Maurizio Martellini
Ralf Trapp *Editors*

21st Century Prometheus

Managing CBRN Safety and Security Affected by Cutting-Edge Technologies

Springer

21st Century Prometheus

Maurizio Martellini • Ralf Trapp
Editors

21st Century Prometheus

Managing CBRN Safety and Security Affected by Cutting-Edge Technologies

Springer

Editors
Maurizio Martellini
Università degli Studi dell'Insubria
Como, Italy

Ralf Trapp
Independent Disarmament Consultant
Chessanaz, France

ISBN 978-3-030-28284-4 ISBN 978-3-030-28285-1 (eBook)
https://doi.org/10.1007/978-3-030-28285-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Part II Evolving Risk Mitigation Strategies and Technologies

Acronyms and Abbreviations

ABEO	Advisory Board on Education and Outreach of the OPCW
AChE	Acetylcholinesterase
AI	Artificial Intelligence
AM	Additive Manufacturing (also "3D Printing")
AMDIS	Automated Mass Spectral Deconvolution and Identification System
APS	Action Protection System
ASAT	Antisatellite (missile, system, etc.)
ATR	Automatic/Automated Target Recognition
AUV	Autonomous Underwater Vehicle
AWS	Autonomous Weapon Systems
BRAIN	Brain Research through Advancing Innovative Neurotechnologies (initiative of the US National Institutes of Health (NIH))
BuChE/HuBChE	Butyrylcholine Esterase/Human Butyrylcholine Esterase
BWC, BTWC	Biological Weapons Convention (also Biological and Toxin Weapons Convention)
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CANDU	Canada Deuterium Uranium pressurized (a Canadian pressurized heavy-water reactor design)
CAS	Chemical Attribution Signature
CBRNe	Chemical, Biological, Radiological, Nuclear and Explosive (weapons, material, technologies)
CCW	Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons
CGC	Cyber Grand Challenge (a cybersecurity competition hosted by DARPA)
CIWS	Close-In Weapon System
CNS	Central Nervous System

CoE	Centres of Excellence (CoE Initiative: CoE initiative of the EU to strengthen CBRN risk mitigation capacities in EU partner countries)
COTS	Commercial Off-The-Shelf (in the context of unmanned aerial vehicles – UAV)
CRISPR-Cas	Clustered Regularly Interspaced Short Palindromic Repeats (These are DNA sequences found in the genomes of prokaryotic organisms such as bacteria; they are derived from DNA related to previous viral infections and form part of the prokaryote's immune defence. The Cas proteins (CRISPR-associated proteins) are enzymes that use the CRISPR sequence to recognise and cleave specific DNA strands. CRISPR-Cas systems are being used as efficient genome editing tools – one of the first systems used to this end was CRSIPR-Cas9.)
CRS	Cyber Reasoning System
CTA	Chemical Threat Agent
CTITF	Counterterrorism Implementation Task Force (of the United Nations)
CWA	Chemical Warfare Agent
CWC	Chemical Weapons Convention
Daesh	See ISIS
DARPA	Defense Advanced Research Projects Agency (a US DOD agency)
DNA	Deoxyribonucleic acid
DOD	Department of Defense (of the USA)
ELF	Extremely Low Frequency (in communications)
EMP	Electromagnetic Pulse
EU	European Union
FAO	Food and Agriculture Organisation of the United Nations
FBI	Federal Bureau of Investigation
FFM	Fact-Finding Mission
GA	Tabun (nerve agent)
GB	Sarin (nerve agent)
GC	Gas Chromatography
GC-MS	Gas Chromatography Coupled with Mass Spectrometry
GD	Soman (nerve agent)
GF	Cyclosarin (nerve agent)
GGE	Group of Governmental Experts
GNEP	Global Nuclear Energy Partnership
GoG	Group of Governmental Experts
GPS	Global Positioning System
HBP	Human Brain Project
HCA	Hierarchical Cluster Analysis
HCM	Hypersonic Cruise Missile
HEU	Highly Enriched Uranium
HGV	Hypersonic Boost-Glide Vehicle

IADM	Improvised Air-Delivered Munition(s)
IAEA	International Atomic Energy Agency
ICA	Incapacitating Chemical Agent (also CNS-acting chemical) – a chemical agent that targets the CNS to cause "selective malfunctions of the human machine" (such as impairments of vision, cognition, state of alertness, etc.)
ICBM	Intercontinental Ballistic Missile
ICT	Information and Communications Technology
IDLH	Immediately Dangerous to Life or Health
IED	Improvised Explosive Device(s)
IEEE	Institute of Electrical and Electronics Engineers
IFNEC	International Framework for Nuclear Energy Cooperation
IHL	International Humanitarian Law
IIT	Investigation and Identification team (of the OPCW, established pursuant to the decision of the fourth Special Session of the Conference of the States Parties of the CWC to investigate and gather information to identify the individuals or parties responsible for CW uses in Syria; the decision also authorizes the OPCW to support national investigations of responsibility for CW uses)
IMS	Ion Mobility Spectrometry
IR	Infrared (Spectroscopy)
ISD	Instructional Systems Design
ISIS, ISIL, IS	Islamic State, also referred to as the Islamic State of Iraq and the Levant (ISIL), the Islamic State of Iraq and Syria (ISIS), Daesh in Arabic
ISTAR	Intelligence, Surveillance, Target Acquisition, and Reconnaissance
ISU	Implementation Support Unit (of the Biological Weapons Convention, part of the UNODA)
JCPOA	Joint Comprehensive Plan of Action (also known as Iran nuclear deal) between Iran, the P5 + 1 (the five permanent members of the UNSC – China, France, Russia, UK and the USA – plus Germany) and the European Union
JIM	Joint Investigative Mechanism (of the OPCW and the United Nations, established by the UNSC to identify those responsible for cases of CW use confirmed by the OPCW FFM in Syria)
LAWS	Lethal Autonomous Weapon System
LC	Liquid Chromatography
LCt_{50}	Median Lethal Dose by Inhalation – the dose (expressed as air concentration multiplied by exposure time) of a toxic, pathogenic or radioactive agent required to kill 50% of a test population after a specified time after acute exposure
LD_{50}	Median Lethal Dose – the dose of a toxic, pathogenic or radioactive agent required to kill 50% of a test population after a specified time after acute exposure

