Band 3 / 2018

Tomorrow's Technology

A Double-Edged Sword

Anton Dengg (Ed.)

Schriftenreihe der
Landesverteidigungsakademie

Schriftenreihe der
Landesverteidigungsakademie

Anton Dengg (Ed.)

Tomorrow´s Technology

A Double-Edged Sword

3/2018
Vienna, March 2018

Imprint:

Copyright, Production, Publisher:
Republic of Austria / Federal Ministry of Defence
Rossauer Lände 1
1090 Vienna, Austria

Edited by:
National Defence Academy
Institute for Peace Support and Conflict Management
Stiftgasse 2a
1070 Vienna, Austria

Schriftenreihe der Landesverteidigungsakademie

March 2018
ISBN 978-3-903121-31-7

Printing:
ReproZ W 18-1248
Stiftgasse 2a
1070 Vienna

Content

The opinions expressed in the articles are those of the authors'. The articles are printed with the authors' permission.

The publisher wants to thank:

Anna Rass, Anna Pichler, Andrea Prerad, Florian Koller, Michael Zinkanell, Christoph R. Cede, André Gazsó (Dr.), Andrea Grausenburger, Austrian Armed Forces Language Institute

for her diligent proofreading.

Abstract

New technologies have always influenced societies. They have not only entailed advantages. Revolutionary technologies have been misused and, in this way, impacted means and methods used in armed conflict, thus changing strategies as well as tactics. Similarly, threat scenarios will change in the face of the ever more speedily increasing technological progress.

Nano- and biotechnology provide for promising changes in future society. The possibilities of miniaturization give reason to expect huge transformations in robotics. Societies spearheading these upcoming complex developments will also play a leading part in global security policy. Competition has already started worldwide and will heat up in the future.

As the result of a project by the Institute for Peace Support and Conflict Management (National Defence Academy, Vienna), this book intends to outline the future complexity of the individual research areas of nano- and biotechnology and robotics.

At the same time, challenges lie ahead concerning international legislation. Efforts in this area and ways of dealing with increasing complexity are discussed in the final chapters.

Possible consequences of these new areas of technology complete this publication.

Foreword

We are living in „times of VUCA“, as Herbert Saurugg explains in his noteworthy article on page 270 of this book, meaning times of volatility, uncertainty, complexity, and ambiguity. Another contributor to this volume, Michael Fredholm, states that we cannot make serious forecasts and that the best we can achieve with regard to new technology is Early Warning and Situational Awareness as well as the implications thereof.

These two statements are indicative of the times we live in and hint at the events we might be in for. Discussions are ongoing on whether the technological changes we are facing and already witnessing should be considered evolutionary or revolutionary. At any rate, Nano-/Bio-/Information Technology, in combination with Robotics, Miniaturization and Artificial Intelligence, has a significant impact on politics, the economy, society and security. However, is this already common knowledge or still only a top priority issue for the elites of society?

Developments with regard to converging technologies as well as their impacts are and, no doubt, should be a research topic of the Institute for Peace Support and Conflict Management at the Austrian National Defence Academy. Thus, we organise expert talks and conferences to which specialists with outstanding knowledge and understanding are invited. Not only do we try to promote academic discourse, but we also work to contribute to the dissemination of our results and conclusions.

This book provides an excellent overview of recent developments regarding converging technologies. Several articles deal with possible impacts of these technologies in strategic or even philosophical terms, while others refer to operational aspects. Special focus is laid on (possible) impacts in the military sphere. “New“ or “converging technologies“, as they are largely referred to in this book, provide new opportunities for state and non-state actors –for better or worse. Consequently, the question of

how to regulate or control these new developments is of outstanding importance.

One pressing question emerges between the lines, namely "Who or what can/should take the final decision?" Can a computer or a „system of systems" take vital decisions or should they be left to humans? This aspect will dominate future discussions and research acitivities. Some questions are touched upon in the present volume–so as to stimulate further discussion. Last but not least, readers of this book may find the gloassary on the initial pages helpful.

Finally, I want to thank all the authors, contributors and, especially, Colonel Dengg for their great work, and congratulate them on the publication of this book.

Walter Feichtinger

1 Glossary[1]

Artificial Intelligence[2]

The capability of a machine to imitate intelligent human behaviour.

Automatic vs. Autonomous [3]

It is very difficult if not impossible to draw a line between 'automated' and 'autonomous' functions. The word 'automatic' is often used for individual functions, but 'autonomous' is used for an assembly of several "automatic" functions. Subcategories might be considered (highly automated, semi-autonomous, fully autonomous etc.).

Automatic/Automated system vs. Autonomous system[4]

An automated or automatic system is programmed to logically follow a predefined set of rules with predictable outcomes, e.g. the Phalanx anti-ship missile defence system, or a remotely piloted aircraft system programmed to return to a fixed point after a signal outage.

An autonomous system is capable of understanding higher-level intent and direction.

From this understanding, as well as a sophisticated perception of its environment, such a system is able to take appropriate action to bring about a desired state. It is capable of deciding on a course of action from among a number of alternatives, without depending on human oversight and control, although these may still be present. Although the overall activity of an autonomous system will be predictable, individual actions

[1] Please note that the following definitions are meant to contribute to the ongoing discussions as no consensus regarding the relevant definitions used by the international community exists. For further discussion see article of Peter Steiner in this book.

[2] Merriam-Webster Encyclopedia. In: https://www.merriam-webster.com/dictionary/Artificial%20intelligence accessed on 31 August 2017.

[3] International Committee of the Red Cross. Autonomous Weapon Systems. Implications of Increasing Autonomy in the Critical Functions of Weapons. Versoix, Switzerland 2016.

[4] Ibid.

may not be (i.e. the system does not merely follow a pattern of rules in a predictable way).

Autonomous Weapons System[5]

Any weapon system with autonomy in its critical functions. That is, a weapon system that can select (i.e. search for or detect, identify, track, select) and attack (i.e. use force against, neutralize, damage or destroy) targets without human intervention.

Weapon systems differ from their 'degree of autonomy', whether described as 'highly automated' or 'fully autonomous'. When distinguishing between automated and autonomous weapon systems, the former were programmed to a pre-defined set of rules with a predictable outcome, while the latter would be capable of deciding on a course of action from among a number of alternatives.

Big Data/Big Data Analytics[6]

Big Data represents information assets characterized by high Volume (quantity), Variety (type of content), Velocity (speed at which the data is generated), and Variability (inconsistency of the data and its accuracy).

Big Data Analytics can be defined as the specific Technology and Analytical Methods for its transformation into Value.

Conflict[7]

Competitive or opposing action of incompatibles; antagonistic state or action (as of divergent ideas, interests, or persons).

[5] Ibid.

[6] Working definition, see article of Fredholm, Michael. Nano-materials Technology: Convergence between Nanotechnology and Materials Science and Engineering. In: Tomorrow's Technology.

[7] Merriam-Webster Encyclopedia. In: https://www.merriam-webster.com/dictionary/conflict accessed on 31 August 2017.

Converging Technologies[8] Convergence occurs where scientific disciplines or key enabling technologies combine with other disciplines or enabling technologies and promise new or added value beyond synergies. Convergence is more than the combination of different disciplines or technologies. It leads to synergies, adding more value through convergence.
Critical Infrastructure[9] The physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in countries.
Drone See **Unmanned Aerial Vehicle (UAV)**
Effect[10] A change in the state of a system (or system element) that results from one or more actions, or other causes.
Hybrid Threat[11] The concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic,

[8] OECD: Directorate for Science, Technology and Innovation - Committee for Scientific and Technological Policy. 2014. Challenges and Opportunities for Innovation through Technology: The Convergence of Technologies. DSTI/STP(2013)15/FINAL. 25 September 2014: p.9. In: http://www.oecd.org/officialdocuments/publicdisplaydocument pdf/?cote=dsti/stp(2013)15/final&doclanguage=en accessed on 1 September 2017.

[9] European Commission. 2006. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection. COM/2006/0786 final – Official Journal C 126. 7 June 2007. In: http://eurlex.europa.eu/LexUriServ/Lex UriServ.do?uri=CELEX:52006DC0786:EN:NOT accessed on 31 August 2017.

[10] NATO: ACO. Comprehensive Operations Planning Directive. v1.0. 17 December 2010.

[11] European Commission. 2016. Joint Communication to the European Parliament and the Council: Joint Framework on countering hybrid threats a European Union response. JOIN/2016/018 final.

military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

Information Environment/Systems/Activities[12]

The Information Environment is defined as the virtual and physical space in which information is received, processed and conveyed. It consists of the information itself and information systems. (MC 422/3)

Information systems are socio-technical systems for the collection, processing and dissemination of information. They comprise personnel, technical components, organisational structures and processes that create, collect, perceive, analyse, assess, structure, manipulate, store, retrieve, display, share, transmit and disseminate information. (AJP-3.10)

Information activities are actions designed to affect information and/or information systems, performed by any actor. (AJP-3.10)

Internet of Things[13]

The Internet of Things (IoT) is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent

[12] NATO. MC 422/3 – NATO Military Policy on Information Operations. 8 July 2008.
[13] CERP-IoT - Cluster of European Research Projects on the Internet of Things. 2010. Vision and Challenges for Realising the Internet of Things. European Commission: Information Society and Media. March 2010. p.43. In: http://www.robvankranenburg.com/sites/default/files/Rob%20van%20Kranenburg/Clusterbook%202009_0.pdf accessed on 1 September 2017.

interfaces, and are seamlessly integrated into the information network. In the IoT, 'things' are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information 'sensed' about the environment, while reacting autonomously to the 'real/physical world' events and influencing it by running processes that trigger actions and create services with or without direct human intervention.
Interoperability[14] The will, common understanding and ability of actors to bridge differences in culture, organisation, procedures and technology to effectively and efficiently cooperate towards achieving a common goal.
Nanobiotechnology[15] Applies the tools and processes of nano/microfabrication to build devices for studying biosystems and applications in drug delivery, diagnostics etc.
Nanotechnology[16] A field of applied sciences and technologies involving the control of matter on the atomic and molecular scale, normally below 100 nanometers. Nanomaterials may exhibit different physical and chemical properties compared with the same substances at normal scale, such as increased chemical reactivity due to greater surface area.

[14] MNIOE/MNE 5. 2007. White Paper – Information Activities in Future Coalition Operations – A Comprehensive Approach from a Military Perspective; Final Draft v1.8. 31 May 2007.

[15] OECD. 2005. A Framework for Biotechnology Statistics. Paris. 2005. p.9. In: http://www.oecd.org/science/inno/34935605.pdf accessed on 4 September 2017.

[16] European Food Safety Authority: Nanotechnology. In: http://www.efsa.europa.eu/en/topics/topic/nanotechnology accessed on 30 August 2017.

Robot[17] An actuated mechanism programmable in two or more axes with a degree of autonomy, moving within its environment, to perform intended tasks.
Security:[18] The condition achieved when designated information, material, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure.
Unmanned Aerial Vehicle (UAV)[19] An unmanned aerial vehicle, commonly known as a **drone**, is a pilotless aircraft, in the sense of Article 8 of the Convention on International Civil Aviation, which is flown without a pilot-in-command on-board and is either remotely and fully controlled from another place (ground, another aircraft, space) or programmed and fully autonomous.

[17] International Standards Organisation. 2012. Robots and robotic devices. ISO/TC184/SC2.
[18] NATO. 2012. AAP-6 – Glossary of Terms and Definitions (03 October 2012).
[19] International Civil Aviation Organization (ICAO).b 2011. Unmanned Aircraft Systems (UAS). Montreal, Canada. Cir 328, AN/190. In: p.3. https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf, accessed on 4 September 2017.

