Terrorism, Security, and Computation

Maurizio Martellini
Andrea Malizia *Editors*

Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges

Threats and Counter Efforts

Springer

Terrorism, Security, and Computation

Series Editor
V.S. Subrahmanian

More information about this series at http://www.springer.com/series/11955

FONDAZIONE
ALESSANDRO
VOLTA

MASTER CBRNe
Chemical, Biological, Radiological, Nuclear and explosive
Department of Industrial Engineering and School of Medicine and Surgery

Maurizio Martellini • Andrea Malizia
Editors

Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges

Threats and Counter Efforts

Springer

Editors
Maurizio Martellini
University of Insubria and Landau Network
Fondazione Volta
Como, Italy

Andrea Malizia
Department of Biomedicine and Prevention
University of Rome Tor Vergata
Rome, Italy

ISSN 2197-8778 ISSN 2197-8786 (electronic)
Terrorism, Security, and Computation
ISBN 978-3-319-62107-4 ISBN 978-3-319-62108-1 (eBook)
DOI 10.1007/978-3-319-62108-1

Library of Congress Control Number: 2017953184

Printed on acid-free paper

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

Contents

Editorial Board

Introduction

The international security landscape is under stress, because of a worldwide new security concept and of the increasing threats of non-state actors, including terrorist groups, as well as of the difficulty to design long-term counter measures and security initiatives. In particular, conventional terrorist attacks could increase the general instability, but we cannot exclude nonconventional, asymmetric, hybrid attacks by non-state actors or states through proxy actors. Among the nonconventional attacks, the governmental agencies, think tanks, and academies should consider the persisting proliferation of chemical, biological, radiological, nuclear, and explosive (CBRNe) assets and the related cyber (Cy) systems involved. It is essential to analyze the evolution of the threats in order to enforce the safety, security, and CBRNeCy risk management. In general, to achieve this goal, a multidisciplinary approach is needed, a multilayer strategy is demanded, and different users should be involved, spanning from the academy to the NGOs/think tanks and to the governmental agencies.

Not only could the CBRNeCy threats directly impact on several critical infrastructures, but they have a wider impact; therefore, a large spectrum of challenges should be considered. These are related to global security issues, like the reduction of fossil energy resources, the massive exploitation of potable water resources, and, in general, catastrophic events related to climate change. The control of energy and water resources might be pursued, in an asymmetric hybrid warfare scenario, through CBRNeCy events. On the other side, major environmental destructive events might be triggered by criminal or unintentional actions such as the Bhopal chemical accident. Moreover, major nuclear/radiological events, like the Fukushima Daiichi one, that are the consequence of a tsunami or an earthquake, can also be the result of a deliberate attack against the safety and security systems of a nuclear power plant. From the academic point of view, the risk management of these major CBRNeCy events, considering their low probability and their high destructive potential, falls under the definition of "black swan" events that require a further boost in the preparedness, prevention, mitigation, and response phases, with respect to conventional events.

An additional CBRNeCy threat is represented by the growing diffusion and availability of scientific knowledge and expertise in this field that represents the "human dimension of proliferation." The mitigation of this risk could be achieved only through "intangible" measures, like education, training, and proliferation awareness raising. In a theoretical social science framework, this contributes to create a "CBRNeCy taboo," "CBRNeCy norms," and "CBRNeCy codes of conduct."

In every industrialized country there are multiple entities (governmental agencies, ministries, universities, think tanks, NGOs, etc.) with specialized teams in very specific fields, but the complexity of CBRNeCy events requires professionals that not only have specific know-how but are also able to look at this phenomenon with a comprehensive approach. Furthermore, an enhanced coordination among these entities is paramount.

This monograph will deal extensively with the security and safety of CBRNeCy assets and management, as well as with the strengthening of the security and safety culture, and will show which risks may emerge and how to face them through an enhanced risk management approach.

This monograph should be the first one tackling the CBRNeCy threats, their risk mitigation measures, and the relevance of raising proliferation awareness and education/training reinforcing CBRNeCy security and safety. It will also present international instruments and legislations/regulations to deal with them as, for instance, UNSC Resolution 1540 of 2004. In general, it should be desirable to transform the CBRNeCy security, in a holistic sense, into a new international mechanism to be placed side by side with the traditional arms control international treaties such as the NPT, BTWC, and CWC.

More importantly, with respect to other "technical manuals," this monograph will address a multitude of stakeholders with different professional backgrounds and will have a multidisciplinary nature as a consequence of the need to consider crosscutting areas like the convergence of biology and chemistry, the development of edging technologies, and, in the cyber domain, the impelling risks of the use of malwares against critical subsystems of CBRNe facilities as, for instance, against the supervisory control and data acquisition (SCADA) subsystems of fertilizer industries or refineries.

In conclusion, facing CBRNeCy threats cannot be achieved only by the aggregation of independent competences. The purpose of this monograph is to introduce a new key concept concerning the holistic and comprehensive approach to CBRNeCy. The editors and the authors, with this monograph, want to demonstrate how an integrated and cooperative scientific and technical CBRNeCy approach can evolve into a new comprehensive discipline.

