, G. A. and K. S. Moran (2005), 'Bioterrorism and Threat Assessment.' *The Weapons of Mass Destruction Commission Occasional Report* No. 22.

Acton, J. M., M. B. Rogers and P. D. Zimmerman (2007), 'Beyond the Dirty Bomb: Re-thinking Radiological Terror.' *Survival*, Vol. 49, No. 3.

Ainscough, M. J. (2002), *Next Generation Bioweapons: The Technology of Genetic Engineering Applied to Biowarfare and Bioterrorism*. USAF Counterproliferation Center, Future Warfare Series Occasional Paper No. 14.

Algemene Inlichtingen- en Veiligheidsdienst (2007), *Jaarverslag 2006*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Algemene Inlichtingen- en Veiligheidsdienst (2009), *Jaarverslag 2008*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Albright, D., K. O'Neill, and C. Hinderstein (2001), 'Nuclear Terrorism: The Unthinkable Nightmare.' *Institute for Science and International Security (ISIS) Issue Brief*.

Allison, G. (2004), 'Nuclear Terrorism: How Serious a Threat to Russia?' *Russia in Global Affairs online edition*, No. 5.

Allison, G. (2008), 'Nuclear Deterrence in the Age of Nuclear Terrorism.' *Technology Review*, No. 6.

Armée de Terre (2007), *Winning the Battle, Building Peace: Land Forces in Present and Future Conflict*. Centre de Doctrine d'Emploi des Forces.

Biological and Toxin Weapons Convention (1972), *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction.*

Baradei, M. el (2009), *IAEA Implementation of the NPT Safeguards Agreement in the Syrian Arab Republic*. International Atomic Energy Agency.

Barnaby, F. (2001), *Waiting for Terror: How Realistic is the Biological, Chemical and Nuclear Threat?* Oxford Research Group.

Behrens, C., and M. Holt (2005), *Nuclear Power Plants: Vulnerability to Terrorists Attack*. Congressional Research Service, Library of Congress.

Bernstein, Paul, John Caves jr., and J. F. Reichart (2007), 'The Future Nuclear Landscape.' *Centre for the Study of Weapons of Mass Destruction Occasional Paper* No. 5.

Betts, R. K. (2002), 'The Soft Underbelly of American Primacy: Tactical Advantages of Terror.' *Political Science Quarterly*, Vol. 117, No. 1.

Bobbitt, P. (2002), *The Shield of Achilles: War, Peace, and the Course of History*. New York: Alfred A. Knopf.

Bobbitt, P. (2008), *Terror and Consent: The Wars for the Twenty-first Century*. New York: Knopf / Penguin.

Bonin, S. (2007), *International Biodefense Handbook 2007: an Inventory of National and International Practices and Policies*. Zürich: Swiss Federal Institute of Technology.

Brodsky, B.H. (2007), *Industrial Chemicals as Weapons: Chlorine*. James Martin Center for Nonproliferation Studies, Monterey Institute of International Studies. http://www.nti.org/e_research/e3_89.html.

Bundesministerium der Verteitigung (2006), *White Paper 2006: On German Security Policy and the Future of the Bundeswehr.*

Bundesministerium des Innern (2008), *Verfassungsschutzbericht Vorabfassung 2008*.

Bundesministerium des Innern (2009), *National Strategy for Critical Infrastructure Protection*.

Bundesverwaltungsamt (2003), *Zentralstelle für Zivilschutz, Neue Strategie zum Schutz der Bevölkerung in Deutschland*. Akademie für Krisenmanagement, Notfallplanung und Zivilschutz.

Bush, G. W. (2002), *National Strategy for Homeland Security*. Washington, DC: Office of Homeland Security.

Campbell, K. M., R. J. Einhorn, and M. Reiss (2004), *The Nuclear Tipping Point: Why States Reconsider Their Nuclear Choices*. Washington DC: Brookings Institution Press.

Center for Counterproliferation Research (2003), *Toward a National Biodefense Strategy: Challenges and Opportunities*. National Defense University.

Center for Infectious Disease Research & Policy (2009), *History, Likely Agents, Perpetrators, and Dissemination*. University of Minnesota. http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/biofacts/bioterr-overview.html.

Cetron, M. J. and O. Davies (2005), '53 Trends Now Shaping the Future.' *Engineering Management Review, IEEE*, Vol. 33, No. 3.