2 General Reflections on Converging Technologies and Emerging Risks

New Technologies Meet New Challenges: Converging Technologies and Emerging Risks in the 21st Century

Anton Dengg

New technologies have always been a driving force for civilization in both a good and a bad way, but they have crucially influenced societies. Basically, technology should be seen as an asset in the daily life of humans. This was the inventors' original intention. Nevertheless, technology has always been misused as a weapon to harm people or - in a friendlier way - to win a war for good causes, such as freedom or democracy. Therefore, new technology is a double-edged sword.

Technology - an old and fascinating topic

Curiosity is a human characteristic and a main driving force for scientific research. This characteristic has contributed greatly to the evolution of mankind. People are always interested in future developments and how they will change their life. People's fascination with science fiction stories demonstrates their curiosity to look into a crystal ball to see the future. Jules Verne is one of the most famous science fiction authors who fascinated people with his stories that look into the future. In his novel *Paris in the Twentieth Century* (1863) Verne describes how Paris will look like in a hundred years. He portrays future comfort in Paris and talks about maglev trains, which are used as passenger transport systems, motorized carriages, electric door openers and windmills producing energy. Verne did not just use his imagination for these stories, but talked to different scientists and 'translated' their inventions into stories.

But in the last centuries there have been a lot of misjudgements: The future impact of many new developments has often been underestimated and misjudged. In 1893, for example, John Wanamaker, the US Postmaster General, claimed that in 100 years U.S. mail would still be delivered by mail coaches.[20] Also, in 1927 during the silent film era, Harry M. Warner, founder of Warner Brothers, asked "Who the hell wants to listen to the speech of actors?"[21] And another misconception came from Thomas Watson, Chief Executive Officer of IBM. He was convinced that there was a world market of perhaps five computers.[22]

All these misjudgements proove that interdisciplinary experts, especially in the field of security policy, should keep in mind Jules Vernes' approach of combining scientific results with imagination. Researchers in the field of security policy could, for example, create a team that keeps an eye on inventions, particularly technical inventions. An important task for those teams would be to review the possibility of misuse. The idea is not to demonize technological progress but rather that scientists have a closer look at converging technologies and to think about the future application of upcoming technologies. Possible impacts of technologies have to be part of the decision-making processes concerning the development of new security strategies and future threat scenarios. Even though people are curious about new technologies, they are afraid of possible negative side effects. As Carl Schmitt put it: "Each of the countless changes and revolutions in human history and developments has produced new forms and dimensions of political groups, destroyed former existing political structures, caused external and civil wars and has increased as well as

---

20 Kaku, Michio.5 2014. *Die Physik der Zukunft – Unser Leben in 100 Jahren*. Rowohlt Taschenbuch Verlag, p. 19.
21 Ibid.
22 Ibid.

reduced the amount of the organized political unities."[23] Technology has the potential for such a revolution.

Technology as a threat scenario of security policy

Apart from the obvious benefits of modern technology there is the need to focus especially on possible damages by malicious acts in the different technological fields. Especially in the field of security policy the benefits and dangers of new technologies are closely linked.

Technological developments always imply changing threats in security policy, therefore posing a challenge regarding countermeasures. According to the so-called Moore`s Law, "the complexity for a minimum component costs has increased at a rate of roughly a factor of two per year […]. Certainly over the short term this rate can be expected to continue, if not to increase"[24]. Therefore, from the perspective of a security policy analyst, Moore`s statement has a tremendous impact on the states' security policy.

Prompted by the changes in technology, conflict scenarios change as well. Although they do not reflect every technological factor, the challenge is that new technologies change political and military strategies and influence the tactics of armed forces. Moreover, new technologies imply greater strength of security forces, give additional momentum to new operations and tactics on the battlefield and influence states via hybrid threat and warfare.

---

23 Schmitt, Carl.1996.6 [1963] Der Begriff des Politischen. Text of 1932 with preface and three corollaries. p.4. Reprint of Edition 1963, Duncker & Humblot, Berlin 1996. p.46. Translated from German into English by Anton Dengg.

24 Moore, Gordon E. 1965. Cramming more components onto integrated circuits. *Electronics* 38 (8). In: http://web.eng.fiu.edu/npala/eee6397ex/gordon_moore_1965_article.pdf, accessed on 27 January 2017.

On the one hand, this could entail a transformation of security forces. But on the other hand, new technology could also change the character of an adversary. With the help of technological equipment, less trained non-state counterparts could harm more people with a smaller number of fighters, less equipment and fewer tools. Also, new technological devices enable adversaries to fight successfully even against a powerful state force. More creative adversaries using new technology and a mixture of sophisticated ideas could pose a bigger threat for state security forces and society than ever before.

A good example of the increasing influence of technology is the rise of the Internet, including all its connected applications. The Internet is both, boon and bane at the same time. On the one hand, we have to be grateful because, owing to the Internet, society enjoys many extraordinary benefits from innovative products; on the other hand the Internet is an excellent tool for causing harm all around the world. E.g. 2015 in Austria, cyber-crime has risen by 11.6 % compared to 2014.[25] The Austrian police categorize the cyber-crime threat scenario as an ongoing ever-increasing problem. Additionally, radical ideas, propaganda and possible targets are spread easily through the Internet and the organisation of terror attacks is facilitated. Currently, the Internet is a perfect tool for any kind of hostile activities. 25 years ago, nearly nobody has foreseen the big influence of the Internet for the threat scenario of states.

The Internet shows in a perfect manner that people can and will always misuse great inventions. This also confirms that technological development will not only change possibilities of state armed forces, but will also increase the power of non-state actors. A changed diverse threat scenario is the output of such new developments. Therefore, the threat analysis of

---

[25] Bundeskriminalamt (Austrian Federal Police Agency). 2015. *Cybercrime Annual Review 2015*, p. 9.

state actors is crucial to guarantee security of society. Additionally, a technological lead position means a political as well as an economic predominance in international politics. A special form of power projection would reveal a special form of asymmetry. Even U.S. Under Secretary of Defense for Acquisitions, Technology and Logistics mentioned, "My biggest concern right now is the overall erosion of our technology superiority …"[26].

There are several examples of 'civil' technological products that could be misused by people and therefore categorized as a threat:

- 3D Printing is on the way to revolutionize e.g. spare part production. In a few years it will be a common procedure when repairing a car to order small mechanical parts via the web and to get them delivered immediately through the 3D printer. First tests at the International Space Station already took place.[27] This could be easily misused by criminal elements, e.g. for the production of 'weapons without borders'.
- In the field of robotics and unmanned vehicles there are several considerations to use robots for delivering goods bought via the Internet. A lot of media articles report about the ideas of companies like *Amazon* or *Media Markt*. Attempts with drones or vehicles on the ground are still in progress.[28] Terrorists could use similar ideas for bringing bombs to a special destination. In

---

26 Wells, Jane. 2014. The man with the Pentagon checkbook. In: http://www.cnbc.com/id/101665010, accessed on 02 June 2014.

27 NASA. International Space Station's 3-D Printer. In: https://www.nasa.gov/content/international-space-station-s-3-d-printer, accessed on 31 January 2017.

28 Die Presse. 2016. Roboter bringt Einkauf bei Media-Markt nach Hause. In: http://diepresse.com/home/wirtschaft/international/5093481/Roboter-bringt-Einkauf-bei-MediaMarkt-nach-Hause?direct=5093728&_vl_backlink=/home/wirtschaft/economist/5093728/index.do&selChannel=, accessed on 31 January 2017.

combination with the dark web the distribution of all kinds of illegal goods can be easily imagined. The so-called 'dark net', a form of parallel Internet without any control possibilities, is well known as a trans-shipment center for all kinds of illegal business. 'Flexible' delivery possibilities with drones are not inconceivable. In July 2016, a German newspaper[29] reported about research in the field of underwater transportation systems with supersonic speed. This would change the international exchange of goods in a revolutionary way. But this technological product could also be turned into a new torpedo weapon system for navies or possibly even for terrorists. If states have similar weapon systems there is a first strike possibility with a hard time to determine the initiator.

- Stephen Hawking mentioned at the Zeitgeist Day 2015 in London that computers with its artificial intelligence overtake human beings in the next 100 years.[30] The misuse of such computers has to be expected as soon as they are on the market.
- Another example is the technology of exoskeletons. An exoskeleton is a kind of robotic suit to support the wearer for carrying e.g. heavy loads or to walk long distances without wasting human energy. Other people describe exoskeletons as wearable robots. The main idea of exoskeletons was to support handicapped persons. People with missing limbs can regain their physical quality of life with the help of an exoskeleton. But this is not science-fiction, it is reality. The military also is interested in this technology for their soldiers: "military exoskeletons are being tested by the

[29] Hegmann, Gerhard. 2016. In unter einer Stunde den Atlantik durchqueren. In: https://www.welt.de/wirtschaft/webwelt/article156778525/In-unter-einer-Stunde-den-Atlantik-durchqueren.html, accessed on 29 August 2017.

[30] The Austrian newspaper *Die Presse* cited Stephen Hawkings explaining future developments at the *Zeitgeist Day 2015* in London. Cf. http://diepresse.com/home/techscience/hightech/4733818/Hawking_Roboter-werden-Menschen-ueberlegen-sein, accessed on 28 March 2017.

U.S., China, Canada, South Korea, Great Britain, Russia and Australia, and these are just the projects that the public is aware of"[31].

Future and technology

There are a lot of books and papers dealing with scenarios of how the future will look like and how our daily life will change. Some of these scenarios picture the future 20 to 30 years ahead and some predictions occasionally even sound grotesque. Also, there is at best a fifty-fifty chance - maybe less - that these fantastic ideas come to life. An important question therefore is what are realistic scenarios about future trends in the field of technology and/or possible resulting threats that can be predicted?

New security challenges are inseparably linked to technological developments. The U.S. security strategy 2010 shows the importance of the current prevailing technological competition: "Our focus on education and science can ensure that the breakthrough of tomorrow will take place in the United States."[32] This sentence underlines the importance of the topic.

Considerable progress is achieved in the field of miniaturization, where constantly new appliances are manufactured. So far, the size of products has been restricted due to physical limits. In this field, nanotechnology will open up new possibilities and take progress to the next level. A progressive unification of different technological dimensions e.g. bio- and nanotechnology will be the next stage of a new development. Miniaturization at nearly any level – including nano-technology – adds to the improvement of products and has a huge impact not only on the civil

---

31 Marinov, Bobby: 19 Military Exoskeletons into 5 Categories. 2016. In: http://exoskeletonreport.com/2016/07/military-exoskeletons/, accessed on 30 March 2017.

32 The White House. 2010. *National Security Strategy*. Washington, p. 2.

but particularly the military application. International research pays special attention to robotics in general, in particular bionic robotics. Research work of several companies like Boston Dynamics show that efforts in this field have increased. Currently, limits exist in the development of products for military use, for example, because of their size, power supply and noise level; another example is the lifespan of batteries that limits the application of products. However, researchers are finding new solutions extremely fast.