A Reflection on the Future of the CBRN Security Paradigm

Maurizio Martellini, Tatyana Novossiolova, and Andrea Malizia

Abstract This paper is focused on the concept of CBRN security paradigm and how this concept is affecting the international community on develop and maintain an appropriate effective measures to account for and secure such items in production, use, storage or transport; on the develop and maintain an appropriate physical protection; on the develop and maintain appropriate effective border controls and law enforcement efforts. Basically on the develop and maintain all the actions needed to reduce risks.

Keywords CBRN security paradigm • WMD • CW • BTWC

1 Introduction

For decades, issues concerning the proliferation of weapons of mass destruction (WMD) – biological, chemical, and nuclear – have been largely addressed within the framework of disarmament and arms control. In the second half of the twentieth century, key international multilateral agreements were negotiated that effectively set the legal grounds for the prohibition of entire classes of WMD (biological and

M. Martellini (✉)
University of Insubria and Landau Network Fondazione Volta, Como, Italy
e-mail: maurizio.martellini@uninsubria.it

T. Novossiolova
Landau Network Fondazione Volta, Como, Italy
e-mail: tnovossiolova@gmail.com

A. Malizia
Department of Biomedicine and Prevention, University of Rome Tor Vergata, Rome, Italy
e-mail: malizia@ing.uniroma2.it

M. Martellini, A. Malizia (eds.), *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges*, Terrorism, Security, and Computation,
DOI 10.1007/978-3-319-62108-1_1

chemical) and the control the spread of others (nuclear). The norms of customary international law have thus been embedded in statute law binding on all States Parties to the respective treaties – the 1968 Non-Proliferation Treaty (NPT), the 1975 Biological and Toxin Weapons Convention (BTWC), and the 1993 (1997) Chemical Weapons Convention (CWC). States are the referent object of all three treaties: it is states that are responsible for both implementing and observing the treaty provisions and that, at the same time are considered the primary source of potential threats.

With the dawn of twenty-first century marked by the tragic events of 9/11 and the subsequent Anthrax Letters Attacks, the limitations of the traditional state-centred lens through which security has been predominantly viewed and assessed have become acutely apparent. Against the backdrop of intense globalisation coupled with rapid scientific and technological advancement, the fragmented realities of post-modernity have given rise to novel security challenges which hardly recognise borders and against which established means of defence often fall short of delivering the intended objectives. Issues such as international terrorism, organised crime, illicit trafficking, and smuggling that previously have been addressed in silos can no longer be dealt with in isolation from other concerns, including the problem of development and proliferation of WMD. Likewise, given the shift in attention to the effects of events rather than their causes, the spectre of possible security risks involving WMD-related knowledge and materials has drastically expanded encompassing natural disasters (e.g. disease outbreaks, physical destruction of nuclear and/or chemical plans as a result of tsunami, hurricane, or other naturally occurring catastrophic event), accidents (e.g. infrastructural failures, laboratory leaks), and deliberate attacks (e.g. terrorist attacks, sabotage).

Within the context of a rapidly evolving security landscape, new strategies and tactics are required, in order to adequately prevent, detect, respond to, and mitigate potential risks. The multifaceted nature of novel security concerns related to WMD knowledge and materials calls for a redefinition of traditional disarmament and arms control approaches, that is designed to enhance their flexibility and adaptability and thus maximise their effectiveness and efficiency. A fundamental element of this process of redefining WMD security is the emergence of a CBRN – chemical, biological, radiological, and nuclear – security paradigm that is underpinned by a comprehensive set of measures, policies, and practices aimed at addressing risks related to CBRN knowledge and materials, regardless of whether the origins of such risks are naturally occurring events, accidents, or acts of deliberate misuse.

2 The CBRN Security Paradigm: Origins and Evolution

By design, the CBRN security paradigm is a relatively recent development which has been steadily evolving over the past two decades. In some respects its origins can be traced back to 2004 when the United Nations Security Council unanimously adopted Resolution 1540 (UNSCR 1540) on *Non-Proliferation of Weapons of Mass*

Destruction – a Resolution that was adopted under Chapter VII of the United Nations' Charter which made it legally binding on all states. Under UNSCR 1540:

> all States shall take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall:

(a) Develop and maintain appropriate effective measures to account for and secure such items in production, use, storage or transport;
(b) Develop and maintain appropriate effective physical protection measures;
(c) Develop and maintain appropriate effective border controls and law enforcement efforts to detect, deter, prevent and combat, including through international cooperation when necessary, the illicit trafficking and brokering in such items in accordance with their national legal authorities and legislation and consistent with international law;
(d) Establish, develop, review and maintain appropriate effective national export and trans-shipment controls over such items, including appropriate laws and regulations to control export, transit, trans-shipment and re-export and controls on providing funds and services related to such export and trans-shipment such as financing, and transporting that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations. [1]

The provisions of UNSCR 1540 have been reinforced by subsequent Resolutions, such as UNSCR 1673, UNSCR 1977, and UNSCR 2325. Yet it is worth noting that whilst UNSCR 1540 is the first international legal instrument to address all three classes of WMD and call upon all states to implement relevant measures, its scope remains largely limited to criminal activities carried out by non-state actors. States are bound by the provisions of the UNSCR 1540 to report on steps that they have taken to implement the Resolution. They are also encouraged to prepare on a voluntary basis, National Implementation Action Plans to map out their priorities for implementing the key provisions of the Resolution [2]. The Security Council Committee established pursuant to Resolution 1540 (1540 Committee) and its Group of Experts administers the collection of national reports and other documentation. The 1540 Committee further has a clearinghouse role to facilitate assistance to others for implementation of the Resolution [3].