LEO	Low Earth Orbit
LEU	Low-Enriched Uranium
LRASM	Long Range Anti-ship Missile
LWR	Light-Water Reactor
MaRV	Manoeuvring Re-entry Vehicle
ML	Machine Learning
MS, MS/MS	Mass Spectrometry/Tandem Mass Spectrometry
MSP	(annual) Meeting of the States Party to the BWC
MTA	Material Threat Assessment
MX	Meeting of Experts (of the States party to the BWC)
NAS	National Academy of Sciences
NATO	North Atlantic Treaty Organization
NGS	Next-Generation Sequencing
NMR	Nuclear Magnetic Resonance (spectrometry)
NPT	Nuclear Non-proliferation Treaty
NSG	Nuclear Suppliers Group
NTI	Nuclear Threat Initiative
OCAD	OPCW Central Analytical Database – the OPCW's reference library of analytical data (mostly GC-MS, IR and NMR data of CWC-relevant chemicals)
OIE	World Organisation for Animal Health (its original name was Office International des Épizooties, still reflected in the organisation's abbreviation)
OODA	Observe Orient Decide Act
OPCW	Organisation for the Prohibition of Chemical Weapons
PCA	Principal Component Analysis
PCR	Polymerase Chain Reaction (a method to generate copies of specific DNA segments)
PPE	Personal Protective Equipment
R&D	Research and Development
RCA	Riot Control Agent
RCS	Reaction Control System (a spacecraft system using thrusters to provide attitude control and sometimes translation)
RDD	Radiological Dispersion Device
RNA	Ribonucleic Acid
RRI	Responsible Research and Innovation (a concept of the EU used in its framework programmes to take into account effects and potential impacts on the environment and society)
RV	Re-entry Vehicle
S&T	Science and Technology
SAB	Scientific Advisory Board (a statutory organ of the OPCW)
SAP	Source Attribution Profile
SLBM	Submarine Launched Ballistic Missile
SOP	Standard Operating Procedure
TIC	Toxic Industrial Chemical

TOF-MS	Time-of-Flight Mass Spectrometer
TRA	Terrorism Risk Assessment
TWG	Temporary Working Group (of the OPCW SAB)
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UCLASS	Unmanned Carrier-Launched Airborne Surveillance and Strike
UGS	Unmanned Ground System
UGV	Unmanned Ground Vehicle
UN	United Nations
UNITAR	United Nations Institute for Training and Research
UNOCHA	United Nations Office for the Coordination of Humanitarian Affairs
UNODA	United Nations Office of Disarmament Affairs
UNODC	United Nations Office on Drugs and Crimes
UNOSAT	UNITAR's Operational Satellite Applications Programme; it delivers imagery analysis and satellite solutions to relief and development organisations within and outside the UN system
UNSC	United Nations Security Council
UNSGM	United Nations Secretary-General's Mechanism (to investigate reports of alleged uses of chemical, biological or toxin weapons)
UUV	Unmanned Underwater Vehicle
WHO	World Health Organization
WMD	Weapons of Mass Destruction

Introduction

Maurizio Martellini and Ralf Trapp

This book deals with the changing landscape of risks posed by chemical, biological, radiological, nuclear and explosive (CBRNe) materials and technologies. It looks, in particular, at how advances in science and technology are changing and reshaping this risk landscape. These risks range from natural events such as major disease outbreaks to industrial, transportation and other accidents leading to the release of CBRNe materials, and to their use for hostile purposes as weapons of terror or war.

At the same time, the book looks at new opportunities that these scientific and technological advances are expected to bring about for mitigating these risks, and it looks more generally at governance strategies for the twenty-first century to manage the evolving CBRNe risk landscape.

Chemical, biological, radiological, and nuclear weapons and materials remain among the most recognised security threats of today. Associated with explosive materials and devices (including improvised ones) that are used for their employment, the threat spectrum associated with these materials and technologies is often set within a broader CBRNe framework.

This CBRNe threat spectrum is typically associated with certain types of materials ("agents") – toxic chemicals and their precursors, pathogenic agents, radiological materials, nuclear isotopes suitable for the construction of nuclear devices, and explosives. However, their threat level is not merely associated with the properties of the materials themselves, but it also critically depends on their means of delivery/employment and the context and mode within which they are used. Furthermore, their acquisition requires technologies and equipment for their manufacturing or extraction from natural sources. A discussion of CBRNe threats therefore cannot be

M. Martellini (✉)
Università degli Studi dell'Insubria, Como, Italy
e-mail: maurizio.martellini@fondazionealessandrovolta.it

R. Trapp
Independent Disarmament Consultant, Chessenaz, France

M. Martellini, R. Trapp (eds.), *21st Century Prometheus*,
https://doi.org/10.1007/978-3-030-28285-1_1

limited to the agents of concern but must also include the technologies associated with their manufacturing, weaponisation and employment.

On the other hand, the threats associated with these weapons and materials will be moderated by the effectiveness of protections against their effects, as well was the degree to which such protection can be provided to troops as well as populations. In addition, science and technology can augment other capabilities that affect the threat landscape, such as the ability to detect and identify agents after release, technical means of verifying regulatory and treaty compliance, medical and other countermeasures to mitigate their effects, forensic methods to help identifying those responsible for any deliberate release/use of such material and weapons, means of recovery from their effects, and technologies and methods used to shape the information environment within which such weapons and agents are being acquired and deployed.

CBRNe threats and their mitigation can be addressed from a number of different perspectives:

- The actors associated with the development, acquisition and use of such weapons and materials (States, terrorist groups, criminal organisations, individuals), and their capabilities and intents
- The types of materials of concern (toxic chemicals including traditional chemical warfare agents and toxic industrial chemicals, natural toxins and other biomolecule, explosives, propellants, precursors of such chemicals, microorganisms, radionuclides)
- Their origin (naturally occurring such as in natural disease outbreaks, synthetic materials or synthetically modified natural materials)
- The level of sophistication, technological maturity and financial power needed to acquire and deploy them in relevant amounts and qualities
- The level of sophistication needed to use them to achieve a desired effect (effects can range from mass casualties or large-scale physical destruction to the terrorisation of groups of people or an entire population, to assassinations of individuals).

In addition, threats posed by CBRNe materials need to be assessed in conjunction with the technologies that are enablers for their development, manufacturing, storage, or employment.

Furthermore, facilities where CBRNe materials are present (manufacturing plants, storage facilities, transportation infrastructure, waste treatment facilities and the like) can suffer accidents as a result of natural catastrophes, or technical malfunctioning, or they can be damaged as a result of sabotage, or become targets of physical, cyber or other forms of attack. Such incidents can lead to the release of agents into the environment, resulting in immediate effects on people and the environment or causing long-term contamination.

Finally, CBRNe threats are embedded in broader contexts (for example an armed conflict with its different belligerents and their capabilities and intentions, an industrial location with its equipment, infrastructure and nearby populations, or a geographical area with its endemic disease patterns and public health capabilities). Risk mitigation strategies will need to take account of these contextual factors.