To identify dangerous developments for society, decision-makers need to carefully monitor research in the field of new technologies in order to prevent or regulate any negative consequences for states and societies. Future developments cannot be stopped, and the rise of robotics is a good example. Soon, robots will part of our daily life. The increase of smart household appliances (coffee machines, lighting systems, toasters, vacuum cleaners etc.) and the Internet of Things are just initial steps towards the change of our daily life due to new technologies. Especially robotics will be of great significance for security forces because of the following reasons: Firstly, machines employed in danger zones can reduce casualties among security forces, which means a lower political risk for decision-makers. Secondly, some experts are convinced that emotionless autonomous robots make less incorrect decisions than armed human beings. Opponents hold that the reactions of emotionless robots could escalate violence in conflict areas while, for example, the emotional reaction of a security guard adds a human factor to the situation that could save lives. An autonomous robot with similar capabilities as a human would have to meet higher performance requirements but, at the same time, increase the calculability of missions. All of these considerations pose many new challenges, especially to the international law and those bound by it.

The specific importance of robotics for future developments is reflected by the high priority given to it by the EU. In June 2014, the EU started the world's biggest robotic program. 180 companies and research institutions are involved in this initiative.[33] Cooperation between the sectors industry, agriculture, health, transport, private security as well as household are to strengthen the position of Europe in the robotic industry.

Enormous potential is attributed to the fields of bio- and nanotechnology. Both branches will have tremendous influence on robotics. Nano-biotechnology, which is a combination of biology and nanotechnology, is expected to gain more and more influence. The Biotechnology Industry Organization lists a number of different applications for Nano-biotechnology, as e.g. "… miniaturizing biosensors by integrating the biological and electronic components into a single, minute component"[34]. Achievements in the field of biotechnology are accompanied by progress in the art of miniaturization and robotics. Revolutionary changes comparable to those linked to the emergence of the Internet have been predicted. Consequences for security forces and armed forces, including direct effects on weapon systems, are probable.

In the field of nanotechnology, researchers intervene in the atomic structure of materials. It focuses on the control of fundamental structures and the behavior of materials at the atomic and molecular levels. This enables the development of products with totally new properties and capacities. Because of potential security risks there is a high demand for

[33] European Commission, Press Release Database: EU launches world's largest civilian robotics programme – 240,000 new jobs expected; https://www.asktheeu.org/en/request/4322/response/13577/attach/html/5/H2020 projects 01.06.2017.csv.txt.html, accessed on 4 December 2017.

[34] Biotechnology Industry Organization. 2008. Guide to biotechnology. In: https://www.bio.org/sites/default/files/files/BiotechGuide2008.pdf , accessed on 29 March 2017.

responsible management in this field of research. Nanotechnology is seen as a key technology of the 21st century. Future developments in several other respects will result from it. There is consensus on that in the international community. In 2004 already, the European Commission was convinced that nano-technology would influence each EU citizen in one way or another.[35] The German Federal Ministry of Education and Research assumed for 2015 a world-wide added value of nano-technology of up to 3 trillion USD, which is a considerable part of the economy.[36] In particular, nanotechnology is expected to have a big influence on armed forces. New products for security forces can be used for purposes of attack, such as weapon technologies, as well as for defence purposes, such as personal protective equipment; as concerns countermeasures, security forces would have to react with the same kind of technology that is used by opponents, which could lead to a new arms race.

Most states recognize the importance of new technologies and engage in research and development concerning this varied field. The website 'Defense News'[37] which deals with new developments in armed forces claims that the U.S. should deal and invest increasingly in innovative materials and nanotechnology. This will improve military as well as economic possibilities.[38] An interview with General Michael Hostage, general of the United States Air Force and Commander Air Combat Command, has confirmed that United States Armed Forces focus their

---

35 European Commission. 2004. Towards a European Strategy for Nanotechnology. In: https://cordis.europa.eu/pub/nanotechnology/docs/nano_com_en_new.pdf ,accessed on 30 November 2016.

36 German Federal Ministry of Education and Research. 2009. nano.DE-Report 2009. Status Quo der Nanotechnologie in Deutschland. In: https://www.bmbf.de/pub/nanode_report_2009.pdf , accessed on 28 August 2014.

37 Defense News. 2017. In: www.defensenews.com, accessed on 25 August 2017.

38 Editorial: Funds for Innovation. 2013. In: http://www.defensenews.com/apps/pbcs.dll/article?AID=2013308110005, accessed on 8 April 2014.

interest on nanotechnology.[39] General Hostage has also stated his common interest in the new auspicious technology without giving further details about current developments.

In the future, nanotechnology is also expected to play a crucial role in agro-chemical industry. This was demonstrated in a conference in Israel 2014, in which Israeli Prime Minister Benjamin Netanyahu and Chinese Foreign Minister Wang Yi talked about closer cooperation in the future. The close teamwork in the field of nanotechnology between Israel and China was mirrored by a joint research center.[40] This could be an economic challenge for neighbor countries and other states.

Turkey is another example of states addressing new technologies. Turgut Senol, CEO of the technological center Turkey´s Teknopark in Istanbul[41] has called information-, nano- and biotechnology its strategic focal points. Its goal is for global companies to transfer their goods into this new center and position Turkey as an important technological hub.

The ability of states to use technological know-how as an instrument of power puts them in an advantageous position concerning security policy. This makes technological knowledge a crucial factor in security policy.

The rapid development of technology also spawns criticism. Eric Drexler, one of the leading researchers and biggest proponents of nanotechnology,

---

39Mehta, Aron 2014. Interview with General Michael Hostage, Commander US Air Force´s Air Combat Command. In: http://www.defensenews.com/apps/pbcs.dll/article?AID=2014302030017, accessed on 8 April 2014.

40 Opall-Rome, Barbara. 2014. China Expands Strategic Presence in Israel. In: http://www.defensenews.com/apps/pbcs.dll/article?AID=2014303010021, accessed on 8 April 2014.

41 Enginsoy, Umit, Ege Bekdil, Burak. 2012. Teknopark Instanbul To Generate $10B in Annual Business. In: http://www.defensenews.com/apps/pbcs.dll/article?AID=2012310090005, accesssed on 8 April 2014.

stated that the impact of new technologies in general will be huge and indicated the necessity of being prepared for those upcoming changes and challenges for societies, states and armed forces.[42] It has to be acknowledged, for example, that there is a relation between technology and legal issues. Upcoming new technologies should be on top of the agenda of national and international security policy committees. This was one of the outcomes of an informal expert meeting at the Convention on Conventional Weapons (CCW) in May 2014[43], where experts dealt with technological, ethical, social, legal, operative and military aspects of lethal autonomous weapons. Special attention was given to efforts in the field of emerging technologies in the area of lethal autonomous weapons systems.[44]

The main idea of the project

In 2015, the Institute for Peace Support and Conflict Management (IFK) of the National Defence Academy Austria (NDA) also concentrated on new technologies within a research project. One of the main driving factors for such a project was the fact that upcoming new technological products could be a danger to states and/or societies. Innovative products developed for the civilian market will sooner or later be applied for military use. The real challenge though does not consist in using those items to gain

---

42 Crichton, Michael. Beute. Karl Blessing. München 2002. In: www.randomhouse.de/content/edition/excerpts/408790.pdf, accessed on 8 April 2014.

43 United Nations. 2014. Meeting of the High Contracting Parties on the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. In: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/048/96/PDF/G1404896.pdf, accessed on 11 April 2017.

44 United Nations. 2014. Meeting of the High Contracting Parties on the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. In: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/048/96/PDF/G1404896.pdf?OpenElement, accessed on 26 May 2017.

a military advantage, but in the fact that new technologies might end up in the hands of the wrong people and be abused in political and military conflict situations. Therefore, the dual use of many technological products should be of considerable concern, especially to international organisations, such as the United Nations, NATO or the European Union. The confusing complexity of modern technology as well as its fast and dynamic development create a dimension of insecurity never witnessed before. Whether such complexity can be dealt with accordingly remains to be seen.

For this purpose, the Institute for Peace and Conflict Management launched a project involving national and international partners. The main idea was to analyze the current and upcoming agenda in the field of technology and define topics that have been dominating and are going to dominate the scene. What technologies will have a major impact in the coming years?

The project started with several workshops involving up to 20 experts from different countries where the best approaches to new technological products and their potential threats were discussed.

All experts agreed to use the term 'converging technology' instead of 'new technology', as many new technical devices and technologies in general are the results of existing knowledge but are now being applied in new ways. New technologies are based on past inventions that have been further developed and diversified. Thus, "converging technology" is the more appropriate term.

The first challenge was to agree on a definition of "new product". When could a product be called "new"? New products are usually invented years before they are put on the market, often for a different than the original

purpose. For instance, the first smartphone was produced by IBM in 1992.[45] With this smartphone it was possible to check emails, send faxes, list appointments and telephone numbers. Of course, one could also use it for phone calls and, what's more, this mobile device had a touchscreen. But it posed a major problem: The device was too complicated and expensive for the general market. In 2007, Apple launched the iPhone that combined all a mobile phone, a playback device for music, a computer and a camera in one single gadget. The biggest advantage was that this little computer was affordable and could be handled comfortably via touchscreen. This 'new' smartphone revolutionized handheld devices.

Another point of discussion was within what timeframe new trends should be researched. The experts came to the conclusion that it would not make sense to look beyond a timeframe of five to ten years. For several reasons: As already mentioned, new products are barely totally 'new'. Most technical knowhow and knowledge, and thus their products, are based on many years of basic research. Often, 'old' inventions are rediscovered after years and put to a new use, as in the case of the smartphone. The product was there, just waiting for someone with an idea of how to exploit it commercially, but the technology itself existed before. Consequently, there is a need for creative people who recognize the potential of new technology and implement innovative ideas. Apart from that, people must be ready for inventions. Right timing in line with the needs of the target group is crucial. Constantly tailored to market needs, the evolution of technological products is happening fast. Therefore, predictions of future developments in this area are very difficult. The project experts agreed on a timeframe of five to eight years.

---

[45] Steinmels, Dennis. 2012. Wie alles begann: Die Geschichte des Smartphones. In: http://www.pcwelt.de/ratgeber/Handy-Historie-Wie-alles-begann-Die-Geschichte-des-Smartphones-5882848.html, accessed on 30 March 2017.

Here are the main research questions:

- What are the necessary definitions in the area of new technologies?
- What technologies have the potential to influence the power projection of global actors in the defined timeframe?
- What legal consequences in terms of human rights and international law can be expected when using critical technologies in the military field, and what preventive, regulative measures are called for?
- What are the possible consequences of the use of converging technologies for future security policy threat scenarios and international conflict and crises management?

Results of the project were presented at the conference 'Converging Technologies and Emerging Risks – Challenges for the Security Sector' at the National Defence Academy in Vienna in 2016. Experts from technical and social science disciplines came together to share their ideas and opinions about the challenges of future threat scenarios arising from converging technologies. Their goal was to enhance the understanding of the 'other' fields of technology, to analyse medium-term future challenges and define possible threats for states and their security apparatuses. The present book summarises the outcome of the conference and the discussions held in the course of the project. The chapters mirror the panels at the conference, each providing in depth knowledge about the different fields of study: nano-, bio-, and information technology; robotic-, cognition- and ICT technology; nano-material technology and international perspectives.

NBIC – Viewpoint of the Austrian Defence Technology Agency

Michael B. Janisch

My statement should be seen as an introduction to the topic of converging technologies (CT). By CT we understand the synergistic combination of four major disciplines of science and technology also called '**NBIC'**. An acronym composed of the initial letters of:

- **Nano**science and nanotechnology
- **Bio**technology and biomedicine, including genetic engineering
- **Information** technology, including advanced computing and communications
- **Cognitive** science, including cognitive neuroscience

Each of these fields is currently **progressing** at a **rapid rate**. The concept of NBIC originated in the U.S. roughly twelve years ago and clearly aims at changing the whole society by implementing robots based upon converging technologies. Some years later, the European Union also began to focus on the issue. The difference lies in the inclusion of cognitive science and the focus on goals in the original concept, whereas the Europeans focus on NBI by looking at their economic advantages.