The CBRN security paradigm has also manifested itself in the context of international multilateral agreements. Whereas the focus of the BTWC, NPT, and the CWC as noted in the previous section has been on disarmament and arms control, including destruction and reduction of existing stockpiles of weapons, in the recent years it has shifted to stakeholder engagement, capacity building, and fostering sustainable systems for oversight at institutional, national, regional, and international level.

One area in which considerable progress has been made is nuclear security. Since 2002, the International Atomic Energy Agency's (IAEA) Board of Governors has been adopting a *Nuclear Security Plan.* The primary objective of the fourth edition of the *Nuclear Security Plan, 2014–2017* is 'to contribute to global efforts to achieve effective security wherever nuclear and other radioactive material is in use, storage and/or transport, and of associated facilities by supporting States, upon request, in their efforts to meet their national responsibilities and international obligations, to reduce risks and to respond appropriately to threats.' [4] To this end, the *Plan* covers seven programme elements, including:

- Information Collation and Assessment;
- External Coordination;
- Supporting the Nuclear Security Framework Globally;
- Coordinated Research Projects;
- Assessment through Self-assessment and/or through Peer Review Missions;
- Human Resources Development;
- Risk Reduction and Security Improvement [5].

In order to enhance nuclear security capacity building, the International Network for Nuclear Security Training and Support Centres (NSSC Network) was set up in 2012 in Vienna by representatives of 30 IAEA Member States. The NSSC Network is a collaborative network of security training and support centres which seeks to:

- 'Promote a high level of nuclear security training and support services as a cornerstone in the development of sustainable national, regional and global nuclear security training and support centres;
- Facilitate cooperation and assistance activities (including technical and scientific), to optimize the use of available resources, and to leverage those resources to meet specific needs.'

The Network comprises three Working Groups. These are: Working Group A on Coordination and Collaboration; Working Group B on Best Practices; and Working Group C on Information Management and other Emerging Issues. Membership is open to all IAEA Member States, observers to the IAEA and other relevant stakeholders involved, or planning to be involved, in the provision of training and/or technical and scientific support in the area of nuclear security [6].

A similar trend has been observed in the area of chemical security. In a Statement delivered on 20 February 2012, the Director General of the Organisation for the Prohibition of Chemical Weapons noted that:

> Despite the existence and progressive strengthening of clear norms against chemical weapons, criminal or terrorist use of either chemical weapons or the use of toxic chemicals as chemical weapons remains a concern. Especially within the contemporary international security environment, there is a real threat of non-state entities acquiring and using dangerous weapons [7].

Besides the risk of non-state actors acquiring chemical weapons, the Statement also recognised that:

> The obligations of the Convention extend through national laws to all citizens of a country including the individual scientist and engineer. Many chemists, academics, scientists, engineers, technicians, however, have little or no exposure during their training and professional life to the ethical norms and regulatory requirements of the CWC. At the same time, advances in the life sciences are creating enormous opportunities. While their potential for benefit is undisputed, these could also be prone to abuse. Education and awareness-raising about the norms and principles enshrined in the CWC are therefore becoming increasingly important.

At the Third Review Conference of the CWC in 2013, States Parties underscored their:

> **Determination** to maintain the Convention's role as a bulwark against chemical weapons; to that end to promote, inter alia, outreach, capacity building, education and public diplomacy; [Emphasis as original; see para.9.15]

and

> acknowledged the role of education, outreach and awareness-raising as a relevant activity for the national implementation of the Convention, including awareness among academia and relevant scientific communities of the provisions of the Convention, the domestic laws and regulations relevant to the Convention. Accordingly, the Third Review Conference welcomed the establishment of the SAB temporary working group on education and outreach [8].

The Eight Review Conference of the Biological and Toxin Weapons Convention (BTWC) held in November 2016 when considering the national implementation of the Convention reinforced the language on the value of education and awareness-raising adopted by its predecessor:

13. The Conference notes the value of national implementation measures, as appropriate, in accordance with the constitutional process of each State Party, to: […]

(a) encourage the consideration of development of appropriate arrangements to promote awareness among relevant professionals in the private and public sectors and throughout relevant scientific and administrative activities and;
(b) promote amongst those working in the biological sciences awareness of the obligations of States Parties under the Convention, as well as relevant national legislation and guidelines;
(c) promote the development of training and education programmes for those granted access to biological agents and toxins relevant to the Convention and for those with the knowledge or capacity to modify such agents and toxins;
(d) encourage the promotion of a culture of responsibility amongst relevant national professionals and the voluntary development, adoption and promulgation of codes of conduct. [9]

With regard to Article VII of the BTWC which pertains to the provision of assistance in case of an alleged use of biological and toxin weapons, the Conference further recognised

> 'capacity building at the national and international levels as the most immediate imperative for enhancing and strengthening the capacity of the States Parties to promptly and effectively detect and respond to the alleged use or threat of use of biological weapons.'

More specifically, the Conference drew attention to the

> 'the need for States Parties to work nationally, and jointly, as appropriate, to improve, in accordance with their respective circumstances, national laws and regulations, their own disease surveillance and detection capacities for identifying and confirming the cause of outbreaks and cooperating, upon request, to build the capacity of other States Parties. The Conference notes that the International Health Regulations (2005) are important for building capacity to prevent, protect against, control and respond to the international spread of disease; such aims are compatible with the objectives of the Convention' [10].