As a result, assessments of CBRNe risks are complex and highly scenario-dependent. This poses serious challenges to traditional approaches to assessing the risks involved. Traditional risk assessment and management strategies build on probabilistic approaches: they identify the relevant hazards, analyse the factors that determine the corresponding impact of incidents, and assess their likelihood (including with regard to the intentions and capabilities of the different actors concerned). Such assessments highlight vulnerabilities in prevention, response and recovery systems, and allow a prioritization of necessary measures to strengthen prevention, response and recovery. On that basis, effective risk mitigation strategies can be designed for a variety of relevant scenarios.

An example of this approach is the CBRNe response planning developed by the US Department of Homeland Security (DHS). DHS is responsible for conducting risk assessments for CBRN agents under the 2004 BioShield Act and various Homeland Security Presidential Directives. To implement these requirements, DHS develops CBRN Terrorist Risk Assessments – TRAs – and Material Threat Assessments – MTAs (GAO 2011). From time to time, these TRAs and MTAs are combined into integrated CBRN Terrorist Risk Assessments (ITRAs). By 2012, the DHS had conducted three TRAs covering biological risk factors, two chemical TRAs, and two Integrated CBRN Terrorism Risk Assessments (GAO 2012).

The methodology used in such probabilistic risk assessments defines a set of specific scenarios on the basis of event trees to capture a relevant and realistic range of risks of concern. It then estimates the probability and consequences for each scenario and from these data calculates risks. The complexity of this approach becomes apparent when one looks at the number of variables and, consequently, scenarios that need to be systematically worked through. For a BTRA, the scope defined by DHS is based on three terrorist organisation categories, 37 different biological hazards, 2 exposure routes, 20 different targets, and 7 possible modes of dissemination – resulting in more than 5 billion (theoretical) scenarios of which more than 600,000 result in consequences (White 2016).

In such an approach that is based on specific threat agents, uncertainty and complexity are the major challenges. Uncertainties exist, amongst others, in the understanding of the agent(s) concerned and their behaviour, in the modelling of how scenarios would play out, and in the input data used in the models. Furthermore, uncertainties are accumulative. This and the complexity of the matter may well be a reason why, according to a 2012 GAO audit, only 2 out of 12 CBRN-specific response plans developed by DHS at the time were directly informed by CBRN risk assessments; another seven were indirectly informed by the existing risk assessments (GAO 2012). Risk assessment, management and communication approaches and their tools remain important for implementing an effective response to a CBRNe incident: together with other considerations and data, they inform the decision making processes during an incident response, from strategic to operational and tactical levels. But for broader CBRNe preparedness planning and prevention, more generic approaches are important, aiming at developing generic response capabilities that can reach back to specialised competencies and resources as and when needed. Such generic preparedness aims at increasing resilience in society to CBRNe incidents.

Experience in Europe underlines that the CBRNe threat spectrum is highly fragmented and dynamic. Basic CBRNe materials as well as information about how to employ them are widely available in open sources including the Internet, and risk assessments for such scenarios are extremely complicated if not impossible given the large number of variables, the variances in those variables, and situational unpredictabilities – hence the need for a refocus on strengthening generic consequence management capabilities and enhanced resilience, combined with reach-back to specialised expertise as and when required (Herzog 2019).

At the heart of any CBRNe risk mitigation strategy, however, must be a sound understanding of the sciences and technologies involved, of the trends and drivers that steer their development and application, and of the manner in which these developments may alter existing or create new risk potential as well as opportunities to manage evolving risks. The role of science and technology in shaping and managing the evolving CBRNe threat landscape, then, is the focus of this book. The different chapters will look at a number of technologies and scientific disciplines that shape this landscape. But this cannot be an all-encompassing, comprehensive review. Other areas of science and technology that may be equally relevant are only touched upon briefly. It was therefore desirable to open the book with a more general reflection on how advances in science and technology may affect the overall CBRNe security landscape.

A first observation is that science and technology are evolving at a fast pace. In recent decades, the time it takes for scientific discoveries to move from the laboratory bench to practical application in industrial development and manufacturing has shrunk considerably. In 2011, an international study commissioned by the US National Academies concluded that "there has been particularly rapid progress in the power of, and access to, enabling technologies, especially those depending upon increased computing power. These include high throughput laboratory technologies and computational and communication resources" (NRC 2011, p. 8). The study highlighted as possible consequences the increase of collaborations at a global scale including the emergence of "virtual laboratories"; increased access to and diffusion of sophisticated reagents, kits and services; the facilitation of the transfer of tacit knowledge across the web; and a reduction of barriers to the spread of S&T knowledge for responsible, but also for malevolent purposes (Ibid.).

It is important, therefore, to recognise the potential of scientific advances and emerging technologies at an early stage, to be able to respond to new safety and security challenges in time. Often called "horizon screening", formal assessments of the possible impact of advances in science and technology are recognised as a means of ensuring that regulatory systems (including arms control agreements, export control systems, national laws and regulations concerning safety and security) as well as administrative measures and industry standards are adapted *before* science and technology have moved from the laboratory to practical use, and *before* these applications have spread widely. In practice, however, regulatory adaptations tend to be slow.

At the same time, "horizon screening" must be aware of certain pitfalls. Evaluations at an early stage of technology development (at the initial up-swing of

the so-called "hype curve", when the real capabilities and limitations of a technology are yet to be fully understood) carry the risk of exaggeration or may be altogether misleading; the selection of technologies that appear to be of concern can be somewhat arbitrary when the technologies considered are still fast evolving; and new technologies do not evolve into an empty space but, most of the time, must compete with well established and mature technologies that have established markets and proven technological and economic viability. In many application fields, tacit knowledge remains important for the effectiveness of technological solutions, and/or for the economy of their exploitation. All this sets limits to how quickly regulatory systems can and should respond to scientific and technological progress, or it may lead to regulatory adaptations that subsequently turn out to be ill-advised "knee-jerk" reactions.

Secondly, advances in science and technology can happen in a non-linear fashion – leaps in understanding as well as chance discoveries (serendipity) that remove obstacles in the way of faster or more widely distributed application of certain techniques, or that result in new understandings or approaches that open up new avenues for scientific inquiry. Such qualitative leaps are more likely when different scientific and engineering disciplines are deployed together, in particular if they have not hitherto been combined. An example is the convergence in the life sciences – the combined deployment of a range of different scientific methods and technologies at the intersection of chemistry and biology. This convergence brings together theoretical concepts and investigative methods from different science and engineering disciplines; from mathematics, modelling and simulation of complex systems; and from manufacturing technologies such as additive manufacturing and DNA origami. It makes use of miniaturization, automation and robotics in research, development and manufacturing. And it exploits new approaches to analysing very large sets of data, including deep learning and artificial intelligence. Any one of these approaches has the potential of creating significant change in science, technology and industrial application – their combination is expected by many to revolutionise the life sciences and their application in society.