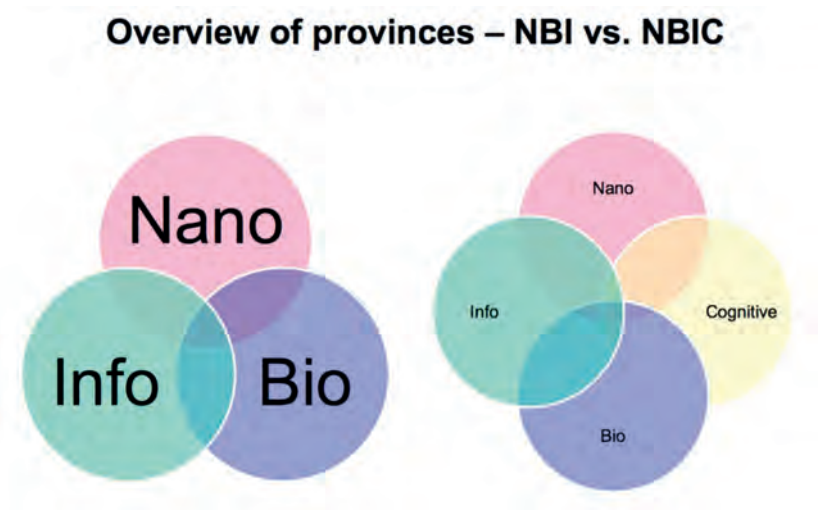


Figure 2: NBI vs. NBIC[46]

NBIC, of course, also plays an increasing role in defense technology. It aims at enhancing human physiology, and therefore may be called "**technological doping"**. The doping of soldiers with substances dates back to the beginnings of mankind. New technologies will most likely add significant capabilities to the warriors. The paramount goal is to gain and maintain **combat superiority** on the battlefield including air and sea in any type of conflict scenario. However, **technological superiority** is the crucial asset. Many the ideas may look like fiction but they are not. Of course we encounter different ethical and moral issues when looking at different projects: Some will not only 'enhance' the soldier but also the human being, due to a permanent and sometimes irreversible adaptation of the body. Bottom line: CT offers a vast bundle of measures of

[46]Janisch, Michael. 2016. Presentation at the Conference Converging Technologies and Emerging Risks. Austria: National Defense Academy.

physiological enhancement already provided by original disciplines of NBIC or a combinations thereof.

The study of U.S. material, in particular, reveals a number of planned CT-projects:

- Invasive micro drones (bio-fluidic chips) checking and reporting physiological condition
- Nano-diamonds delivering insulin for wound healing
- Add-on extremities (arms) controlled via brain-machine interfaces
- Invasive information projection on visors for risk reduction
- Increase of connectivity
- Direct non-invasive interfaces to bypass traditional input methods (aircraft, missiles etc.)
- Neurogenesis stimulation
- Sleep emulation…

Robotics is seen as the primary combination of informatics, mechanical engineering and cognitive sciences. Therefore, we should focus on one decisive point: the difference between human intelligence (HI) and artificial intelligence (AI). The main ethical dispute erupts when speaking about autonomous, AI-guided combat-buddies or 'killer-robots': Based upon which algorithm should machines kill or be allowed to kill humans? This is a highly emotional and difficult issue, which should be solved before such machines are developed. Of course in an all-out war nobody asks who was killed by an artillery grenade penetrating a house sheltering civilians and near-by combatants. The difficulties to spare own soldiers and non-combatants are the dominant issue.

In ten years' time, soldiers will be accompanied by a swarm of military robotic systems – robots. And they most likely are to accompany them on the ground, in the air and in water. Those robots are going to support

reconnaissance, for example, by equipping soldiers with multi-sensor packages with data-fusion. This results in the challenge of big data management as those systems will provide enormous amounts of data. As most data is trash, the assistance systems need perfect data management systems based on algorithms.

The second big task will be transportation. Here we will see systems carry personal equipment, ammunition, secondary weapons, batteries, bulk water, shovels etc., most likely in small containers, which means saving loading time. But also logistic tasks could be taken over in the future, e.g. by convoys of autonomous guided, driverless trucks and logistics bases with robots loading and unloading ships, trucks, containers etc.

As a third task robots may bring invisible light illuminators on to the battlefield. Thereby the actual firing of mortars or artillery could be avoided, especially if rules of engagement don't allow for their use or if collateral damage must be avoided by all means. Of course, these illuminators could be enhanced with passive detecting systems, like night vision goggles, or active devices, like blending lasers etc.

We might witness robots as passive situation trackers. Equipped with a set of sensors and guided by an algorithm, they will move autonomously in the area of operations and scan it via passive sensors. In case their algorithm detects strangers or enemies, the system sends a burst message to its controller and waits for being activated and tele-operated. They could also be used for fire-operation support or to target illuminators.

A further mission transferred to robots might well be medical evacuation. While this will most likely focus only on very special circumstances, such as radioactively contaminated areas, we have to accept that the human capability to lift and tie things at the same time is hard to imitate in a robot.

Already today we have a huge number of robots working in the field of explosive ordnance disposal (EOD) or improvised explosives device detection. Most of them are tele-operated as the sensor packages do not allow for more yet. But stand-off detection and automated visual identification based upon algorithms are steadily developing and offer a lot of future potential. Another development in this context is the splitting of tasks between various robot systems, e.g. on the ground and in the air.

The most complex and controversial issue are definitely combat-buddy systems. There are two different concepts. The first is a combat-support robot, currently in the shape of a small tank (APC) carrying a vast amount of different weapons or weapons systems, including machine guns, cannons, mortars, missile launchers etc. These systems are HI-controlled and allow especially the increase of fire support for infantry troops. The challenge for the commander in charge lies in coordinating fire and movement. In practice this development mirrors the combat technique of armored infantry when the dismounted commander has to co-ordinate fire and movement with his armoured personnel carriers. The differences are the terrain, the size, and the stand-off capability of the robot. The second concept is based on small, mostly chained vehicles carrying automatic rifles or usually sniper rifles. They are intended to provide precise fire support, for instance to neutralised specific objects or targets. As they are much smaller and their movement usually focuses on the vicinity, their mission can be much easier controlled, most likely by a single person. The small size makes them difficult to detect, especially if sealed with specialised materials that make them nearly undetectable.

Almost as fast as robotic systems anti-robotic systems are developing. Their weak points are that both brain and machinery are based on electronics and that tele-operated systems need huge amounts of telecommunication assets and frequencies. Electrical engineering plus information technology plus physics offers huge opportunities for electronic warfare as well as directed energy weapons. This includes, for

example, hacking, jamming, rendering useless or destroying robots, UAV, NBIC-systems as well as components thereof, like video systems, sensors etc.

Another CT option would be the combination of nanotechnology plus chemistry and physics for the enhancement of camouflage systems. Photo- and/or thermo-chrome cells could make those systems adaptable, depending on light conditions or temperature. Those cells would use zeolites able to 'store' information. Photochromism describes components that undergo a reversible photochemical reaction where an absorption band in the visible part of the electromagnetic spectrum changes dramatically in strength or wavelength. Thermochromism refers to the ability of substances to change its colour according to temperature. Zeolites are microporous, aluminosilicate commonly used as commercial adsorbents and catalysts. Further, nanotechnology is used to insert ceramic-like materials or photo-electrical cells into textiles in order to increase the protective function of uniforms or to allow for small-scale energy production when soldiers are exposed to the sun.

Last but not least I'll give you a brief overview of the Austrian NBI-capabilities and plans. The science unit for robotics and AI focus on autonomous systems with passive guidance. A desk for nanorobotics is planned therein. A science desk for nanotechnology has been earmarked within the sub-division for material technology. On 1st June 2016 we will open the Austrian Armed Forces Biotechnology Centre (BTZ). The new science desk for bioinformatics, ADTA's youngest technology discipline, was already implemented last year. The number of biologists has doubled and the number of disciplines multiplied within the past five years! The sub-division for technology forecast in the staff division for military technology is headed by a military biologist: we are starting to be prepared for NBI- systems monitoring and their potential development.

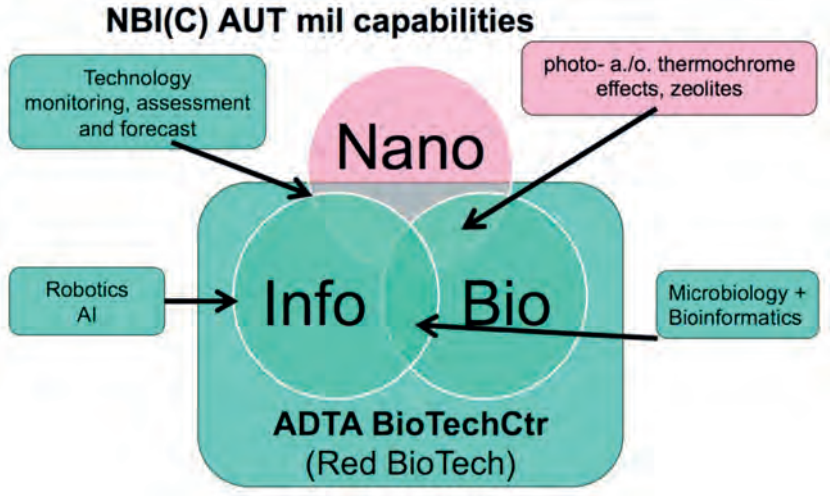


Figure 1: Austrian military NBI(C) capabilities[47]

Most of the current weaponry is still mostly based on war-proven technology of mid-20th century. Aircraft and helicopter capability as well as missile technology precision have remarkably increased but the technology itself is half a century old. Materiel developed in the 21st century will definitely add new technologies, including

- ‚Swarms' of **robotic systems** of all kinds at land, air and sea/ sub-surface
- **AI-** supported autonomous systems
- **HI-** controlled add-ons and combat support systems
- **Directed energy, electromagnetic** and **EMP**-weapons
- **NBIC-systems**

[47] Janisch, Michael. 2016. Presentation at the Conference Converging Technologies and Emerging Risks. Vienna: National Defense Academy Austria.

- **Biogenetic** ”weapons”, whereby these might influence not only humans but the whole biosphere

I’d like to conclude with a statement made by the former DARPA - Defence Science Director, Michael J. GOLDBLATT, PhD J.D.: “As impossible as these visions sound ... we are talking about science action, not science fiction”[48]

[48] Goldblatt, Michael J. 2005. In: Garreau, Joel. Radical Evolution. New York, p. 22.

X-Events and the GNR Problem[49]

John Casti

It's the Law

In the issue of 19 April 1965 of the Journal Electronics Magazine the engineer Gordon Moore, co-founder of Intel Corporation, wrote the following prophetic words about advances to be expected in semiconductor technology:

"The complexity for minimum component costs has increased at a rate of roughly a factor of two per year. […] Certainly over the short term this rate can be expected to continue, if not to increase […] B y 1975, the number of components per integrated circuit for minimum cost will be 65,000. I believe that such a large circuit can be built on a single wafer."