Chassaing, R. (2008), 'CBRN Protection.' *Doctrine* No. 15.

CIA Office of Transnational Issues (2003), *The Darker Bioweapons Future*. Central Intelligence Agency Directorate of Intelligence.

Cordesman, A. H. (2001), *Radiological Weapons as Means of Attack*. Centre for Strategic & International Studies. http://csis.org/publication/radiological-weapons-means-attack.

Cornish, P. (2007), *The CBRN System: Assessing the Threat of Terrorist Use of Chemical, Biological, Radiological and Nuclear Weapons in the United Kingdom*. London: Royal Institute of International Affairs.

Council of the European Union (2003a), *A Secure Europe in a Better World: European Security Strategy*.

Council of the European Union (2003b), *EU Strategy Against Proliferation of Weapons of Mass Destruction.*

Council of the European Union (2003c), *Fight Against the Proliferation of Weapons of Mass Destruction – EU Strategy Against Proliferation of Weapons of Mass Destruction.*

Council of the European Union (2005), *Second Annual Presidency report (2004) to the Council on the Implementation of the Joint Programme of the Council and the Commission, of 20 December 2002, to Improve Cooperation in the European Union for Preventing and Limiting the Consequences of Chemical, Biological, Radiological or Nuclear Terrorist Threats (2002 CBRN Programme).*

Council of the European Union (2008), *Inventory of EU Instruments Relevant for Addressing Chemical, Biological, Radiological and Nuclear risks ('CBRN Inventory').*

Council of the European Union (2009a), *Annex 1: EU CBRN Action Plan.*

Council of the European Union (2009b), *Council Conclusions on Strengthening Chemical, Biological, Radiological and Nuclear (CBRN) Security in the European Union - an EU CBRN Action Plan.*

Cravens, G. (2002), 'Terrorism and Nuclear Energy: Understanding the Risks.' *The Brookings Review*, Vol. 20, No. 2.

Daly, S., J. Parachini, and W. Rosenau (2005), *Aum Shinrikyo, al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism*. RAND Corporation.

Dando, M. (2002), 'Scientific and Technological Change and the Future of the CWC: the Problem of Non-Lethal Weapons.' *Disarmament Forum*, Vol. 4, No. 4.

Davison, N. (2007a), 'The Contemporary Development of 'Non-Lethal' Weapons.' *Bradford Non-Lethal Weapons Research Project Occasional Paper,* No. 3.

Davison, N. (2007b), "Off the Rocker' and 'On the Floor': The Continued Development of Biochemical Incapacitating Weapons.' *Bradford Science and Technology Report*, No. 8.

Davison, N. (2009), 'Marketing New Chemical Weapons.' *The Bulletin of Atomic Scientists online edition.*

Department of Defense (2006), *Report of the Defense Science Board Task Force on Nuclear Capabilities.*

Department of Defense (2008a), *Final Report of the Defense Science Board Task Force on Nuclear Deterrence Skills.*

Department of Defense (2008b), *National Defense Strategy.*

Department of Defense (2008c), *Sustaining the Competitive Advantage: Chemical Biological Defense Program Strategic Plan.*

Department of Defense (2009), *Chemical and Biological Defense Program, Annual Report to Congress.*

Department of Foreign Affairs and International Trade Canada (2007), *A Guide To Canada's Export Controls.*

Department of Homeland Security (2005a), *State and Urban Area Homeland Security Strategy: Guidance on Aligning Strategies with the National Preparedness Goal.*

Department of Homeland Security (2005b), *Universal Task List Version 2.1.*

Department of Homeland Security (2007a), *National Strategy for Homeland Security.*

Department of Homeland Security (2007b), *Office of Inspector General, DHS' Management of BioWatch Program.*

Department of Homeland Security (2008a), *National Incident Management System*.

Department of Homeland Security (2008b), *National Response Framework*.

Department of Homeland Security (2009a), *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*.

Department of Homeland Security (2009b), *Budget-in-Brief: Fiscal Year 2010*.

Department of National Defence and the Canadian Forces (2005), *Canada First Defence Strategy*.

Department of National Defence and the Canadian Forces (2009a), *Canadian Military Doctrine*.

Department of National Defence and the Canadian Forces (2009b), *Chemical, Biological, Radiological and Nuclear Defence Strategic Doctrine*.