The concept of CBRN security has been considered within the framework of various international ad-hoc initiatives. A case in point is the Global Partnership against the Spread of Weapons of Mass Destruction which was established during the G8 (currently G7) Summit held in 2002 in Kananaskis, Canada. In 2009 the

Global Partnership Working Group (GPWG) issued a document titled ‘Recommendations for a Coordinated Approach in the Field of Global Weapons of Mass Destruction Knowledge Proliferation and Scientist Engagement’ which drew attention to the fact that:

> 2. The proliferation of WMD expertise, or any sensitive knowledge in the chemical, biological, radiological, and nuclear (CBRN) areas, remains a serious concern. Preventing the illicit use of such knowledge is one of the most difficult non-proliferation challenges to address, as we are dealing with scientists, engineers and technicians who, in some cases (those doing biological research, for instance), may not consider their expertise and current activities as potentially vulnerable to misuse by others for whom their “proliferation-critical” knowledge could represent a route to developing a WMD capability. They should be made aware that their legitimate work could have dual-use applications and be diverted for malicious purposes.

The document went on to underscore that

> 4. Closer attention is now needed to engaging scientists and raising awareness and responsibility among them, to prevent their knowledge in legitimate scientific disciplines to be diverted for unintended malicious purposes, and to strengthen frameworks within which to prevent the spread of sensitive information and to promote collaborations to advance common non-proliferation objectives.
> [and that]
> 5. Chemical, biological, radiological and nuclear research and applications are receiving growing attention in this perspective. Education and training are becoming increasingly important, notably in areas where the knowledge and expertise are rapidly advancing [11].

The CBRN security paradigm has further been endorsed within the context of collective security, something evident in the activities of the North Atlantic Treaty Organisation (NATO). Starting in 2006, NATO launched its system of Centres of Excellence (COE), international military organisations that train and educate leaders and specialists from NATO Member and Partner Countries [12]. There are 24 NATO COEs covering a wide variety of areas such as civil-military operations, cyber defence, military medicine, energy security, naval mine warfare, defence against terrorism, cold weather operations, and counter-IED. The scope of work of NATO COEs includes but is not limited to:

- Assisting in doctrine development;
- Identification of lessons learned;
- Improvement of interoperability and capabilities;
- Testing and validating concepts through experimentation.

The NATO Joint CBRN Defence COE became officially operational in 2007 [13]. It is a NATO military body and a multi-national organisation featuring the following Member Countries: Austria, Czech Republic, France, Germany, Greece, Hungary, Italy, Poland, Romania, Slovakia, Slovenia, the United Kingdom, and the USA. The NATO Joint CBRN Defence COE offers recognised experience and expertise in such areas as:

- NATO Transformation Process;
- Operational Support by providing a CBRN Defence advice; and
- Support of CBRN Defence Education, Training and Exercises [14].

Another milestone in the evolution of the CBRN security paradigm was the launch in 2010 of the EU CBRN Centres of Excellence Initiative. Initially the legal basis for the EU CBRN Centres of Excellence Initiative was Regulation (EC) No 1717/2006 of 15 November 2006 establishing an Instrument for Stability (IfS) which was superseded in 2014 by the Instrument contributing to Stability and Peace (IcSP), the latter currently being managed by the European Commission's Directorate-General for International Cooperation and Development (DG DEVCO). The primary aim of the EU CBRN Centres of Excellence Initiative is to address the need to strengthen the institutional capacity of Partner Countries to mitigate CBRN risks through, *inter alia,* enhancing local ownership, fostering local expertise, and promoting long-term sustainability [15]. To this end, the Initiative is structured in a way that avoids a traditional top-down approach: it is centred on a worldwide network of local experts and collaborating partners.

The EU CBRN Centres of Excellence Initiative is currently present in more than 55 Partner Countries grouped around eight EU CBRN Centres of Excellence Regional Secretariats, located mainly in Africa, Asia, and the Middle East. At the national level, each Partner Country appoints a National Focal Point for the EU CBRN Centres of Excellence Initiative. The National Focal Point is responsible for supporting the creation of an inter-ministerial CBRN National Team, comprising relevant representatives from ministries, national agencies and institutions representing relevant communities involved in CBRN risk mitigation, e.g. police and law enforcement, defence, the judiciary, government officials dealing with science, technology, industry, and trade, civil protection and emergency services, universities and research centres, public laboratories, intelligence services, and diplomats.

The EU CBRN Centres of Excellence Initiative seeks to facilitate regional cooperation among Partner Countries, in order to enhance their CBRN risk mitigation capabilities. To this end, a specific cycle of activities has been defined, starting from the Partner Countries' needs assessment at the local level (bottom-up approach) to the definition of project objectives, the selection of implementers, the actual project implementation, the monitoring of activities, and evaluation of project outcomes and impacts overall.

3 CBRN Security: Next Steps

CBRN security is a *new organising principle* of the international multilateral relations that deal with international security in a holistic approach on CBRN knowledge and materials, and a possible mechanism for doing so it is through the so-called "*soft law*".