Thirdly, one development is causing particular concern today: the shift in risk potential from materials and equipment to information. The nexus of disruptive technologies and CBRNe security will require more and more to take a holistic and bold approach towards CBRNe risk mitigation. The "dematerialization" of the CBRNe threat spectrum is the result, amongst others, of the growths of the "internet of things" in our digital age. Indeed, the theoretical possibility provided by AI-driven storage and analyses of mega-data can render the role of the material substrate on which traditional CBRNe threats have traditionally been based, less essential.

For example: if State actors, or even terrorist or criminal groups, were to deploy Stuxnet-like worms to attack national critical infrastructure, even when they are "air-gapped", traditional protections and threat reduction measures would become irrelevant. In such a scenario, traditional protections (detecting and fending off an attack, securing the perimeter and preventing access by the attacker to critical assets) are bound to fail – what is needed instead are means that enable critical systems to continue functioning and to recover even if they are "infected" by threats.

Such a paradigm shift from CBRNe protection to CBRNe resilience needs to be promoted and advanced in the near future, but it will call for a rethinking of some of our current risk mitigation approaches.

A fourth issue is S&T diffusion: one possible effect of scientific and technological progress is the lowering of thresholds for the conduct of certain scientific, technical or economic activities in the CBRN domain. This may include a spread of capabilities for conducting certain types of experiments, manufacturing certain types of products, or gaining access to certain types of materials that in the past have stood in the way of their broader application. CRISPR-Cas9 based genome editing, additive manufacturing ("3D printing"), the emergence of an Internet-based supply chain for complex biomolecules, and cloud manufacturing to customer specification of chemicals and biologicals are recent examples of such "democratization" trends. Whilst such new tools don't do away with the importance of theoretical understanding and tacit knowledge, they certainly contribute to the fast and global diffusion of new methods, technologies, equipment and materials that may pose concerns with regard to the proliferation of CBRNe capabilities.

At the same time, science and technology evolve in a particular economic, institutional and societal context. New scientific discoveries or methods don't automatically result in new types of weapons, or lead to activities that may carry risks to society. The directions which scientific inquiry takes towards technological development and industrial application are not unconstrained, but influenced by external as well as internal factors, amongst them (but not limited to):

- Laws and regulations that create barriers that institutionalised science and technology organisations respect as constraints for their projects
- Expectations and demands from society that create a context within which scientists and engineers define their objectives, and societal recognition of achievements reinforces this "self-image" and channels the utilisation of science and technology in certain directions
- Funding priorities that reflect both internal interests and objectives of the S&T enterprise and expectations and demands of funders in governments, societal actors, and private investors
- The scientific method itself (systematic observation, measurement, and experimentation; the formulation, testing, and modification of hypotheses; rigid documentation of experimental methods and result and their publication to allow results to be reproduced by others), which sets standards for what is generally accepted as proper scientific conduct, which in turn guides the ethics of science and its own perceptions of proper conduct.

From a scientific perspective, or perhaps more accurately from the perspective of the science and technology enterprise, CBRNe risk mitigation therefore is in essence a matter of building a culture of responsible behaviour, and of shaping the space available for scientific inquiry and its practical application in ways that minimises CBRNe risks. Like in other domains of influencing behaviour (such as laboratory safety, or the prevention of falsification of research results), developing such a culture of responsibility does not replace other means of risk mitigation (such as laws and

regulations and their enforcement including sanctions), but without it, compliance with accepted norms would remain fragile and norms could easily be undermined by new developments.

A crucial issue in this context is the different time scale between developments in science and technology, and the normatization process which includes law framing and the enactment and application of regulations by the States bodies. It has been argued in several contexts that there exists a time gap between these two realities and that State as well as international institutions are not able to catch up with the pace of scientific and technological change. Due to this ineluctable reality, the only practical solution to this conundrum is to boost the ethical responsibility of scientists and engineers, and to train young scientists to become drivers in finding solutions to risk mitigation rather than becoming part of the problem.

Until now, many of the approaches to CBRNe risk mitigation have their origin in prevention and protection concepts developed against weapons of mass destruction during the Cold War. These were concepts developed with State-level weapons programmes in mind. They involved strategic deterrence and force protection, technology transfer controls and embargos to deny certain countries access to critical technologies, as well as arms control and disarmament measures aimed at limiting certain types of weaponry or their delivery systems, in terms of qualitative characteristics as well as overall numbers, and where possible reducing their numbers or altogether eliminating them. International humanitarian law, too, remains an important constraint on the manner in which such weapons may be used, or must not be used, in armed conflict.

Arms control measures developed during the Cold War included data exchanges and verification measures such as the acceptance of the use of certain national technical means, on-site inspections conducted bilaterally or by international inspectors, transparency measures to build confidence and create a degree of predictability, and political and institutional compliance management tools to clarify compliance concerns and resolve problems and disputes. Technical measures to verify compliance with arms control measures were constructed in ways that would ensure the detection of militarily significant violations in a timely manner to deny a violator any significant advantage from cheating.

Whilst this system of international, regional and bilateral treaties and arrangements in the arms control domain remains important until today, the security environment within which risk mitigation strategies need to function has changed profoundly from that of the Cold War and the immediate post-Cold-War period. In a review of the priorities of the OPCW conducted by a high-level panel set up by the OPCW Director-General in 2011 under the leadership of Swedish diplomat Rolf Ekeus, this evolving security environment was characterised thus (OPCW 2011):

- Conflict is no longer framed in the context of opposing military alliances in a bipolar world. The number of inter-State conflicts has declined yet the level of violence has not. The borderline between war, civil war, large-scale violations of human rights, revolutions and uprising, insurgencies and terrorism as well as organised crime are blurred.

- In addition to traditional military forces, more non-State actors have appeared on the battlefield, i.e. paramilitary groups, warlords and their militias and volunteers, mercenaries and private military companies, terrorists and criminal groups. As a consequence, contemporary threat perceptions are also driven by attacks on populations and critical infrastructure, in addition to more traditional state-based threats.
- Furthermore, there are worries, in such types of conflict and with such actors, that the rules of international law applicable in armed conflict, and in particular the principles and rules of international humanitarian law, may be undermined.

As the science and technology CBRNe landscape is changing rapidly, the advancement of disruptive technologies such as artificial intelligence, the exploitation of cyberspace, synthetic biology, omics and big data, raises more concerns due to the absence of a unified arrangement to mitigate these CBRNe challenges and of the related technologies.

An early indication that, funding and time permitting, non-State actors are *capable* of deploying a WMD capability was the Sarin attack of the Aum Shinrikyo in the Tokyo subway in 1995. The attacks of September 11 (2001) and the subsequent Anthrax mail attacks in the USA confirmed that non-State actors were capable of inflicting mass casualties, or causing terror and economic damage, at a significant scale. They and subsequent developments and the use of improvised explosive devices and chemical weapons in Iraq and Syria also signalled a growing *intent* of certain kinds of non-State actors to resort to unconventional attack schemes.