Department of National Defence and the Canadian Forces (2009c), *Chemical, Biological, Radiological and Nuclear Defence Operations*.

Department of National Defence and the Canadian Forces (2009d), *Nuclear, Biological and Chemical (NBCD) Operations*.

Department of Public Safety Canada (2005), *The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada*.

Department of Public Safety Canada (2008), *Working Towards a National Strategy and Action Plan for Critical Infrastructure*.

Dickinson, L. (1999), 'The Military Role in Countering Terrorist Use of Weapons of Mass Destruction.' *Future Warfare Series*, Occasional Paper No. 1.

Dunn, L. A. (2009), 'The NPT.' *Nonproliferation Review*, Vol. 16, No. 2.

European Commission (2009a), *Proposal for a new policy package on chemical, biological, radiological and nuclear (CBRN) security*.

http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/291&type=HTML.

European Commission (2009b), *REACH, What is REACH?* http://ec.europa.eu/environment/chemicals/reach/reach_intro.htm.

Fangmark, I, and L. Norlander (2005), *Indicators of State and Non-State Offensive Chemical and Biological Programmes*. Weapons of Mass Destruction Commission.

Federal Emergency Management Agency (2009a), *FEMA GPD Grant Program Accomplishments Report: Summary of Initial Findings*.

Federal Emergency Management Agency (2009b), *Integrated Public Alert and Warning System (IPAWS)*.

Federation of American Scientists (2009), *Nuclear Suppliers Group*. http://www.fas.org/nuke/control/nsg/index.html

Feinstein, L. and A. M. Slaughter (2004), 'A Duty to Prevent.' *Foreign Affairs* Vol. 83, No. 1.

Ferguson, C. and W. Potter (2005), 'Improvised Nuclear Devices and Nuclear Terrorism.' *Weapons of Mass Destruction Commission Occasional Paper* No. 2.

Ferguson, C., W. Potter, A. Sands, L. Spector and F. Wehling (2005), *The Four Faces of Nuclear Terrorism*. New York: Routledge.

Fitzpatrick, M. ed. (2007), *Nuclear Black Markets: Pakistan, AQ Khan and the Rise of Proliferation Networks: A Net Assessment*. International Institute for Strategic Studies.

Government of Canada (2004), *Securing an Open Society: Canada's National Security Policy*.

Government of Canada (2005a), *CanAlert*.

Government of Canada (2005b), *Securing an Open Society, Canada's National Security Policy: One Year Later. Progress Report on the Implementation of Canada's National Security Strategy*.

Graham, B., J. Talent et al. (2008), *World at risk: the report of the Commission on the Prevention of WMD Proliferation and Terrorism*. New York: Vintage, 2008.

Gregory, Shaun. (2009). 'The Terrorist Threat to Pakistan's Nuclear Weapons.' *CTC Sentinel*, Vol. 2, No. 7.

Hemel, C. van and J. Polo (2007), *Frankrijk: Europese speler in veiligheidstechnologie*. TWA Netwerk. http://www.twanetwerk.nl/default.ashx?DocumentId=8029.

Heptonstall, J. and N. Gent (2008), *CBRN Incidents: Clinical Management and Health Protection (Revised)*. London: Health Protection Agency.

Her Majesty's Government (2008), *The National Security Strategy of the United Kingdom: Security in an Interdependent World.*

Her Majesty's Government (2009), *UK, Pursue, Prevent, Protect, Prepare: UK's strategy for countering international terrorism.*

Hincal, F. and P. Erkekoglu (2006), 'Toxic Industrial Chemicals (TICs) – Chemical Warfare Without Chemical Weapons.' *Fabad Journal of Pharmaceutical Sciences*, Vol. 31, No. 4.

Hirsch, H. (2001), *Danger to German nuclear power plants from crashes by passenger aircraft*. World Information Service on Energy. http://www10.antenna.nl/wise/index.html?http://www10.antenna.nl/wise/terrorism/112001gre.html.

Hoffman, B. (2007), 'CBRN Terrorism Post-9/11,' in Howard, R. and J. Forest, *Weapons of Mass Destruction and Terrorism*. New York: McGraw-Hill.

Hughes, L. (2007), 'Why Japan Will Not Go Nuclear (Yet): International and Domestic Constraints on the Nuclearization of Japan.' *International Security*, Vol. 31, No. 4.