Given the multifaceted security challenges arising from the intersection between complex globalising dynamics and the rapid pace of advancement of science and technology, manifested in the diffusion of knowledge and materials outside their traditional domains, it is vital to keep the momentum of dialogue and interaction among the communities dealing with biological security, chemical security, and radiological/nuclear security.

A possible end goal of such an enhanced interaction could be a common methodology for addressing CBRN risks. From a functional point of view, the CBRN domains are the skeleton of the CBRN security concept but they are not exclusive. In perspective, CBRN security needs to be interpreted in a holistic way by including safety issues, possible future challenges, such as the problem of Improvised Explosive Devices (IEDs) chemical precursors, cyberattacks against CBRN critical infrastructures, and the proliferation of sensitive tacit knowledge. The EU CBRN Centres of Excellence Initiative, the EU Community of Users on Secure, Safe, and Resilient Societies [16] and the IAEA NSSC-Network, among others, could serve as reference models in the elaboration of a CBRN risk mitigation methodology.

One observation that merits specific attention is the fact that at present the CBRN security initiatives remain largely fragmented, not harmonized, limited in geographical scope, and focusing on a different range of stakeholders. Addressing these and other related obstacles requires a further adjustment of the CBRN security paradigm through, *inter alia,* institutionalised dialogue and focused deliberation and hence, the transformation of the CBRN security concept and practices into a new "*formal Institution*".

Indeed, CBRN security might be institutionalised at a lower level with respect to the international treaties dealing with arms control and disarmament, which do not cover CBRN risk mitigation. The reference framework for doing so could be the so-called counter proliferation initiatives, such as the 2003 Proliferation Security Initiative [17]. Another possible reference framework model for a formal CBRN security Institution could be the establishment of an *ad hoc* "*CBRN UN-Governmental Group of Experts (CBRN UN-GGE)*", similarly to the UN-GGE launched for the global Information and Telecommunication security [18], or the development of an arrangement tailored on the so-called Intergovernmental Panel on Climate Change (IPCC) [19].

The CBRN UN-GGE could be tasked with the development of codes-of-conduct, guidelines, principles and standards on CBRN risk mitigation. It could also serve as a "*clearance platform*" for discussion and data sharing, including the exchange of best practices and lessons learned, as well as the international harmonization of the national laws/regulations and national governance systems on CBRN security.

The CBRN UN-GGE could also be responsible for the administration of a database with relevant information, in order to facilitate multi-stakeholder engagement. As kick-off, a simple move could be to set a common digital agenda for all CBRN initiatives (e.g. workshops, fact finding missions, professional association gatherings, etc.), which could play an essential role in informing the formulation of an envisaged "*CBRN Global Action Plan*". Each State might provide national assistance and technical cooperation, as appropriate, to the CBRN UN-GGE, and formulate, if not already in place, a National Action Plan (NAP) that is compatible and consistent with the measurable objectives of the CBRN UN-GGE.

States' adherence to the CBRN UN-GGE needs to be un-discriminatory, voluntary and not restricted to the States Parties to international disarmament and arms control agreements, such as the NPT, CWC, and BTWC. A close collaboration with those and other existing international or multilateral instruments needs to be explored and actively pursued.

Furthermore, a CBRN UN-GGE could pave the way to adopt a *new UNSC Resolution* (including and generalizing the UNSCR 1540) demanding the enforcement of laws and regulations at national levels against the deliberate and criminal uses of CBRN expertise, materials and technologies.

References

1. United Nations, Security Council, *Resolution 1540*, S/RES/1540 (2004), 28 April 2004. Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540%20(2004) (accessed 3 April 2017).
2. For further information see 1540 Committee: Security Council Committee Established Pursuant to Resolution 1540 (2004)*, General Information* available at http://www.un.org/en/sc/1540/national-implementation/general-information.shtml (accessed 4 April 2017).
3. For further information see 1540 Committee: Security Council Committee Established Pursuant to Resolution 1540 (2004), *Assistance*, available at http://www.un.org/en/sc/1540/assistance/general-information.shtml (accessed 4 April 2017).
4. International Atomic Energy Agency, *IAEA Nuclear Security Plan for 2014–2017,* available at http://www-ns.iaea.org/security/nuclear-security-plan.asp?s=4 (accessed 4 April 2017).
5. International Atomic Energy Agency, *IAEA Nuclear Security Plan for 2014–2017,* available at http://www-ns.iaea.org/security/nuclear-security-plan.asp?s=4 (accessed 4 April 2017).
6. Further information about the International Network for Nuclear Security Training and Support Centres. 2017. – NSSC Network is available at http://www-ns.iaea.org/security/nssc-network.asp?s=9&l=76 (accessed 4 April 2017).
7. Address by Ambassador Ahmet Uzumcu, Director General of the Organisation for the Prohibition of Chemical Weapons (OPCW), *Perspectives in the Context of the Third Review Conference of the Chemical Weapons Convention,* IUPAC Workshop, 'Trends in Science and Technology Relevant to the Chemical Weapons Convention (CWC)', 20 February 2012, Spiez, Switzerland. Available at https://www.opcw.org/fileadmin/OPCW/ODG/uzumcu/IUPAC_DG_Statement_Feb_2012.pdf (accessed 4 April 2017).
8. Organisation for the Prohibition of Chemical Weapons, *Report of the Third Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention*, RC-3/3, 19 April 2013, The Hague. Available at https://www.opcw.org/fileadmin/OPCW/CSP/RC-3/en/rc303__e_.pdf (accessed 1 April 2017).
9. United Nations, The Eighth Review Conference of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Geneva, 7–25 November 2016, *Final Document*, BWC/CONF.VIII/4. Available at http://www.unog.ch/__80256ee600585943.nsf/(httpPages)/57a6e253edfb1111c1257f39003ca243?OpenDocument&ExpandSection=3#_Section3 (accessed 4 April 2017).
10. United Nations, The Eighth Review Conference of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Geneva, 7–25 November 2016, *Final Document*, BWC/CONF.VIII/4. Available at http://www.unog.ch/__80256ee600585943.nsf/(httpPages)/57a6e253edfb1111c1257f39003ca243?OpenDocument&ExpandSection=3#_Section3 (accessed 4 April 2017).
11. G8, *Recommendations for a Coordinated Approach in the Field of Global Weapons of Mass Destruction Knowledge Proliferation and Scientist Engagement*, 2009. See http://www.g8.utoronto.ca/summit/2011deauville/2011-gpassessment-en.html#engagement (accessed 4 April 2017). Full text of the Recommendations is available at http://www.mofa.go.jp/policy/economy/summit/2009/report_gp-a2.pdf (accessed 4 April 2017).