These incidents, furthermore, demonstrated a level of sophistication that had not been seen previously with regard to non-State actors. The Aum Shinrikyo sect was able to set up a pilot-plant-scale production line for the nerve agent Sarin (it failed, however, to develop effective dissemination techniques); al Q'eda turned commercial aircraft into weapons to huge destructive effect and reportedly developed and successfully tested a blueprint for a device to disseminate toxic chemicals; and Bruce Irwin, the presumed instigator of the Anthrax letter attacks, managed to formulate anthrax spores in ways that some observers described as "military-grade".

These and other developments raised concerns about the possibility that terrorists and criminal organisations might be able to harvest new technological advances and scientific discoveries to acquire even more effective means of causing large-scale terror and destruction.

Subsequent developments in particular in the Middle East, on the other hand, underscored that CBRNe threats are not only associated with scientific and technological advances exploited for novel types of weapons and war fighting, but can equally involve the employment of old technologies and long-established types of weapons and materials, albeit in ways and circumstances that may differ from traditional military scenarios. A striking example for the association of CBRN threats with advances in science and technology was the assessment by the US Director of National Intelligence in 2016 that genome editing constituted a global security threat alongside other WMD threats (Clapper 2016). A striking example for

the use of old and widely distributed technology for mass killing and the terrorisation of populations was the use of chlorine gas in the Syrian armed conflict.

The Syrian conflict is also an example for the increasing association of CBRNe attack scenarios with propaganda warfare. This is not *per se* a new phenomenon – chemical as well as biological methods of warfare have long been associated with misinformation and propaganda. Partly this was the result of certain technical complexities of these methods of warfare that made it more difficult to establish precisely what had happened in an attack; partly it emanated from the secrecy that surrounds WMD programmes – some attack scenarios were in fact clandestine operations involving concealed agent releases; and partly it reflected the perfidy that is often associated with the use of these types of weapons – the use of poison and disease as weapons is considered a dishonourable means of war fighting in many cultures (and of course some are prohibited under international law). What has changed is the ease with which misinformation (from half-truth to outright lies) can be spread through informal yet highly influential and widely distributed channels – social media and Internet platforms – and the intensity and sophistication with which States as well as non-State actors are using such platforms as well as traditional media outlets to create narratives that serve their objectives.

These complexities – the association of CBRNe threats with a multitude of State, State-sponsored and non-State actors, the wide range of scenarios, the impact of enabling technologies on their effectiveness, and combination of CBRNe weapons uses with information warfare – are increasingly being mirrored by national security strategies. In its 2018 National Strategy for Countering Weapons of Mass Destruction (WMD) Terrorism, the United States emphasized the need for continuous pressure against WMD-capable terrorist groups, enhanced security for dangerous materials throughout the world, and increased burden sharing among the US' foreign partners (USA 2018). The strategy defines a set of US policy objectives, which include putting agents, precursors and materials to acquire WMD beyond the reach of terrorists and other malicious actors, deterring States and individuals from providing support to would-be WMD terrorists, establishing an effective architecture to detect and defeat terrorist WMD networks, strengthening defences against and preparedness for mitigating WMD threats at all levels, and identifying and responding to technological trends that may enable terrorists to develop, acquire and use WMD.

The EU, too, in the context of its Action Plan to enhance preparedness to mitigate CBRN security risks, points to a range of terrorist and other violent threats, from both networked groups and lone actors (EC 2017). It observes that terrorist organisations have not used CBRN agents in Europe, but points to credible indications suggesting that they might have the intention of acquiring CBRN materials or weapons and are developing the knowledge and capacity to use them. The action plan emphasises the need for significant investments by EU Member States to reinforce resilience against CBRN threats in terms of prevention, preparedness and response, and calls for a more focused and better coordinated, all-hazards approach (including with regard to mitigating large scale CBRN hazards unconnected to terrorism). To a certain degree, its objectives mirror those of the US National Strategy: reducing

the accessibility of CBRN materials, ensuring a more robust preparedness for and response to CBRN incidents, building stronger links both within the EU and with external partners, and enhancing the knowledge of CBRN risks.

As a kind of a "spin-off" of the EU's Strategy against Weapons of Mass Destruction and its CBRN Action Plan, and aligned to its evolving Common Foreign and Security Policy, the EU has been implementing its CBRN Centre of Excellence Initiative since 2010. The initiative is currently funded under an external financial instrument know as the Instrument contributing to Stability and Peace (IcSP)[1] – see also at the end of this introduction. This EU mechanism, as well as the programmes implemented by the United States to strengthen security and cooperation in CBRN risk mitigation to develop global capacity, are cooperative, bottom-up, voluntary and all-stakeholders approaches based on the idea that promoting and ensuring the security of CBRNe materials and technologies worldwide is a common objective not restricted to zero-sum geopolitical calculations or selected geographic domains.

The Canadian Security Intelligence Service in its 2018 security outlook study (Canada 2016), too, noted that development and use of WMDs would be a continuing concern. While weapons technology will not leap ahead as fast as information technology, the risks of proliferation, or miscalculation, would continue to require constant monitoring and attention. The foresight study also drew attention to the potential of the Internet and cyber technology as a strategically disruptive force. The Canadian study pointed out that international trade, the movement of populations and instability in some countries enabled the spread of WMD expertise, and that there was little prospect of a corresponding improvement in proliferation control mechanisms. Whilst acknowledging the terrorist CBRN threat, it placed particular emphasis on the threat potential emanating from the activities of certain States.

The international community's response to the evolving CBRNe threats emanating from non-State actors has included a wide range of legislative, regulatory, enforcement and administrative measures. A prime example is UN Security Council Resolution 1540 (2004). Adopted under Chapter VII of the Charter, it created legally binding responsibilities for all states to take measures to prohibit and prevent the proliferation of WMD capabilities to non-State actors, in a comprehensive fashion.

The practical measures that this binding resolution compels States to adopt include (UNSC 2004):

- Refraining from providing any form of support to non-State actors in their attempts to acquire, transfer and use nuclear, biological and chemical weapons and their means of delivery;
- Adopting and enforcing appropriate effective laws which prohibit such acts by any non-State actor, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them;

[1] The CoE Initiative was initially launched under the forerunner instrument of the IcSP – the Instrument for Stability (IfS). For the upcoming financing period starting in 2020, a new external financing instrument is being developed that is expected to continue funding the initiative.

- Taking and enforcing effective measures to establish domestic controls to prevent the proliferation of such weapons and means of delivery, including by establishing appropriate controls of related materials (through accountancy measures, physical protection measures, and effective border controls and law enforcement);
- Establishment and enforcement of effective national export and trans-shipment controls including appropriate laws and regulations to control exports, transit, trans-shipment and re-export, and controls on providing funds and services related to such export and trans-shipment.