A few years later, semiconductor pioneer and Caltech professor Carver Mead dubbed this statement 'Moore's Law', a term that techno-futurists and the media have now enshrined as the definitive statement underpinning technological advancement in the age of machines. Subsequent mutations, modifications and tinkering led to the general belief that what Moore said was that transistor packing/computer memory capacity/computer performance per unit cost/ ... will 'double every 18 months'. Moore actually said no such thing. What he actually meant was that the number of something absolutely central to digital technology improvement would increase at an exponential rate – with no increase in

[49] This chapter is a slightly edited version of Chapter 10 of "Casti, John. 2012. X-EVENTS. New York: Harper Collins." The article in this book is published with the special permission of John Casti.

cost and, moreover, that this development would continue for at least several decades, if not longer.

Despite the rather grandiose labeling of Moore's observation as a 'law', there is actually nothing at all remarkable about what he claimed. In fact, it is a statement that equally applies to the overall life cycle of just about any new technology. When a technology in its infancy tries to shove the existing technology off center stage, its market share is very small. As the new technology gains adherents and begins to make serious inroads into the market, the growth rate increases exponentially. It then peaks and starts a downhill slide until it is itself replaced by the 'next big thing'.

Many studies have shown that the life cycle represented by growth rate (say in number of units of the product sold per month) very much follows the well-known bell-shaped probability curve. And if we measure the cumulative growth of the technology, that is, the fraction of its ultimate total market share achieved over the course of time, it follows the familiar S-shaped curve governing many living and life-like processes. The high-growth part of the S-curve displays exactly the exponentially-increasing growth pattern for semiconductors claimed by Moore.

Even though Moore's Law is neither a law nor an extraordinary insight into the growth of a new technology, it is extremely important in the historical development of digital technology, serving as a kind of goal for an entire industry. The reason is that the research and marketing departments of major players in the industry actually believed the forecasts by 'The Law', which drove them to fiercely develop new products geared to attain the predicted performance capabilities as they were convinced that their competitors would soon produce the product if they did not. So in a certain sense one can think of Moore's Law as a self-fulfilling prophecy. An obvious question is: Where are the limits of this principle?

To answer this question one might start with Gordon Moore himself, who stated in a 2005 interview that the law does not apply indefinitely. At that time, he said "It can't continue forever. The nature of exponentials is that you push them out and eventually disaster happens." In the same interview, Moore also noted that "Moore's Law is a violation of Murphy's Law. Everything gets better and better." Other researchers, including MIT quantum computing expert Seth Lloyd, see the limit reached after 600 years!

In this spirit, speculative futurists, like the inventor Ray Kurzweil and the mathematician, computer scientist and science-fiction author Vernor Vinge, have conjectured that continuation of Moore's Law for only another few decades will bring on a so-called technological *singularity*. In his book *The Singularity is Near* (2005), Kurzweil suggests that the evolution process includes six epochs, starting with the emergence of information in atomic structures and moving to Epoch Four, the state we are in today, in which technology is able to embody information processes in hardware and software designs. Kurzweil believes that we are currently at the forefront of Epoch 5, which involves the merging of technology and human intelligence. In other words, this is the point where technology manages to incorporate the methods of biology—primarily self-repair and replication. These methods are then integrated into the human technology base. The *singularity*—Epoch 6—occurs when the knowledge embedded in our brains merges with the information-processing capability of our technology (read: machines).

In a 1993 article Vinge, called *The Singularity,* a point where our old models must be discarded and a new reality rules." Since humans have the ability to internalize the world and ask "What if?" we can solve problems thousands of times faster than evolution can do it in its shotgun approach of trying everything and sorting out what works from what doesn't. By being able to create our simulations at a vastly greater speed than ever before, we will

enter a regime so different that it will be tantamount to throwing away all the old rules overnight.

It's of more than passing interest to see that Vinge credits the great visionary John von Neumann for seeing this possibility in the 1950s. Von Neumann's close friend, mathematician Stan Ulam, recalls in his autobiography a conversation the two of them had centering on the ever-accelerating progress of technology and changes in human life. Von Neumann argued that the rate of technological progress gives rise to an approaching *singularity* in human history beyond which human affairs as we know them cannot continue. Even though he didn't seem to be using the term *singularity* in quite the same way as Vinge, who refers to a kind of superhuman intelligence, the essential content of the statement refers to what today's futurists have in mind: an ultra-intelligent machine beyond any hope of human control.

Radical futurists claim that this fusion between the human mind and machines will enable humankind to surmount many problems—disease, finite material resources, poverty, hunger. But they warn that this capability will also open up the possibility for unparalleled capabilities for humans to act on their destructive impulses. For those readers old enough to remember the golden age of science-fiction films, this is all eerily reminiscent of the marvelous 1956 classic Forbidden Planet, in which intrepid intergalactic explorers discover the remains of the Krell, an ancient civilization that possessed the power of creation by pure thought alone. The Krell apparently vanished overnight when the destructive power of their alien IDs was given free reign. Should you have missed the film, a reading of Shakespeare's Othello makes the same point.

It's important to note at this juncture that Kurzweil's argument does not depend on Moore's Law, remaining in effect indefinitely, at least not in its original form pertaining just to semiconductors. Rather, he believes that some new kind of technology will replace the use of integrated circuits and

the exponential growth according to Moore's Law will then start anew for this new technology. To distinguish this generalized version of Moore's Law, Kurzweil has coined the term The Law of Accelerating Returns.

The type of X-event we focus on in this paper involves the emergence of an 'unfriendly' technological species whose interests conflict with those of the lowly human beings. In such a planetary battle, the humans might win out. But it's not the way to bet. So let's look into the arguments for and against this type of conflict, and see if we can get some insight why the radical futurists think we should be wondering and worrying about these matters at all.

The GNR problem

There are three rapidly developing technologies that concern most '*singularity* theorists' like Kurzweil, Vinge and others. They are genetic engineering, nanotechnology and robotics, which taken together form what is often termed The GNR Problem. Here's a bird's eye view of each.

Genetic engineering: In the past decade or so, the manipulation of the DNA of plants and animals opens up the possibility of producing organisms having specific properties deemed desirable by the 'breeders'. These might be practical things like disease-resistant tomatoes or bigger, fatter chickens. Or they might extend to breeding more attractive or smarter humans. In any case, people are concerned about this kind of advanced genetic manipulation getting out of control and leading to a runaway flood of species that could push humankind off the planet.

Nanotechnology: Huge research efforts are underway to provide practical means to control matter at the molecular, or even atomic, level. The catch-all term 'nanotech' is used to describe a cluster of such efforts, which includes things, like the use of engineered molecules to clean out clogged arteries (nanomedicine), the employment of molecules as switches in

electronic devices (nanoelectronics), and the construction of atom-sized machines to assemble totally novel sorts of products (nanomanufacturing). Ethicists and futurists worry about the possibility of these nano- objects attaining the capability to manufacture copies of themselves, leading to a cascade of 'nanobots' flooding the planet.

Robotics: The past decade or two have seen the development of machines performing specific functions, like welding parts for automobiles or vacuuming the floor in your house. What is not at all common is a machine driven by a computer program outside the control of the programmer possessing the ability to think like a human being. Moore's Law suggests that computer hardware is approaching the point where such an artificial intelligence can be realized.

All of these threats provide the same apocalyptic vision: a technology run amok that has developed beyond human control. Whether it is genetically engineered organisms pushing nature's creations off center stage, a plague of nano-objects vacuuming-up matter to leave a kind of 'gray goo' coating the entire planet, or a race of robots breeding like hyperactive rabbits to force humans out of the evolutionary competition, the common factor underwriting each of these dark visions is the heretofore unseen ability of engineered technology to replicate. Killer plants breeding copies of themselves, nano-objects soaking up whatever resources they need to make more and more nano-objects or robots building more robots, all lead to the same unhappy end for humans: A planet that can no longer sustain human life, or what's worse, a planet in which we humans can no longer control our destiny but have been usurped by objects generated by our own technology.

Up to now, a potentially dangerous technology, like a nuclear bomb, can be used just once—build it and use it. But then we humans have to build it again. Technologists argue that genetically-engineered organisms, nano-objects and robots, will be free of this constraint. They will be capable of

self-reproduction at an unprecedented speed and scale. When that crossover point is reached, the curtain starts to fall for humankind as the dominant species on the planet. Or so goes the scenario painted by techno-pessimists like Bill Joy, co-founder of Sun Microsystems, who argued in 2002 that we should impose severe restrictions on research in these areas in order to short-circuit this kind of technological *singularity*. We will take up those arguments, pro and con, a bit later.

Now let's look at one of the more interesting threats of the foregoing type, a plague of robots, as a viable candidate for relegating us humans to the scrapheap of history.

Intelligent Machines

Almost from the very inception of the modern computer era in the late 1940s, the idea of the computer as a 'giant brain' has been a dominant metaphor. In fact, early popular accounts of computers and what people claimed they would be able to do refer to them as 'electronic brains'. This metaphor gained currency following a now-legendary meeting at Dartmouth College in 1950 on the theme of what we now call 'artificial intelligence', the study of how to make a computer think just like you and me. At about the same time, British computer pioneer Alan Turing published an article titled 'Computing Machinery and Intelligence', in which he outlines the case for believing that it would be possible to develop a computer that could think in a human way. In this article, Turing even suggests a test, now called the Turing test, for determining if a computer was indeed thinking like you and me. The Turing test says the computer is thinking like a human if a human interrogator cannot reliably decide whether the machine is a human or a machine through a sequence of blind interrogations, in which the interrogator cannot see the object under interrogation. What is relevant here is that for a race of robots to take over the world, they must have some way of processing information about the

physical world received through their sensory apparatus. In short, they need a brain.

The question is whether technology has come to the point at which a brain sufficient for the job can be put together from the kind of computing equipment currently on offer or to be on offer soon. (Note: It is not required that the robot be able to solve all the same problems that humans encounter. Nor is it necessary that the robot think in the same way as a human. All that is needed is that the brain be good enough to give the robot a survival advantage in competition with humans.) But for the sake of comparison, let us confine our attention to the question of how much computing power we need in order to match or exceed the computing power of the human brain.

At first, we consider the processing power of the brain. From numerous studies focusing on estimating the processing required to simulate specific brain functions, like visual processing, auditory functions and the like, we can extrapolate the processor requirements for the particular part of the brain involved to the entire brain by just scaling-up. So, for instance, estimates suggest that visual processing in the retina requires roughly 1000 million instructions per second (MIPS or cps). As the human brain is about 75,000 times heavier than the neurons in the processing part of the retina (about one-fifth of the entire retina, weighing approximately 0.2 grams), we arrive at an estimate of 1014 instructions per second for the entire brain. Another estimate of the same sort can be obtained from examination of the auditory system. It leads to a figure of 1015 cps for the entire brain. All other such exercises have arrived at more-or-less this same number as a reasonable estimate of the processing power of a single human brain.

How does this compare to a computer? Today's personal computer provides about 109 cps. By the Law of Accelerating Returns, we can expect this figure to be stepped-up to that of the brain in about fifteen years—or less! So much for processing. What about memory?

Estimates indicate that a human who is expert in some domain, such as medicine, mathematics, law or chess-playing, can remember around ten million 'chunks' of information. These chunks consist of pieces of specific knowledge, along with various patterns specific to the domain of expertise. Furthermore, experts say that each such chunk requires about one million bits to store. So the total storage capacity of the brain comes to around 1013 bits. Estimating memory requirements in the brain by counting connections between neurons leads to a larger figure of 1018 bits of memory for a brain.

According to the technological growth curves for computer memory, we should be able to buy 1013 bits of memory for less than one thousand dollars in about ten years. So it's reasonable to expect that all the memory needed to match that of the brain will be readily available not later than around the year 2020.