12. For further information see North Atlantic Treaty Organisation, *Centres of Excellence,* available at http://www.nato.int/cps/en/natohq/topics_68372.htm (accessed 4 April 2017).
13. For further information see JCBRN Defence COE*, History of JCBRN Defence COE,* available at http://www.jcbrncoe.cz/index.php/history (accessed 4 April 2017).
14. For further information see JCBRN Defence COE*, JCBRN Defence COE Mission and Tasks,* available at http://www.jcbrncoe.cz/index.php/organization-65/mission-64 (accessed 4 April 2017).
15. Further information on the EU CBRN Centres of Excellence is available at http://www.cbrn-coe.eu/ (accessed 4 April 2017).
16. European Commission, Directorate-General for Migration and Home Affairs (DG HOME), *A Community of Users on Secure, Safe, and Resilient Societies (CoU): Mapping EU Policies and FP7 Research for Enhancing Partnerships in H2020,* available at https://www.cbrn-networkofexcellence.org/filter-results-3/publication (accessed 4 April 2017).
17. Further information on the Proliferation Security Initiative is available at http://www.psi-online.info/Vertretung/psi/en/01-about-psi/0-about-us.html (accessed 4 April 2017).
18. For further information see United Nations Office for Disarmament Affairs, *Developments in the Field of Information and Telecommunications in the Context of International Security,* available at https://www.un.org/disarmament/topics/informationsecurity/ (accessed 4 April 2017)
19. For further information on the Intergovernmental Panel on Climate Change, see http://www.ipcc.ch/organization/organization.shtml (accessed 4 April 2017).

Selected Issues of Cyber Security Practices in CBRNeCy Critical Infrastructure

Stanislav Abaimov and Maurizio Martellini

Abstract The article highlights the strong relevance and crucial importance of cyber security defence and response capacities in CBRNeCy assets and management, including in ICS and SCADA systems. Based on the overview of the recent cyber security publications and available information on global cybercrime, it reviews types of cyber and cyber related physical attacks on CBRN Industrial Control Systems; classifies attack types and defence techniques by network layer of attack; analyses security testing approaches based on knowledge of the targeted system, and evaluates types of due protection. The proper combination of existing physical security measures and cyber security testing exercises is considered, by the authors, as one of the most efficient ways to ensure sufficient protection against increasing global cyber threats to CBRNeCy infrastructures. The paper deals also with the best security practises, and contains enumeration of the globally recognized testing techniques and methodologies required to design effective multi-disciplinary security measures, thus providing a substantial ground for their practical implementation in the areas of concern.

Abbreviations

APT	Advanced Persistent Threat
BYOD	“Bring your own device”
CBRNe	Chemical, Biological, Radioactive, Nuclear and Explosives
CBRNeCy	Chemical, Biological, Radioactive, Nuclear, Explosives and Cyber

S. Abaimov (✉)
University of Rome Tor Vergata, Rome, Italy
e-mail: stanislav.abaimov@uniroma2.it

M. Martellini
University of Insubria and Landau Network Fondazione Volta, Como, Italy
e-mail: maurizio.martellini@uninsubria.it

M. Martellini, A. Malizia (eds.), *Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges*, Terrorism, Security, and Computation,
DOI 10.1007/978-3-319-62108-1_2

DoS	Denial of Service
DDoS	Distributed Denial of Service
DMZ	Demilitarised Zone
ICS	Industrial Control System (or Systems)
IEEE	Institute of Electrical and Electronics
PLC	Programmable Logic Controller
RFID	Radio-frequency identification
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
UN	United Nations
US CERT	United States Computer Emergency Readiness Team

1 Introduction

In the age of global communication, sophisticated technologies and widely available cyber tools, industrial, corporate and political espionage merged with cybercrime has become an issue of significant global concern. The information security has been on the UN agenda since 1998, when the Russian Federation first introduced a draft resolution in the First Committee of the UN General Assembly. It was adopted without a vote (A/RES/53/70).[1] The UN has raised it high on the international agenda, calling cyber security as one of the pillars for maintenance of international peace and stability and stressing the need for a universal cyber security legal framework, global cyber diplomacy and internet governance.[2]

In the 2015 *Report of the Group of Governmental Experts on Development in the Field of Information and Telecommunications* the UN Secretary-General notes: "Few technologies have been as powerful as information and communications technologies in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can only be achieved through international cooperation, and the foundation of this cooperation must be international law and the principles of the UN Charter."[3]

Due protection, early warning and effective response are especially crucial in chemical, biological, radioactive, nuclear and explosives (CBRNe) facilities, whose damage not only entails country-level process disruptions, but also endangers human existence globally.