This and subsequent Security Council resolutions encouraged States to review their situation with regard to measures to prevent the proliferation of WMD capabilities to and by non-State actors, to report to the Security Council about the measures they have taken, to adopt action plans to enhance their measures to prevent WMD proliferation by and to non-State actors, and they encouraged technical assistance to States that so required, including by other countries and by relevant International and Regional Organisations.

In parallel, efforts are being made to further strengthen the treaty system that has been constructed during and after the Cold War to reduce and where possible eliminate WMD threats. Treaties such as the Biological and Toxin Weapons Convention (BWC) of 1975 and the Chemical Weapons Convention (CWC) of 1997, although designed to address State-level WMD threats, contain provisions that compel their parties to enact and enforce domestic controls to prohibit and prevent the proliferation and use of such weapons and materials by individuals and legal persons subject to their jurisdiction or control. In addition, the international treaty system was further developed in such areas as countering terrorism, enhancing nuclear safety and security, strengthening transportation safety and security, ensuring biosafety and biosecurity, and in other relevant areas.

Natural events such as the 2014-2015 Ebola outbreak in West Africa, and major accidents caused by environmental disasters such as the 2011 meltdown of the Fukushima Daiichi nuclear power plant caused by the Tōhoku earthquake and tsunami, were further reminders of the destructive power inherent in CBRNe materials. But it is also recognised that many CBRNe materials are utilised in society as part of normal life, and that, consequently, there will always remain certain risks emanating from accidents or malevolent acts associated with their manufacturing, distribution and use for industrial, agricultural, medical and other peaceful purposes.

Efforts are being made to strengthen capacities to manage these risks, across the entire risk range (the whole of the CBRNe spectrum, as well as with regard to natural, accidental and hostile releases). Measures to this end involve strengthening civil defence organisations, the public health sector, first responder organisations, safety and security organisations within industry and the transportation sector, the development and adoption of safety and security measures and protocols by academic, research and other scientific communities and organisations, and many more.

It has been argued that arms control law provides a common legal framework for CBRN security (Myer and Herbach 2018). CBRN security, it is argued, was primarily

about preventing non-state actors from obtaining, developing, using, and illicitly trafficking weapons of mass destruction (WMD) or related materials and technologies that may be used for hostile purposes. Although different from other instruments of arms control law that deal with controlling weapons and military capabilities of states, CBRN security arrangements deal fundamentally with the control of arms and related technology.

This may indeed be so at the level of international law dealing with CBRNe weapons and materials. Yet, there are no comprehensive legally binding international mechanisms or multilateral arrangements that deal with enabling technologies associated with CBRNe threats. The UN Convention on Certain Conventional Weapons (CCW) is currently used at the level of a UN Group of Governmental Experts (GoG) to discuss how to regulate lethal autonomous weapons systems (LAWS) – an issue that is taken up in several chapters of this book. A similar UN GoG might be launched to deal with the whole CBRNe threats spectrum and related enabling technologies for their employment.

At the practical level as well as with regard to policies and governance structures, however, finding a common approach to effectively mitigating CBRNe risks has remained a challenge. In practice, legislative, preventive, deterrence and response/recovery measures have often remained fragmented. For example, whilst States took steps under Security Council Resolution 1540 (2004), they also needed to respond to initiatives that took a more narrow, sectoral approach. International organisations (IAEA, OPCW, UNODA, UNODC, international organisations for the different transport modes, WHO, OIE, UNOCHA and many others) defined their respective contributions to the fight against terrorism within the context of their respective mandates and capabilities.

All these approaches are complementary, and coordination mechanisms such the UN's Counter-Terrorism Implementation Task Force (CTITF), as well as several UN Security Council Committees, were set up. Additional legal instruments were created, for example in the fields of counterterrorism and nuclear safety and security, and existing instruments were adapted to better address the evolving CBRN threats. Even legal instruments that on the surface might appear to have little to do with non-State actor CBRNe threats have been used to address certain aspects of the CBRN risk spectrum; an example is the International Health Regulation (2005) which requires States to develop core capabilities in their Public Health sectors – in the explicit understanding that these may be called upon to respond to health risks irrespective of whether they resulted from natural causes (disease outbreaks), accidents, or malicious acts.

The multitude of actors, the wide range of relevant technologies and their diversity in terms of maturity and risk potential, the fast and broad diffusion of some new technologies across the globe, and the widespread use of CBRN materials and technologies in society – all these factors complicate the development and application of a holistic and comprehensive CBRNe risk mitigation strategy. With regard to protection and response to incidents, such a "fuzzy" and ever-changing environment calls increasingly for a generic, resilience-based approach rather than the use of traditional (i.e., probabilistic) risk assessment and management tools. With regard

to prevention and deterrence, at the same time, traditional arms control approaches are becoming out-dated and less likely to succeed. Nor are they likely to keep pace with the rapid advances in science and technology, the changes in industrial manufacturing, or the increasingly unpredictable global security environment. Some would argue that this signals the end of arms control as we have known it from previous decades.

The traditional arms control paradigm of the post Cold War period needs to be refocused in the twenty-first century since the so-called "strategic stability" can be affected by the advent of cyber and autonomous technologies, including artificial intelligence, and the close entanglement of nuclear and non-nuclear systems. An underpinning suggestion emerging throughout this book is the need to enhance the dialogue among different specialists in the CBRNe realm to keep a handle on the intangible dimensions of proliferation. Indeed, education, the development of professional ethics, and the development and application of tailored codes of conduct in the CBRNe field could enhance scientific responsibility globally. An appropriate framework for doing so is the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction.

At the same time, in certain CBRN domains such as the life sciences, governments are no longer the primary producers and users of science. It has been noted that the primary producers and users of such technologies are becoming essential partners in preventing the misuse of technology for malevolent purposes (McLeish and Trapp 2011). For example, whilst traditional biosecurity policies have been government-instigated and top-down, the evolving world of science and technology calls for a multi-stakeholder governance approach. Furthermore, the increasingly global diffusion of certain enabling technologies (the Internet, cloud manufacturing, manufacturing at or close to the end user, point of care diagnostics and the like) is an indication that in some respect, we are already living in a "post-proliferation" world. It has been observed that "[in] such a world, traditional models of proliferation control are certain to fail, and the traditional top-down government approaches no longer seem appropriate. From a broader regulatory perspective, the role of governments is changing. The state alone is no longer able to control the way that life sciences discoveries are used. The circumstances beg instead for a governance system that brings together all stakeholders – science, industry, government, and the public – and broadens as well as deepens the basis for compliance with the safe and responsible conduct and utilization of science, thus supporting the norm against biological weapons" (Ibid p. 540).