Institute for Science and International Security (2009), *Burma Tunnels: ISIS Imagery Brief*.

International Atomic Energy Agency (1970), *The Nuclear Non-Proliferation Treaty*. http://www.iaea.org/Publications/Documents/Infcircs/Others/infcirc140.pdf.

International Atomic Energy Agency (2007), *IAEA Illicit Trafficking Database (ITDB) Fact Sheet*. http://www.iaea.org/NewsCenter/Features/RadSources/PDF/fact_figures2007.pdf.

Ivanova, K. and T. Sandler (2006), 'CBRN Incidents: Political Regimes, Perpetrators, and Targets.' *Terrorism and Political Violence*, Vol. 18, No. 3.

Ivanova, K. and T. Sandler (2007), 'CBRN Attack Perpetrators: An Empirical Study.' *Foreign Policy Analysis*, Vol. 3, No. 4.

James Martin Center for Nonproliferation Studies (2002), *Chemical and Biological Weapons: Possession and Programs Past and Present*. Monterey Institute of International Studies. http://cns.miis.edu/cbw/possess.htm

Jenkins, B. M. (1975), *Will Terrorists Go Nuclear?* California Seminar on Arms Control and Foreign Policy.

Johnston, Robert (2005), *Dirty Bombs and Other Radiological Weapons*. http://www.johnstonsarchive.net/nuclear/dirtybomb.html.

Joint Chiefs of Staff (2006), *National Military Strategy to Combat Weapons of Mass Destruction*.

Joint Requirements Office for Chemical, Biological, Radiological and Nuclear (CBRN) Defense (2008), *2008 CBRN Defense Modernization Plan*.

Joint Working Group of the American Physical Society and the American Association for the Advancement of Science (2008), *Nuclear Forensics: Role, State of the Art and Program Needs*.

Kelle, A. (2007), 'Science, Technology and the CBW Control Regimes.' *Atti Dei Convegni Lincei – Accademia Nazionale Dei Lincei*, Vol. 230.

Keohane, Daniel (2005), *The EU and Counter-Terrorism*. Centre for European Reform.

Kerr, P. K. (2008), *Nuclear, Biological, and Chemical Weapons and Missiles: Status and Trends*. Congressional Research Service, Library of Congress.

Langewiesche, W. (2006), 'How To Get a Nuclear Bomb.' *The Atlantic*, No. 10.

Laqueur, W (1999), *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. London: Oxford University Press.

Lee, R. (2005), *The Dark Side of the Nuclear Smuggling Business*. Testimony submitted to the Subcommittee on Prevention of Nuclear and Biological Attack, House Committee on Homeland Security, 2005.

Lieberman, J. (2009), *S. 1649: To Prevent the Proliferation of Weapons of Mass Destruction, to Prepare for Attacks Using Weapons of Mass Destruction, and for Other Purposes*. Senate of the United States. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s1649is.txt.pdf

Lindstrom, G. (2004), *Protecting the European Homeland*. Paris: European Union Institute for Security Studies.

Luijff, H., H. Burger and M. Klaver (2003), *Bescherming Vitale Infrastructuur: Quick-scan naar Vitale Producten en Diensten*. TNO Fysisch en Elektronisch Laboratorium.

Masse, T., S. O'Neil and J. Rollins (2007), *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*. Congressional Research Service, Library of Congress.

Matoušek, J. (2007), *Impact of Advances in Science and Technology on the Chemical Weapons Convention: Threats and Benefits*. EU Research Centre of Excellence for Environmental Chemistry & Ecotoxicology.

Medalia, Jonathan (2004), *Nuclear Weapon Initiatives: Low-Yield R&D, Advanced Concepts, Earth Penetrators, Test Readiness*. Congressional Research Service, Library of Congress.

Ministère de l'Intérieur (2004), *Organisation de la Réponse de Sécurité Civile: pour la Protection Générale des Populations.*

Ministère des Affaires Étrangères et Européennes (2008), *Infosynthese: Civil Defence in France.*

Ministerie van Binnenlandse Zaken (2007), *Strategie Nationale Veiligheid.*

Ministerie van Defensie (2005), *Nederland Defensie Doctrine.*

Ministerie van Defensie en Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2005), *Spionage en Veiligheidsrisico's.*

Ministry of Defence (2003), *Delivering Security in a Changing World: Defence White Paper.*

Ministry of Defence (2004), *Delivering Security in a Changing World: Future Capabilities.*

Ministry of Defence (2008), *The British Defence Doctrine.* Joint Doctrine Publication.