[1] http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70

[2] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 68th General Assembly, A/68/98, June 2013, pp. 8–11.

[3] http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

Ensuring the serene existence of humanity and advancing technological progress by using a wide range of materials and agents, the above-mentioned facilities have one area in common: automation and control systems, which coordinate the whole process. Invention of computers promoted their successful use in manufacturing and eventually in the management itself, thus enhancing the quality and speed of the production cycle, but escalating danger at the same time.

Both computer and industrial control systems (ICS) have evolved over the decades. Having emerged initially for different needs and in different centuries, they merged together in the later decades and acquired very similar architectures. From the time when, in 1936, the first principle of the modern computer was proposed by Alan Turing in his paper "On Computable Numbers", the computer has materialized, initially as a calculation machine, and made a quantum leap in its functions and use.

The world's first stored-program computer was built at the Victoria University of Manchester and ran its first program on 21 June 1948. Although considered "small and primitive", it was the first working machine to contain all elements essential to a modern electronic computer. In April 1951, the newly developed LEO I computer became operational and ran the world's first regular routine office computer job. In 1949, the first integrated circuit was invented; its mass use and the following invention of the microprocessor in 1970, led to a fast popularization of personal and industrial computers. The modern computer architecture, based on the microprocessor technology, is widely used in ICS and industrial workstations, office and personal computers, smartphones and embedded devices.

It is also worth mentioning that the automatic feedback control systems have been known and used for more than 2000 years. Some of the earliest examples are water clocks described by Vitruvius and attributed to Ktesibios (circa 270 B.C.). About 300 years later, Heron of Alexandria in his works "Automata" and "Pneumatica" described a range of mechanisms which employed a variety of feedback mechanisms. The term *feedback* was introduced in the 1920s by radio engineers to describe parasitic, positive feeding back of the signal from the output of an amplifier to the input circuit. This feedback mechanism is the basic principle in any Control System [1].

Early minicomputers were used in the control of industrial processes since the beginning of the 1960s. Thus, the IBM 1800 was an early computer that had input/output hardware to gather process signals in a plant for conversion from field contact levels (for digital points) and analogical signals to the digital domain.

In 1950, the Sperry Rand Corporation built UNIVAC I, the first commercial data processing machine. The machine tools began to be automated in the 1950s with Numerical Control (NC) using punched paper tape. This lately evolved into Computerized Numerical Control (CNC). The first industrial control computer system was built in 1959 at the Texaco Port Arthur, Texas, refinery with an RW-300 of the Ramo-Wooldridge Company [18].

Prior to the 1950s, the predominant control systems were analogical-based or were simply "on/off" controls due to switch or relay positions [8]. The first reported use of digital control systems (DCS) took place in 1956, and was placed into operation in 1959 at the Port Arthur (Texas) refinery and in 1960 at the Monsanto ammonia plant in Luling, Louisiana. These systems were supervisory in nature and the individual loops were controlled by conventional electrical, pneumatic or hydraulic controllers, but monitored by a computer.

It was in 1959 when the researchers initiated to design a digital computer that could fully control the industrial controls process. In the late 1960s, specialized process control computers arrived on the scene offering direct digital control, so that the computer architecture could implement a discrete form of a control algorithm [20]. However, research and technological advancements of these systems were expensive and they were superseded by the cheaper microcomputers of the early 1970s.

(IEEE Communications Surveys & Tutorials [13])

Supervisory controls and data acquisition (SCADA) history is rooted in distribution applications, such as power, natural gas, and water pipelines, where there is a need to gather remote data through potentially unreliable or intermittent low-bandwidth/high-latency links. SCADA systems use open-loop control with sites that are geographically dispersed. A SCADA system uses Remote terminal/telemetry units (RTUs), to send supervisory data back to a control center. Most RTU systems have some limited capacity to handle local controls while the master station is not available. However, over the years RTU systems have grown more and more capable of independently handling local controls.

Programmable logic controller (PLC) evolved to replace racks of relays in ladder form. The latter were not sufficiently reliable, were difficult to rewire and to diagnose. PLC control tends to be used in very regular, high-speed binary controls. Originally, PLC equipment did not have remote control racks, and many could not perform more than rudimentary analog controls. Only physical access could compromise the security. With the introduction of electronic, and later computer architecture, the remote access created new attack vectors and patterns.

Distributed Control Systems (DCS) generally refer to the particular functional distributed control system design that exist in industrial process plants (including CBRNe agents). The DCS concept came about from a need to gather feedback data and control the systems on a large scale in real time. It is common for loop controls to extend all the way to the top level controllers in a DCS, as everything works in real time. These systems evolved from a need to extend control systems beyond just a small cell of control units.