As a consequence, future policies and mechanisms in the CBRNe domain are likely to be less reliant on top-down approaches such as global arms control treaties, and instead they will need to place more emphasis on arrangements between governments and other stakeholders, including measure taken by the developers and users of technologies such as voluntary compliance and control measures adopted by industry and traders, and the applications of soft tools such as codes of conduct and ethics. This signals a shift from attempts to control and prevent the spread of sensitive technologies and materials to certain actors, to a risk management approach that accepts that whilst prevention, prohibitions and deterrence will continue to play

a role, they will not be able to prevent proliferation. What is needed instead is the development of a culture of non-proliferation and a stronger societal resistance to such threats. Chesney and Citron have argued, in the context of information warfare, that "democracies will have to accept an uncomfortable truth: in order to survive the threat of deepfakes, they are going to have to learn how to live with lies" (Chesney and Citron 2018). The same reasoning may apply to the risks posed by CBRNe materials and technologies. Society will have to accept that CBRNe risks cannot be eliminated altogether, and nor can the proliferation of CBRNe materials and technologies be completely prevented. Instead, society will have to learn how to live with these risks and how best to mitigate against them and develop resilience (Martellini et al. 2017).

The multitude of actors involved in such broader risk management strategies will also call for an approach that relies on effectively connecting hitherto unconnected networks of actors, to share information about the different mandates and capabilities, and to create platforms for coordination and collaborations. Such a "patchwork approach" of expanding and at the same time connecting different regimes and initiatives to create a broader framework to deal with the emerging CBRNe threat spectrum is gradually evolving. But the degree of fragmentation remains significant. Attempts to coordinate and synchronise the activities of the different actors have had only limited success. There have been attempts to develop common, more integrated platforms for practical measures in CBRN risk mitigation. For example, the EU's CBRN Centres of Excellence Initiative (a flagship programme under the EU's Instrument contributing to Security and Peace that provides technical support to non-EU partner countries in the field of CBRN risk mitigation) has taken a comprehensive risk mitigation approach, covering natural as well as man-made risks, accidental as well as hostile scenarios, risks associated with State as well as non-State actors, and risks from the entire spectrum of CBRN materials. More importantly perhaps, it builds on the context and the needs identified by the partner countries themselves, attempting to align technical assistance to these needs and conditions.

The CoE Initiative also has articulated the ambition to offer coordination and collaboration platforms that could be used by other actors, sponsors and benefactors alike. This has indeed been done in a few cases, but they remain few and far between. Despite some success, the initiative continues to struggle with effectively interfacing with other relevant initiatives and programmes that aim at strengthening CBRNe risk mitigation capacities.

This book is an attempt to help developing such a broader conceptual and practical framework towards a more holistic and comprehensive CBRNe risk mitigation strategy. It is structured into two Parts: Part 1 looks at key science and technology dimension of the changing CBRNe risk landscape, and considers the challenges that these developments create for governance approaches of emerging technologies and research, using the developments in the life sciences as a key example. Part 2 looks at some approaches to mitigating the evolving risks.

In Part 1, the book first develops and analyses key examples for advances in science and technology that have the potential of creating new CBRNe proliferation risks; Part 2 looks at technologies that have the potential to help mitigating these evolving as well

as existing threats; and thereafter it discusses a number of practical measures that can be developed further to strengthen resilience and response to CBRNe threats.

With regard to advances that have the potential to change the level and nature of CBRNe threats, the book combines overviews of advances in science and technology with regard to the relevant agent groups and their manufacturing (toxic chemicals, explosives, biological agents, radiological/nuclear materials) with a survey of specific technologies that may change some of the fundamentals underpinning the CBRNe threat spectrum: new and increasingly widely distributed means of delivery (such as hypersonic missiles, drones and other UAVs, and autonomous weapons systems), vulnerabilities emanating from the possibility of cyber attacks on facilities and systems associated with CBRNe materials and technologies, and the potential for the misuse of artificial intelligence to develop novel types and means of warfare involving CBRNe materials and weapons. This section of the book also addresses evolving concepts of hybrid warfare that combine propaganda warfare with the threat or actual use of CBRNe weapons.

In the second Part of the book, Chaps. 11, 12, 13, 14, and 15 address technologies and scientific advances, as well as broader strategies and policy options, that are expected to help strengthening resilience against CBRNe threats. This includes trends in the detection of agent releases as well as medical countermeasures (using the medical response to nerve agent poisoning as a pertinent example). A field that has received increasing attention in recent years is forensics with regard to CBRN incidents. This is partly as the result of CBRNe threats associated with non-State actors; it also reflects the experiences of recent investigations of uses of chemical weapons in Syria, Malaysia and the UK. These investigations have underlined the importance of robust forensic and analytical methodologies as well as databases to be able to attribute responsibility to such incidents, based on scientific evidence. Finally, this Part offers practical guidance on training and education in the CBRNe risk mitigation field, as well as considers methodologies of assessing the effectiveness of such measures.

Whilst individual chapters draw their own conclusions in the context of their particular thematic scope, there was no attempt to put forward overall conclusions. However, as already indicated above, certain common themes emerged from several of the chapters, and we felt it might be useful to summarize them here to give the reader an overall perspective of what the current trends are that shape the CBRNe risk landscape today, and what concepts and strategies might be the most appropriate to manage these risks.

CBRNe risk mitigation, by its very nature, is multidisciplinary, science and technology based, and highly context/scenario dependent. At the same time, there are technical dimensions that are specific to the types of agent concerned, and there are also overarching and generic issues – these call for a holistic strategic approach.

What has become apparent is that within this complicated risk landscape, information management, processing and analysis are becoming more and more important. New tools are drastically enhancing our ability to process vast amounts of data and to analyse complex data sets in ways that the human brain itself is not able to master (including by means of deep machine learning / artificial intelligence).

This is about to change drastically the way in which CBRNe risks are evolving. At the same time, the growing global diffusion of technology and new manufacturing concepts (industry 4.0) are spreading capabilities globally, bringing manufacturing closer to the end user. All this is creating huge new opportunities to identify and manage CBRNe risks, but at the same time it also creates new vulnerabilities and complexities.

To us, it indicates the need for a shift in emphasis: from prohibitions, prevention and protection to strengthening resilience in society. To be clear, prevention and protection remain important and must not be neglected. In fact, strengthening resilience will overlap with preventive strategies (for example in the case of hardening critical infrastructure against the effects of CBRNe threats). But resilience will place a stronger emphasis on "softer", longer-term, strategies such as

- More strongly and explicitly fostering a culture of ethical behaviour and responsible foresight as part of the self-image and professional conduct of scientists, engineers and other professionals who deal with CBRNe materials and technologies
- Embedding these concepts and principles in educational systems – not as an add-on or a form of "securization" but as an integral part of the way in which science, technology and ethics are being taught and understood
- Promoting voluntary, self-regulatory compliance assurance systems in research and development institutions, industry and trade (in a manner perhaps comparable to safety as well as quality assurance systems widely employed today – voluntary but certifiable and seen as a bonus)
- Strengthening the role of international humanitarian law in international relations (thereby modulating the concepts of arms control and disarmament which traditionally function within narrowly defined sets of definitions and prescriptions rather than on a more holistic "do no harm" basis).