Morland, H. (1999), *The Holocaust Bomb: A Question of Time.* http://www.fas.org/sgp/eprint/morland.html

Nationaal Coördinator Terrorismebestrijding (2005), *CBRN Terrorismebestrijding/Rampenbestrijding: Voortgangsrapportage 2005.*

Nationaal Coördinator Terrorismebestrijding (2006), *Europees Programma Bescherming Vitale Infrastructuur.*

National Consortium for the Study of Terrorism and Responses to Terrorism (2009), *Global Terrorism Database.* University of Maryland. http://www.start.umd.edu/gtd/

NATO (2003), *NATO's Multinational Chemical Biological Radiological Nuclear Defence Battalion: Fact Sheet.* Supreme Headquarters Allied Powers Europe Public Information Office.

Nationaal Coördinator Terrorismebestrijding (2005), *CBRN Terrorismebestrijding/ Rampenbestrijding: Voortgangsrapportage 2005*.

Nationaal Coördinator Terrorismebestrijding (2006), *Europees Programma Bescherming Vitale Infrastructuur.*

National Consortium for the Study of Terrorism and Responses to Terrorism (2009), *Global Terrorism Database*. University of Maryland. http://www.start.umd.edu/gtd/

NATO (2003), *NATO's Multinational Chemical Biological Radiological Nuclear Defence Battalion: Fact Sheet*. Supreme Headquarters Allied Powers Europe Public Information Office.

NATO (2008), *Reducing Global Nuclear Threats: Contribution of Official Nuclear Weapon States*. NATO Parliamentary Assembly Committee Report.

NATO (2009), *NATO's Comprehensive, Strategic-Level Policy for Preventing the Proliferation of Weapons of Mass Destruction (WMD) and Defending against Chemical, Radiological, Radiological and Nuclear (CBRN) Threats*. http://www.nato.int/cps/en/natolive/official_texts_57218.htm.

NATO Review (2001), 'Interview: Ted Whiteside, Head of NATO's WMD Centre.' *NATO Review*, Vol. 49, No. 4.

Nixdorff, K., Davison, N., Millett, P. and Whitby, S. (2004), 'Technology and Biological Weapons: Future Threats.' *University of Bradford Science and Technology Papers*, No. 2.

Organization for the Prohibition of Chemical Weapons (2009), *The Chemical Weapons Ban Facts and Figures*. http://www.opcw.org/factsandfigures/index.html#CWDestructionUnderWay.

Parachini, J. (2003), 'Putting WMD Terrorism into Perspective.' *The Washington Quarterly*, Vol. 26, No. 4.

Pluta, A. M., and P. D. Zimmerman (2006), 'Nuclear Terrorism: A Disheartening Dissent.' *Survival*, Vol. 48, No. 2.

Présidence de la République (2008), *The French White Paper on Defence and National Security*.

Purkitt, Helen E. (2005), *'Biowarfare Lessons, Emerging Biosecurity Issues, and Ways to Monitor Dual-Use Biotechnology Trends in the Future.'* USAF Institute for National Security Studies Occasional Paper No. 61.

Republik Österreich Bundesministerium für Inneres (2008), *Der Verfassungsschutzbericht 2008*.

Rossin, D. (2005), *Nuclear Facilities and Terrorism*. International Nuclear Energy Academy Executive Statement.
http://www.euronuclear.org/reflections/nuclear-facilities.htm.

Sagan, S. D. (1996), 'Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb.' *International Security*, Vol. 21, No. 3.

Salama, S. and L. Hansell (2005), 'Does Intent Equal Capability?' *Nonproliferation Review*, Vol. 12, No. 3.

Schneider, B. R. (2004), 'Asymmetrical Rivals: The Enemy Next Time,' in B.R.

Schneider and J. Davis, eds., *The War Next Time: Countering Rogue States and Terrorists Armed with Chemical and Biological Weapons*. Maxwell, Alabama: USAF Counterproliferation Center.

Shea, D. (2007), *Oversight of Dual-Use Biological Research: The National Science Advisory Board for Biosecurity*. Congressional Research Service Report for Congress.