When putting the two hardware estimates together, we can see that we will be able within twenty years to match the brain's processing and memory capacity with a computing machine costing around one thousand dollars.

Now, what about software? Matching the hardware requirements of the human brain is likely within the next decade or so. But the 'killer app' arrives when we can match the computer's speed, accuracy and unerring memory with human-level intelligence (i.e., software). In order to do this, we have to effectively 'reverse engineer' the brain, capturing its software in the hardware of tomorrow.

When it comes to simulating the brain, the first thing we have to note is all the many ways the human brain differs from a computer. Here are just a few of the more important differences:

Analog versus Digital: A modern computer is essentially a digital device, relying upon great speed to turn switches on and off at a dazzling rate. The

brain, on the other hand, uses a combination of digital and analog (mostly) processes for its computations. While in the early days of computing people set great store by the seeming digital aspect of the brain's neurons, we have found that they are actually mostly analog devices using chemical gradients (neurotransmitters) to open and close. So to argue a similarity between a computer switching circuit and one in the brain is a big stretch, to say the least.

Speed: The brain is slow; a computer is fast. In fact, the typical cycle time of even a slow computer is billions of times faster than the cycle time of a neuron, which is about twenty milliseconds. So the brain has only a few hundred cycles to do its job of recognizing patterns.

Parallel versus serial: The brain has trillions of connections linking its neurons. This high degree of connectivity allows lots of computations to be carried out in parallel. This is totally unlike almost all digital computers, which do one operation at a time in serial fashion.

These are but a few of the features distinguishing a human brain from a computer. But with the computing power just around the corner, we will still be in a position to simulate the brain without actually trying to fabricate it. What's needed for the next stage of evolution is for computers to be functionally equivalent to the brain, not to duplicate its precise physical structure.

All this having been said, simulating a human brain functionally inside a computer is not quite the same thing as simulating a human being. Or is it? Of course, a disembodied supra-human brain might easily displace carbon-based humans as the dominant species on the planet. But even a disembodied brain needs somehow to sustain its existence in some type of material medium. Nowadays this medium is the motherboard, keyboard, monitor, hard drive, RAM memory chips and all the other hardware of your computer. Tomorrow, who knows? But what we do know is that

there will have to be some type of physical embodiment of the intelligence. This means a sensory apparatus for accessing the world outside the intelligence, as well as some sort of boundary separating that intelligence from what is 'outside'. So much for computers. What about robots?

A Brain-in-a-Vat versus Robby, the Robot

As I write these words in my office at home, in the next room a robot called a 'Roomba' is moving about in the living room diligently vacuuming-up the carpet and floors. My hat is off to the design team at iRobot Inc., who developed this little gizmo, as it does an excellent job at a task that I hate—exactly what most of us wish for in a robot. Basically, what we usually have in mind is some sort of automaton that will do our bidding with no questions asked, relieving us of various chores and duties that need doing (like vacuuming) but that in truth are pretty tiresome and boring. But what we certainly do not have in mind is a collective of intelligent robots who think that perhaps the tables should be turned and that humans should serve them instead of the other way around. What are the possibilities of that flip-flop?

Just before setting the Roomba loose in my living room, a friend and I watched the classic 1956 sci-fi film 'Forbidden Planet" that I mentioned earlier. Although the technology envisioned by the film's producers fifty years ago is now a bit antiquated, the story and the moral is as fresh as this morning's croissants from the bakery on the corner.

Although the F/X specialists in the Fifties were not quite up to today's standards, the portrayal of Robby, the Robot, a piece of machinery that serves humans as a driver, cook, transport device, and overall factotum is wondrous. Even my teenage mind was fascinated by the possibilities when I first saw the film, and I marveled at Robby's capability to learn new tasks and comprehend human instructions. Moreover, at the story's denouement

Robby remains loyal to his human masters, as all of his wiring short-circuited when he was given instructions to harm a human.

The question raised for us by Robby is whether a robot with those almost superhuman properties can be guaranteed to follow something like Isaac Asimov's Laws of Robotics. In about 1940, Asimov proposed the following laws for a robot to remain a servant to humans, and not become an evolutionary competitor.

First Law

A robot may not injure a human being or, through inaction, allow a human being to come to harm.

Second Law

A robot must obey orders given to it by human beings, except where such orders would conflict with the First Law.

Third Law

A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

These Laws of Robotics stipulate that robots are to be slaves to humans (the Second Law). However, this role can be overridden by the higher-order First Law, which prevents robots from injuring a human, either by their own action or by following instructions given by a human. This prevents them from continuing any activity that would lead to human injury. It also prevents robots from being used as a tool for or to assist in various types of physical assaults on humans.

The Third Law generates a robotic survival instinct. So in the absence of conflict with a higher order law, a robot will

- Seek to avoid his destruction through natural causes or accident;
- Defend itself against attacks from other robots;
- Defend itself against attacks by humans.

Roger Clarke and others have noted that under the Second Law a robot appears to be required to comply with a human order, so as to (1) not resist being destroyed or dismantled, (2) cause itself to be destroyed, or (3) (within the limits of paradox) dismantle itself. In various stories, Asimov notes that the order to self- destruct does not have to be obeyed if obedience would result in harm to a human. In addition, a robot would generally not be precluded from seeking clarification of the order.

Another gap in Asimov's three Laws, and one that is very important for our purposes here, is that the Laws refer to individual human beings. Nothing is said about robots taking actions that would harm a group, or in the extreme case, humanity as a whole. This leads to the

Zeroth Law

A robot may not injure humanity or, through inaction, allow humanity to come to harm.

These 'laws' of robotic good-citizenship impose severe constraints as to what is needed to keep a band of intelligent robots in check. Given the propensity of intelligent objects to evolve so as to enhance their own survival, it seems unlikely that robots of the sort we are envisioning here will be satisfied to serve humans as they develop the capacity to serve themselves. In the 2004 film 'I, Robot', which is loosely based on Asimov's 1950 collection of short stories, robots reinterpret the Laws and logically conclude that the best way to protect humans is to rule them. The paradox here is that to be really useful robots have to be able to make their own decisions. But as soon as they have the capacity to do this, they acquire the ability to violate the Laws.

Now back to the vexing question: Will robots take over the world? The short answer is . . . a definite maybe!

One of my favorite rejoinders to the claims of some futurists about robotic takeover in the next few decades is that the bodies of robots will be made of mechanical technology, not electronic. And mechanical engineering technology is simply not developing at the same furious rate as computers. There is no Moore's Law in the mechanical realm. For instance, if automobiles had developed at the same pace as computers we would now have cars smaller than a match box, traveling at supersonic speeds, and transporting a train load of passengers while consuming a teaspoonful of gasoline. In short, size matters when it comes to mechanical technology, and the rule is the bigger it is, the more powerful it is. Computers are just the opposite.

So even if we have robots hundreds of times more intelligent than us in a few decades, humans will still maintain a vast mechanical superiority. Humans will be able to knock over such a robot without breaking a sweat, climb stairs and trees easier than any robot on wheels could hope to do, and generally outperform robots on almost any task requiring the delicate manipulative capabilities that we have in our hands and fingers.

If I were a betting man, I'd put my money on the above argument for human superiority in the mechanical dexterity department. And this despite the fact that we already have robots doing surgical operations by remote control, along with robotic soldiers carrying out missions in regions infested with land mines, poisonous gases and other hazards to humans. The fact that robots can execute such tasks is indeed impressive. But these are very special-purpose robots, just like the Roomba vacuum, designed to perform a very special job—and only that job.

Humans, on the other hand, have a far greater capacity to deviate from the planned program when circumstances do not quite fit into the

predefined framework that the robot's 'brain' expects to encounter. Of course, you might argue that when the robot brain begins to surpass the human brain in its information-processing capabilities and in its ability to adapt to unanticipated circumstances, the game may indeed be up for us humans. With this ambiguous prospect in mind for a robotic takeover, let us return to the question of s*ingularity* and examine when it might happen.

The Singularity

In the 1993 paper by Vinge that sparked off volumes of debate, several paths are sketched out that could lead to the technological creation of a trans-human intelligence. To paraphrase Vinge, these include:

- The development of computers that are 'awake' and superhumanly intelligent;
- Large computer networks (e.g., the Internet) and their associated users 'wake up' as a superhumanly intelligent entity;
- Computer/human interfaces become so intimate that users of the interface are considered superhumanly intelligent;
- Biological science provides the means to improve natural human intelligence.

The first three elements on this list involve improvement in computer technology, while the last is primarily genetic. And all may well rely on nanotechnological developments for their realization. So each facet of the GNR problem discussed earlier makes its appearance in the unfolding of *The Singularity*. And once such an intelligence is 'alive', the likelihood is that it will lead to an exponential runaway in development of even greater intelligences.

From a human point of view, the consequences of the emergence of these superhuman intelligences are incalculable. All the old rules will be thrown

away, perhaps in just a few hours! Developments that previously were thought to take generations or millennia may unfold in a few years—or less.

For the next decade or so we probably won't notice any dramatic movement toward *The Singularity*. But as hardware develops to a level well beyond natural human abilities, more symptoms of *The Singularity* will become evident. We will see machines take over high-level jobs such as executive management that were previously thought of as the province of humans. Another symptom will be that of ideas spreading far quicker than ever before. Of course, we already rely on computers for a bewildering array of tasks, as we described solely in the context of communication in our chapter on the Internet. But even in such a mundane matter as writing this book, I occasionally shudder when I think of what it was like just three decades ago, when I wrote my first book—literally by hand! That thought is but a distant early-warning sign of things to come as we approach *The Singularity*.

And what of the moment when *The Singularity* actually arrives? According to Vinge, it may seem as if our artifacts simply 'wake up'. From the moment of crossing the threshold of *The Singularity* we will be in the post-human era.

The most crucial point here is whether *The Singularity* is actually possible. If we can convince ourselves that it can indeed happen, then nothing short of the total destruction of human society can stand in its way. Even if all the governments of the world were to try to prevent it, researchers would still find ways to continue making progress to the goal. In short, if something can happen, it will happen—regardless of what governments, or societies as a whole, might think about it. That is the natural way of human curiosity and inventiveness. And no amount of political bombast or hand-wringing morality is going to change that state of affairs.

So assuming *The Singularity* can take place, when is the 'crossover' going to occur? There seems to be a reasonably uniform consensus on the answer: Within the next 20-30 years. The technology futurist Ray Kurzweil has been even more specific. In his book *The Singularity is Near*, a kind of 'bible of Singularitarians', he states:

"I set the date for The Singularity—representing a profound and disruptive transformation in human capability—as 2045. The non-biological intelligence created in that year will be one billion times more powerful than all human intelligence today."

That is about as definite as you can get in the forecasting business!

For what it is worth, even though I firmly believe that there will be a *singularity*, I'm personally rather skeptical about the timing aspect of the whole business. The arguments from Moore's Law, accelerating returns, human curiosity and the like leading to this 'grand' event in a couple of decades strikes me as rather reminiscent of the kinds of pronouncements made in the early 1950s by AI advocates about what computers would (or wouldn't) do in the years to come. Some of those claims included becoming the world chess champion with ten years, translating languages at the skill level of first-rate human translators in the same time frame, becoming electromechanical butlers serving dry martinis after a hard day at the office and so on. Well, some of these goals have actually been achieved, such as a computer (Deep Blue II) beating the world chess champion (in 1997, not in the 1960s, and by using methods totally unlike what a human player would employ), while others are as far away as ever from being achieved (high-quality human-level language translation). In fact, the whole line of argument by 'Singularitarians' is a familiar one in the futurology business: Extrapolate current trends and ignore the possibility of any surprises getting in the way. But, of course, this argument only puts off the day of accounting, and I strongly suspect we will see the kind of super-human intelligence *The Singularity* calls for before the end of this century.