At the practical level, this will require outreach by governments and international organisations working in the field, engagement with a wide range of stakeholders, and the creation of suitable platforms – local, regional and global – that allow multiple actors to work together on analysing problems and devising and delivering solutions to CBRNe risks. This must be a bottom-up approach (aimed at strengthening indigenous capabilities that can take account of local conditions and needs), but it will also need an overarching strategic orientation and shared objectives of the different stakeholders.

Martellini and co-authors (Martellini et al. 2017) have argued that CBRN security is a sort of a new organizing principle of the international multilateral relations dealing with international security. Such an approach, even if theoretically sound, is difficult to operationalize and to harmonize with traditional arms-control arrangements.

A deep analysis of the new, cutting-edge technologies, as well as the re-emergence of well-established technologies applied today using new materials or being employed within a different industrial processes environment, including the management and utilization of mega-data, shows that despite these radical changes in the science, technology and industry environments, the fundamental architecture and the legal framework of WMD arms control and the related arms control treaties are still valid.

What is necessary is to "update" their definitions, technical concepts and implementation mechanisms to manage compliance, including national mechanisms to implement treaty requirements and verification processes used to provide confidence in compliance.

To give a few examples: in the BWC, the definition of a biological weapon should be understood to encompass "artificial DNA" (synthetic DNA using base pairs not expressed in nature) – consistent with but expanding on the common understandings adopted by BWC States Parties; in the CWC, the industry verification system in the domain of non-scheduled chemicals needs to be adapted to take account of the impact of chem-bio convergence (such as the changing nature of industrial manufacturing – bioprocesses, AM, cloud manufacturing, etc.); in the NPT the concept of minimal weapon-usable material ("significant quantity") should take into account that the sub-critical nuclear tests allow the five NW-States to design new thermonuclear weapons using sub-critical amounts of nuclear material, and that even the concept of ballistic missile as a vehicle of NWs delivery is too restrictive – indeed, the XXI Century is fast becoming the age of hypersonic gliders with nuclear payloads which would end any kind of nuclear strategic stability and deterrence as we know it from the Cold War. Furthermore, the brain-machine interface and AI augmented reality will create new ethical problems in International Humanitarian Law.

Furthermore, traditional approaches to the WMD arms-control verification processes need to be rendered sufficiently flexible and adaptive to account for the new disruptive technologies and materials that are going to shape the WMD landscape of the XXI Century. That adaptation, however, must not weaken the WMD arms-control norms and legal constraints. To say it in other words: the architecture and normative basis of the WMD arms control regimes should be perpetual whilst their definitions, implementation processes and review mechanisms (e.g., the WMD Treaty Conferences of States parties) should be revised whenever necessary, synchronised with the advances in science and technology as well as industrial application over time.

Of course, the diplomatic process itself would be enhanced by more actively engaging CBRNe scientists and engineers – as proactive partners of the diplomats that are in charge of the multilateral diplomatic gatherings that attempt to manage the new Prometheus S&T challenges. How to achieve concretely this task is not clear today, but some global reflection is needed if one wants to avoid the risk of a full collapse of XXI Century arms-control under the new S&T developments of our epoch.

References

Canada. 2016. Canadian Security Intelligence Service: 2018 Security Outlook – Potential Risks and Threats – a foresight project, Occasional Papers (June 2016).

Chesney, Robert and Danielle Citron. 2018. *Deepfakes and the New Disinformation War*, Foreign Affairs (11 December 2018). https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war accessed on 12 January 2019.

Clapper James R. 2016. Director of National Intelligence: Worldwide Threat Assessment of the US Intelligence Community, US Senate Armed Services Committee, Statement for the Record on 9 February 2016. https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf accessed 9 January 2019.

European Commission. 2017. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, COM(2017) 619 final (18 October 2017).

GAO. 2011. U.S. Government Accounting Office (GAO), Report to the Committee on Homeland Security and Government Affairs, US Senate: *National Preparedness – DHS and HHS can further strengthen coordination for Chemical, Biological, Radiological, and Nuclear Risk Assessment*, GAO-11-696 (2011).

———. 2012. U.S. Government Accounting Office (GAO), Report to the Committee on Homeland Security and Government Affairs, US Senate: *Chemical, Biological, Radiological, and Nuclear Risk Assessments – DHS should establish more specific guidance for their use*, GAO-12-272 (2012).

Herzog, C. 2019. *Preparedness for low-probability incidents with high consequence potential – the example of bioterrorism, strategies and problems*, presentation at the annual meeting of the Working Party on CBW Non-proliferation, Berlin 2019, private communication.

Martellini, Maurizio, et al. 2017. *A reflection on the future of the CBRN security paradigm*. In *Cyber and chemical, biological, radiological, nuclear, explosives challenges – Threats and counter efforts*, ed. Maurizio Martellini and Andrea Malizia. Switzerland: Springer.

McLeish, Caitríona, and Ralf Trapp. 2011. *The life science revolution and the BWC*. The Nonproliferation Review 18 (3): 527–543.

Myer, Eric, and Jonathan Herbach. 2018. *Arms control law as a common legal framework for CBRN security*. In *Enhancing CNRNE safety and security: Proceedings of the SICC 2017 conference*, ed. Andrea Malizia and Maurizio D'Arienzo, 2018, 207–214. Switzerland: Springer Intl. Publ.

NRC. 2011. *Trends relevant to the biological weapons convention*. Washington D.C.: National Research Council of the National Academies (of the United States of America) in cooperation with the Chinese Academy of Sciences, IAP – the Global Network of Science Academies, the International Union of Biochemistry and Molecular Biology, and the International Union of Microbiological Societies, The National Academies Press.

OPCW. 2011. Note by the Director General: *Report of the Advisory Panel on Future Priorities of the Organisation for the Prohibition of Chemical Weapons*, Technical Secretariat document S/951/2011 (25 July 2011).

United Nations Security Council. 2004. Resolution S/Res/1540(2004), 28 April 2004.

United States. 2018. National strategy against weapons of mass sestruction terrorism, December 2018.

White, Scott. 2016. *CBRN Terrorism Risk Assessments – Methods and Applications*, Military Operations Research Society (MROS) 28 July 2016, available at https://www.pic.gov/sites/default/files/DHS%20Terrorism%20Risk%20Assessments%20July%202016_Part1.pdf. Accessed 13 February 2019.

Part I
The Changing CBRN Risk Landscape