Shultz, R. H. and A. Vogt (2002), 'The Real Intelligence Failure on 9/11 and the Case for a Doctrine of Striking First,' in R. Howard and R. Sawyer, *Terrorism and Counterterrorism: Understanding the New Security Environment, Readings and Interpretations*. New York: McGraw-Hill.

Sweijs, T. and N. Chehin (2007), *The CWC: Past Achievements and Future Challenges*. Organisation for the Prohibition of Chemical Weapons Academic Forum.
http://www.opcwacademicforum.org/page/355.

Tenet, G. (2004), *The Worldwide Threat 2004: Challenges in a Changing Global Context*. United States Senate Select Committee on Intelligence.

The Hague Centre for Strategic Studies (2009), *Idiocracy and the Changing Distribution of Knowledge*. Den Haag: The Hague Centre for Strategic Studies.

Thomas, W. (2005), 'NATO Develops NBC Defense Capability.' A*rmy Chemical Review*, No. 1

Tulliu, S. and T. Schmalberger (2004), *Coming to Terms with Security: A Lexicon for Arms Control, Disarmament and Confidence-Building*. Geneva: United Nations Institute for Disarmament Research.

United Nations Special Committee (1995), *Tenth Report of the Executive Chairman of the Special Commission Established by the Secretary-General Pursuant to Paragraph 9 (b) (i) of Security Council Resolution 687 (1991), and Paragraph 3 of Resolution 699 (1991) on the Activities of the Special Commission.*

United States Government (2002), *National Strategy for Combating Weapons of Mass Destruction.*

United States Government (2006a), *The National Security Strategy of the United States of America.*

United States Government (2006b), *National Strategy for Combating Terrorism.*

United States Government (2008), *Defending Against Weapons of Mass Destruction Terrorism. Commission Report Endorses Administration Initiatives and Calls for Continuation of Successful WMD Policies to Address Increasing Threat: Fact Sheet.*

Villepin, Dominique de (2006), *Prevailing Against Terrorism: White Paper on Domestic Security Against Terrorism*.' Paris: La Documentation Française.

Waltz, K. (1981), 'The Spread of Nuclear Weapons: More May Be Better.' *Adelphi Papers*, No. 171. London: International Institute for Strategic Studies.

Wheelis, M. (2000), *Agricultural Biowarfare and Bioterrorism.* Federation of American Scientists Chemical and Biological Arms Control Program. http://www.fas.org/bwc/agr/main.htm

Wheelis, M. and M. Dando (2003), 'New Technology and Future Developments in Biological Warfare.' *Military Technology*, Vol. 27, No. 5.

Wijk, R. de (2006), *Doelwit Europa: Complotten en Aanslagen van Moslimextremisten.* Amsterdam: Mets en Schilt.

Zimmerman, P. D., and C. Loeb (2004), '"Dirty Bombs": The Threat Revisited.' *The Back Page* Vol. 13, No. 3.

Consulted Websites

Department of Foreign Affairs and International Trade Canada
http://www.dfait-maeci.gc.ca/

Department of Health Canada http://www.hc-sc.gc.ca/index-eng.php.

National Defence and the Canadian Forces, www.forces.gc.ca.

Department of Transport, Infrastructure and Communities
http://www.tc.gc.ca/.

Agence National de la Recherche
http://www.agence-nationale-recherche.fr/IPSUK.

Areva, www.areva.com.

Armée de terre http://www.defense.gouv.fr/terre.

Biopole
http://www.lyonbiopole.com/presentation-of-the-cluster/summary-58-2.html.

Ministère des Affaires étrangères et européennes
http://www.diplomatie.gouv.fr/en/.

Ministère de la Défense, http://www.defense.gouv.fr/defense.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, http://www.bbk.bund.de/nn_402322/EN/oo__Home/homepage__node.html__nnn=true.

German Bundeswehr, www.bundeswehr.de.

Website of the German Federal Office of Economics and Export Control
http://www.bafa.de.

Website of the German Federal Ministry of Economics and Technology
http://www.bmwi.de/English/Navigation/root.html

Website of the German Federal Foreign Office
http://www.auswaertiges-amt.de/diplo/en/Startseite.html

Ministerie van Buitenlandse Zaken www.minbuza.nl.

Ministerie van Defensie www.mindef.nl.

Ministerie van Justitie www.justitie.nl.

Nationaal Coördinator Terrorismebestrijding www.nctb.nl.