Adding it all up

The complexity increase in the world of machines is rapidly outpacing that of the human side of the ledger, creating a gap that will almost surely result in an X-event, *singularity*, within the next few decades. In contrast to some of the complexity gaps we have spoken of earlier, such as an EMP attack or an Internet crash, *singularity* is an X-event, whose unfolding time is decades, not minutes or seconds. But its impact will be dramatic and irreversible, pushing humans off center-stage in the grand evolutionary drama of life on this planet.

It should go without saying that the occurrence of any one of the GNR triumvirate, let alone a combination of the three, would be of great concern for national defense establishments and multi-country organizations like the European Union. *Singularity* represents a direct threat to the way of human life that has been taken for granted since humans arose many millennia ago. Since it is virtually certain that *singularity* will occur at some point in this century, our goal should be to understand it well enough that we can manage it so as to ensure that humans will still have a place in that brave, new world governed by the kind of transcendent intelligence that *singularity* will usher-in.

3 Implications in the Fields of Nano-/Bio-/Information Technology

Security Risks of Converging Technologies in the Areas Bio-, Nano- and Information Security

Johannes Rath

Aldous Huxley once said "Technological progress has merely provided us with more efficient means for going backwards."[50] There is no easy answer to the question whether technological progress is a driving force in the evolution of society. Today, many of the technological advances challenge our socially and biologically limited capacities regarding governance, cognition and empathy. Some of these constraints have developed over thousands of years of biological and cultural evolution and are enshrined in our genes, cultures and laws. For example, the way modern technologies have been used in recent elections to manipulate, mobilise and polarise voters based on untrue and unverifiable claims highlights these challenges. Therefore Aldous Huxley might have been right that by integrating these technologies into our world we have gone backwards in our societal and cultural achievements – one of them being empathy and with it our desire for peace.

In the recent workshop organised by the Austrian Ministry of Defence and Sports on Converging Technologies in the security sector, I had the honour to moderate a panel of distinguished scholars who provided their views on specific societal challenges posed by modern nano-, bio- and information technologies.

[50] Huxley, Aldous. 1937. Ends and Means. New York, London: Harper and Brothers.

Dr. Norbert Frischauf provided an overview on current and future trajectories of such technological developments. He stressed that technological progress can be a disruptive as well as incremental process and emphasized the relevance of fundamental research reagarding the cycle of technological development. Dr. Frischauf mentioned the application neutrality of technologies, where the sinister potential of such technologies only comes into play when humans use it for certain purposes. With this in mind he concluded with a proverb attributed to Thomas Jefferson on the need for 'eternal vigilance' to ensure liberty.

Dr. Filippa Lentzos provided insights into two key areas of converging technologies in the context of biology. First, she focused on synthetic biology. Dr Lentzos outlined three key concerns regarding synthetic biology: a. making it easier to create dangerous pathogens, b. contributing to a break-down of the expert vs. non-expert boundary, c. enhancing the capacity to create radically new pathogens. She concluded that although there are substantial risks related to this technological development in the future, the short-term risk might be overrated. Second, Dr. Lentzos focussed on neurobiology and its ramifications with the security sector, ranging from human enhancement to the development of new chemical warfare agents. In the final part, she focused on potential misuse of these technologies and the international legal framework that should help minimizing misuse risks.

Dr. Wolfgang Schallenberger discussed a very concrete example of objective risk management in the area of biological research. He focused on a recent study conducted by the Austrian 'Kuratorium Sicheres Österreich'. By focussing on semi-quantitative risk assessment approaches, Dr. Schallenberger presented "risk matrixes" for various biological agents that should be used in guiding and prioritizing risk management practices. He also addressed the current developments in the area of research governance (e.g. dual use research of concern, GOF experiments in influenca). In his concluding remarks, Dr. Schallenberger stressed the need for an integrated

biorisk management/bio-preparedness approach based on objective risk assessment, together with a strong element of self-governance by life scientists.

Technology today provides us not only with answers to questions but increasingly defines the questions we ask. As a consequence, the fundamental distinction between individuals and society, on the one hand, and technology, on the other hand, is becoming more and more blurred. So if Aldous Huxley is correct, the fast pace of technological progress is a fundamental risk to our societal achievements, like peace, fundamental freedoms and human rights. It is too early to judge, whether the recent events and trajectories in politics and the security field are harbingers of what we can expect from a future technology-driven society – but, as Thomas Jefferson stated, more vigilance might be needed than ever before to ensure that our freedom does not become the price for technological progress.

What is the 'Sinister' Potential of Nano-, Bio-, and Information Technology Products in the Year 2025?

Norbert Frischauf

There is not a single day without news related to a product of nano-, bio-, or information technology, such as inventions based on graphene or quantum dots, bucky balls, and carbon nano tubes; cloning, cryosleep, gene therapy, or stem cell treatment; big data, Machine-to-Machine (M2M) communication, the Internet of Things (IoT), cloud services, swarm and artificial intelligence – the list is sheerly endless.

Most of these news items are generated by a research group and/or a start-up looking for additional funding and/or investment, and quite often investors – especially Venture Capital (VC) firms – who are ready to seize the opportunity, e.g. the Fartner Group assume that there may be a large untapped market that could be served[51]. The following figure provides a snapshot of the emerging technologies as of 2014, summarised in the so-called 'Hype Cycle' by the Gartner Group, a listing of emerging technologies and the associated expectations.

[51] Analysts like the Gartner Group assume that the number of connected devices will rise dramatically in the years to come; from 12.5 billion in the year 2010 to 80 billion by 2020. In the same period the number of mobile phones is predicted to increase from 5.6 to 9 billion.

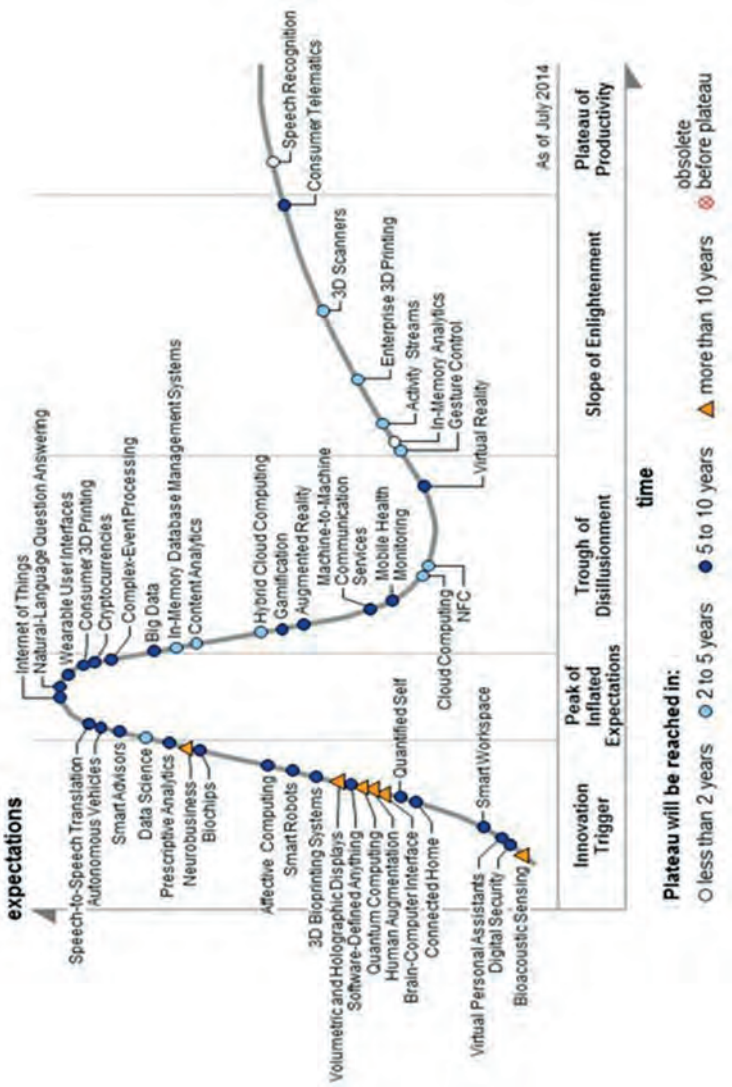


Figure 1: 2014 Hype Cycle of Emerging Technologies[52]

[52] Gartner Group. 2014. Gartner's 2014 Hype Cycle for Emerging Technologies Maps the

While not all of these emerging technologies will be realised, several will, and the gains of those will make up for the losses of the others. A VC runs his investment portfolio with a targeted success rate of 10-20% - if two out of ten investments survive, the VC is making profit.

This 20:80 ratio prevails also in technological progress. Contrary to common belief, technological progress is most of the time an incremental process – the disruptive innovation[53], as powerful as it is, is the exception. Nonetheless, it is these disruptive technologies and the embedded opportunities that stimulate the imagination of people. Who cares if the computer performance doubles every second year? 3D printing, autonomous cars, the human genome, cloud computing and big data are the buzzwords that make it into the news. The following graphic from McKinsey lists twelve of these disruptive innovations, which are currently making the headlines of all sorts of technology magazines.

Journey to Digital Business.

[53] A disruptive innovation is an innovation that creates a new (and unexpected) market by applying a different set of values (e.g. the lower-priced Ford Model-T).