> The definitions of different typed of control and information processing modules are blurring as time goes on (IEEE [12]). The technical limits that drove the designs of these various systems are no longer as much of an issue. PLC platforms can now perform as a small DCS, being sufficiently reliable for SCADA systems to manage closed loop control over long distances.

Advancing technologies have merged computers and ICS as one. Remote access to controlled equipment, and even to a controlled facility, has become a standard for the majority of industries, and the issues of cyber security have become crucial. The series of critical infrastructure disruptions, caused by cyber attacks, alerted defence forces and sparked the cyber security scrutiny.

Significant interest in potential cyber-related disaster events started to emerge in the mid-1990s (e.g. the US Security in Cyber-Space (GAO 1996); Winn Schwartau "Information Warfare: Chaos on the Information Superhighway" (Schwartau 1994). In 1991, Jim Bidzos, a security industry pioneer, originated the much-repeated phrase: "Digital Pearl Harbor". Another peak of concern was in 1998 and 1999 over fears of the Y2K bug [6]. It was born on the assumption that the older versions of computer systems were not programmed to cope with date presentation in the upcoming millennium and would fail to function in a designated manner [23]. This concern has not lost its relevance nowadays.

One of the earliest publicly announced events related to the CBRN infrastructure vulnerability to cyber attacks occurred in January 2002. The malware successfully breached the perimeter network defences at Ohio's Davis-Besse nuclear power plant (tough the employees claimed the network was protected by a firewall), infiltrated a private computer network and disabled a safety monitoring system for nearly 5 h.[4]

In October 2006, the attackers gained access to computer systems at a Harrisburg water treatment plant in the USA. The ICS network was accessed after an employee's laptop computer was compromised via the Internet, and then used as an entry point to install a malware that was capable of affecting the plant's water treatment operations.

In October 2008, the derailment of the tram in the city of Lodz injured 12 people. The attacker used the repurposed television remote control to change track points through Infrared sensor. He was also suspected of having been involved in several similar incidents. The problems with the signaling system on Lodz's tram network were detected when a driver was attempting to steer his vehicle, the rear wagon of the train derailed and collided with another passing tram.[5]

The 2010 event in Iran confirmed that information technology could be used not only to trigger remote CBRN attacks,[6] but could be also perceived as a direct threat to physical CBRN ICS equipment. Stuxnet was the first malware to infiltrate and cause physical disruption in multiple ICSs in a CBRN facility (the uranium enrichment

[4] http://www.securityfocus.com/news/6767

[5] https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html

[6] https://www.cia.gov/library/reports/general-reports-1/terrorist_cbrn/terrorist_CBRN.htm

plant) and multiple other facilities over 2 years with similar equipment.[7] This malware was a wake-up call, which united cyber security community and CBRN defence experts by the same goal of protecting the planet [24].

In 2011, the Trojan "Poison Ivy" was used to collect intellectual property from 29 international chemical companies. It was one of the largest industrial espionage attempts in history, raising the awareness of cyber security specialists in the topic of cyber security in critical infrastructure.

In 2014, the Malware Shamoon wiped 30,000 workstations in Saudi Aramco's corporate network, raising concern over cyber attacks that can bypass firewalls and intrusion detection systems to physically affect technology networks in a large scale.[8]

In 2014, the 13 different types of malware disguised as ICS/SCADA software updates (e.g. Siemens Simatic WinCC, GE Cimplicity, and Advantech) were detected in the spear-phishing emails. After a due forensic investigation, the malware was identified as the re-purposed banking Trojan, aiming to collect private information and credentials.[9] This event confirmed the capabilities of ICT malware to be used against industrial networks.

In December 2015, the Denial of Service in a power plant and multiple substations in Ukraine triggered a power outage. In February 2016, it was acknowledged that BlackEnergy3 malware was used for the cyber attack.[10]

The Verizon data breach digest [21] describes several attacks investigated by the company, including one aimed at the systems of an unnamed water utility referred to by Verizon as the Kemuri Water Company.

In October 2016, the Domain Name System provider Dyn was targeted by a DDoS attack, whose systems support major websites and online services. The investigation is conducted by the US Homeland Security. The attackers have not been identified yet. J. McAfee claims, "The massive cyber attacks that temporarily disabled websites including Twitter, Reddit and *The New York Times* offline may be a precursor to a "cyber atomic bomb"". Several security experts believe the attacks are part of tests designed to probe for vulnerabilities ahead of a much larger attack.[11]

The events listed above indicate a constant evolution of attack capabilities of threat actors. There is no single solution to secure critical infrastructures against cyber-attacks, and hence several layers of defence should be set [4]. Based on the approaches to physical and operational security and safety, this article explores comprehensive cyber security applications and strategies related to ICSs, implemented in critical infrastructure that uses CBRNe agents and technologies.

[7] http://www.computerworld.com/s/article/9226469/Iran_confirms_cyberattacks_against_oil_facilities

[8] http://www.darkreading.com/attacks-breaches/banking-trojans-disguised-as-ics-scada-software-infecting-plants/d/d-id/1318542

[9] http://www.darkreading.com/attacks-breaches/banking-trojans-disguised-as-ics-scada-software-infecting-plants/d/d-id/1318542

[10] http://www.ibtimes.com/us-confirms-blackenergy-malware-used-ukrainian-power-plant-hack-2263008

[11] http://europe.newsweek.com/dyn-north-korea-bureau-121-ddos-hackers-internet-attacks-513098?rm=eu