UK Army (CBRN) http://www.army.mod.uk/equipment/defence/default.aspx

British Energy http://www.british-energy.com/pagetemplate.php?pid=134.

Cabinet Office, UK Resilience http://www.cabinetoffice.gov.uk/ukresilience.aspx.

UK Department of Health http://www.dh.gov.uk/.

UK Health and Safety Executive http://www.hse.gov.uk/nuclear/ocns/.

UK Home Office http://security.homeoffice.gov.uk.

MI5 www.mi5.gov.uk.

Royal Air Force, (JCBRN) http://www.raf.mod.uk/rafhonington/aboutus/jt_cbrn_regt.cfm.

JCBRN Defence COE http://jcbrncoe.cz/joomla/index.php?option=com_content&view=frontpage&Itemid=63

NATO www.nato.int

Public Register of Council Documents http://register.consilium.europa.eu

European Centre for Disease Prevention and Control http://ecdc.europa.eu/

Federation of American Scientists www.fas.org

On the authors

Erik Frinking

Erik Frinking is Programme Director National Security and Intelligence at HCSS. He holds a Masters degree in political science from the University of Leiden. His responsibilities and activities at HCSS focus on identifying and analyzing policy options, evaluating policy outcomes, and developing strategies pertaining to issues of national and international security and intelligence. He currently leads the HCSS activities for the Project National Security, supporting the roll out of the National Security Strategy which was accepted by the Dutch Cabinet in April 2007. In addition, he is responsible for the State of the Future product of the Security Foresight. He was an active member of the Working Group foresight and scenarios of ESRIF.

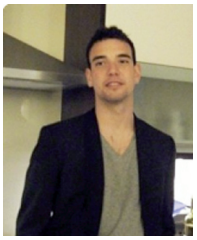
He worked at TNO Defense, Security and Safety between March 2006 and December 2007. His work here covered man security issues primarily in the field of homeland security and security research. Among others, he supported the TNO contributions to ESRAB. Before that, Frinking worked at RAND Corporation for more than 13 years, residing in the European offices in Leiden. Here, he was director of the Education, Science &Technology, and Innovation program.

Tim Sweijs

Tim Sweijs is a policy analyst with the Security Studies Programme. Prior to coming to HCSS he served as a research assistant at NATO's Parliamentary Assembly. He received degrees in War Studies (MA, King's College), International Relations (MSc, University of Amsterdam) and Philosophy (BA, University of Amsterdam). He has been involved in a variety of projects; the current focus of his work is on geopolitical risk assessment and security foresight. Tim also teaches at the political science department of the University of Amsterdam.

Teun van Dongen

Teun van Dongen holds a Master's degree in history and in international relations, both with a strong interest in ideologically inspired political movements in the 20th and 21st century. Before working at HCSS, he worked for the Dutch Permanent Representation at NATO. His PhD research focuses on terrorism and counterterrorism. He is interested in the effectiveness of counterterrorism policies.



Aksel Ethembabaoglu

Aksel Ethembabaoglu is a policy-analyst at HCSS. Aksel worked as an intern at the Dutch Ministry of Foreign Affairs where he wrote his thesis as part of his MA Science and Security at King's College in London. He previously worked as a policy analyst at the Hudson Institute. Prior to his MA, Aksel worked in Cairo as an international facilitator and as a researcher at the University of Amsterdam. Aksel holds a BSc. in Artificial Intelligence from the University of Amsterdam.

In times of tightening security budgets, the way in which countries prepare for Chemical, Biological, Radiological and Nuclear (CBRN) incidents, deserves renewed scrutiny.

The 'one percent doctrine' – prepare for the worst, even if the worst is highly unlikely – which is the current paradigm, must be replaced by a more realistic approach. This involves the prioritisation of capabilities against C, B, R, or N in the analysis, prevention and response phases. This will have to be done against the background of limited availability of data on the intentions and capabilities of actors to actually use CBRN weapons and uncertainty about scientific developments in the field of chemistry, biology and nanotechnology.

This report analyses the nature and size of present and future CBRN-threats. It compares policy approaches towards CBRN threats in six countries (Canada, France, Germany, the Netherlands, the United Kingdom and the United States), as well as two international organisations (NATO and the EU).

The Hague Centre
for Strategic Studies

Lange Voorhout 16
2514 EE The Hague
The Netherlands

info@hcss.nl
www.hcss.nl