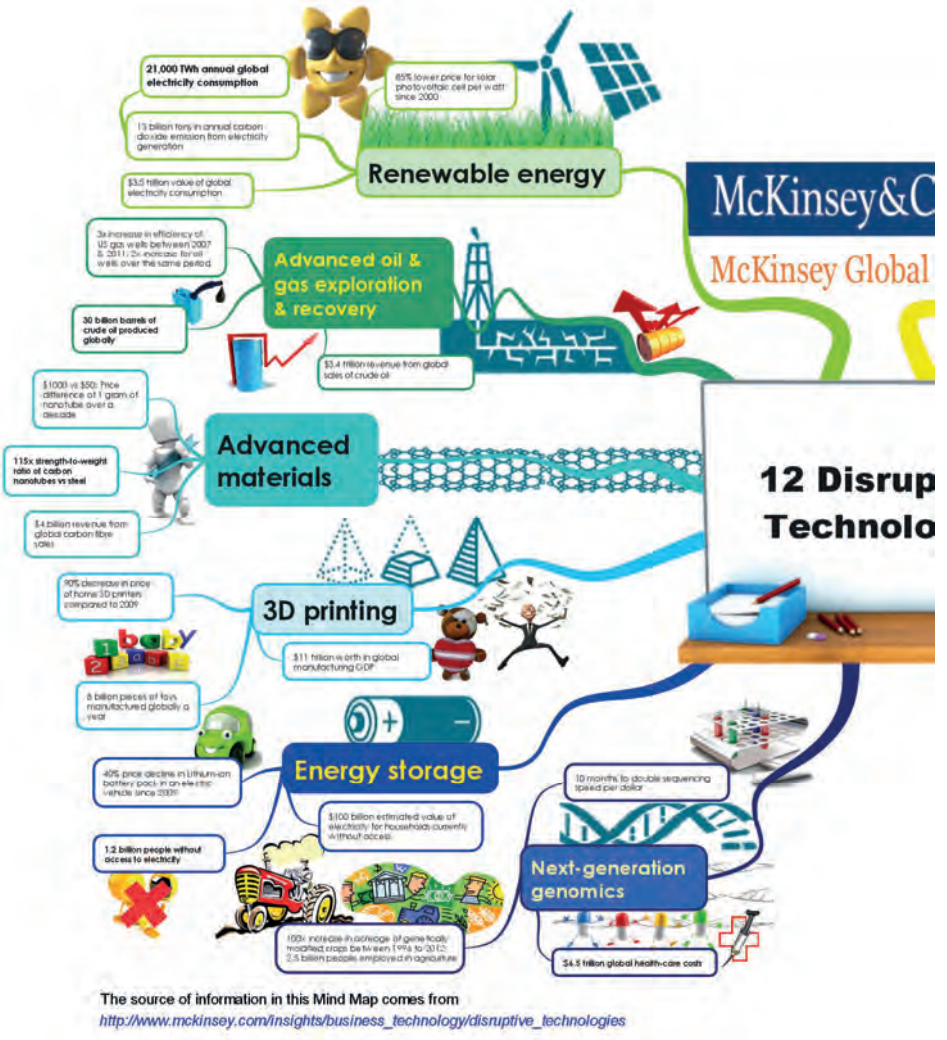
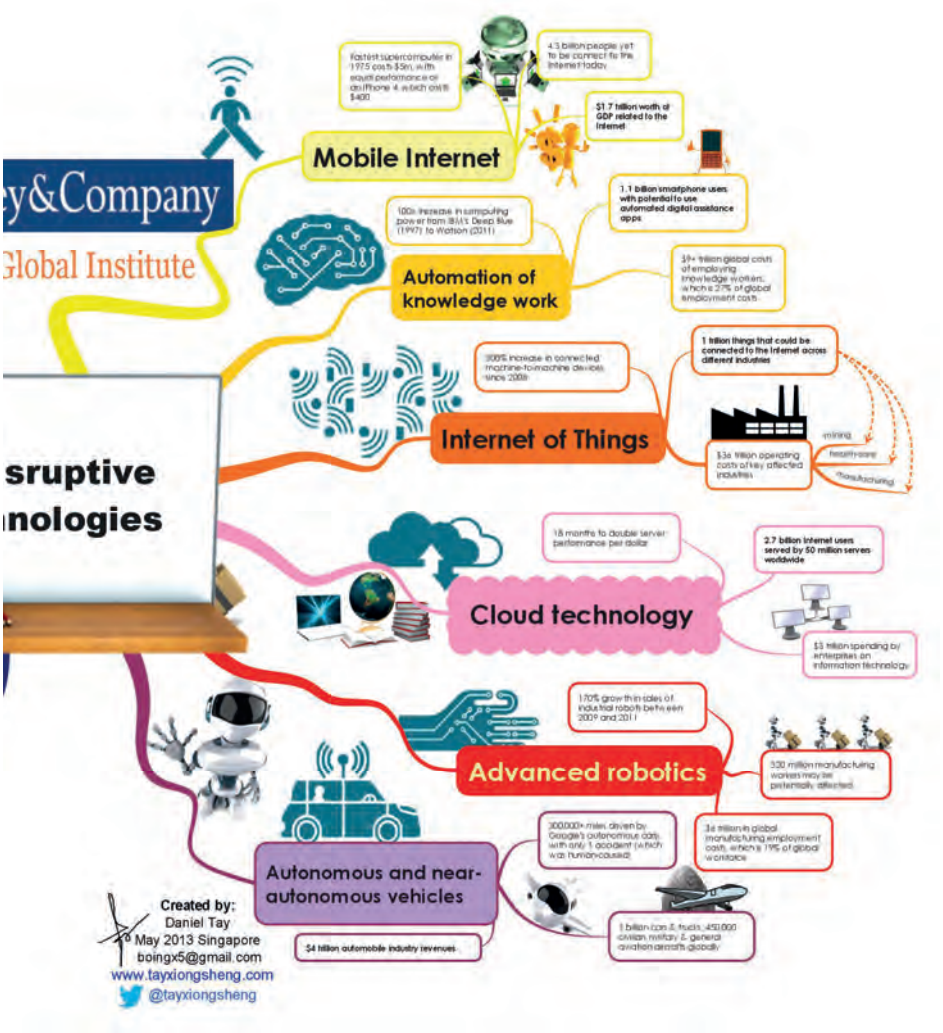


Figure 2: Portfolio of twelve Disruptive Technologies[54]

[54] McKinsey Global Institute: g. 12 Disruptive Technologies. www.mckinsey.com/insights/business_technology/disruptive_technologies accessed on 29 March 2016.


y&Company
Global Institute
sruptive
nologies
Mobile Internet
Fastest supercomputer in 1975 cost $5m, with equal performance of an iPhone 4, which cost $400
4.3 billion people yet to be connect to the Internet today
$1.7 trillion worth of GDP related to the Internet
1.1 billion smartphone users with potential to use automated digital assistance apps
Automation of knowledge work
100x increase in computing power from IBM's Deep Blue (1997) to Watson (2011)
$9+ trillion global costs of employing knowledge workers, which is 27% of global employment costs
Internet of Things
300% increase in connected machine-to-machine devices since 2009
1 trillion things that could be connected to the Internet across different industries
$3t trillion operating costs of key affected industries
mining
healthcare
manufacturing
Cloud technology
18 months to double server performance per dollar
2.7 billion internet users served by 50 million servers worldwide
$3 trillion spending by enterprises on information technology
Advanced robotics
170% growth in sales of industrial robots between 2009 and 2011
320 million manufacturing workers may be potentially affected
Autonomous and near-autonomous vehicles
300,000+ miles driven by Google's autonomous cars with only 1 accident (which was human-caused)
$4 trillion in global manufacturing employment costs, which is 19% of global workforce
1 billion cars & trucks, 450,000 civilian, military & general aviation aircrafts globally
$4 trillion automobile industry revenues
Created by:
Daniel Tay
May 2013 Singapore
boingx5@gmail.com
www.tayxiongsheng.com
@tayxiongsheng

When comparing disruptive technologies and their application as outlined in Figure with the three technology domains projected by physics, chemistry and biology, it becomes obvious that the three classical natural sciences are the basis of technological progress.

In the end our current progress paradigm builds upon the technological progress, which is introduced into the (western) human society via the so-called Product Life Cycle (PLC). The PLC comes along with several distinct phases, as depicted in the figure below.

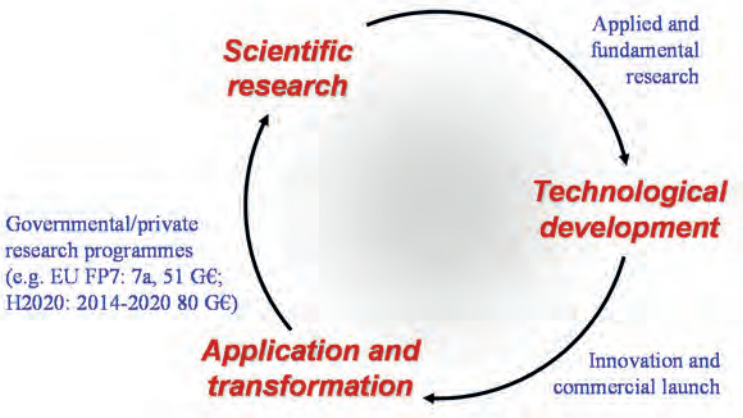


Figure 3: Technological progress paradigm[55]

Starting with scientific research (involving fundamental and applied research), the follow-on technological development enters the market due to innovation and commercial launch. As the technology is implemented by creating a product or service, it better serves the needs of customers. When the end of the PLC is reached, the next generation is prepared for market launch – the associated research may be strategically or market-driven, such

[55] Copyright Norbert Frischauf.

as by governmental/private research programmes, like the European Union's H2020 Research Programme.

Analysing the three domains of technological progress (energy, information, biotech) one will find that some items do not belong to one domain but to several, such as sensor implants and mobility devices.

Ubiquitous and reliable communication is a major driving force behind all this progress, since it

- allows to interconnect distant systems with each other;
- enables distant intelligence; and
- is essential to remotely control activities and processes.

Google's Loon is seen as a great tool to bridge the 'Digital Divide', allowing for a cost-effective access to communication services in areas and regions, which are currently underserved – like Sri Lanka.

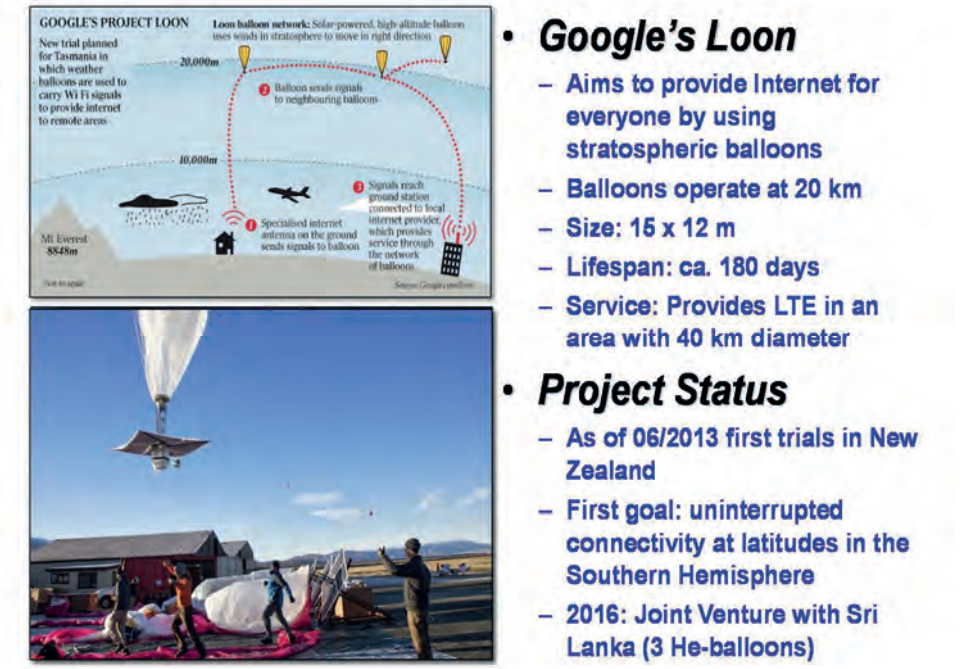


Figure 4: Google's Loon in a nutshell

There are significant deficits worldwide concerning the access to communication infrastructures – not only from that perspective can Africa be considered 'the lost continent' – and systems like Loon are essential to realise the global Internet of Things (IoT), Machine-to-Machine (M2M) and the Industry 4.0 Vision, as they hold the promise for worldwide ubiquitous and reliable communication.

While all this may sound like 'Brave, new world', one thing that may not be forgotten is that all these technologies are 'application-neutral', i.e. they may be used for good, not so good or entirely bad purposes. Naturally, products created by nano-, bio- and information technology are in themselves neither good nor bad; their sinister potential is somewhat embedded and will be unleashed dependent on the application, like in the case of any other technology. One difference,

however, is that such products are both disruptive and ground-breaking. This stems from the fact that nano- and biotechnology have the potential to fundamentally change the world, as both build upon natural processes that 'mother nature' has been using for billions of years. Due to the similarity of all these processes, certain inventions risk to create an unwanted spill-over effect into another nano- or biosystem. One example within the biotech sector may be that a researcher aims to remove a malevolent genetic code in a patient using CRISPR-Cas, and unwillingly changes the genes in a different way with potentially undetectable but nonetheless fatal results. The sinister side is that someone might want to do this on purpose and against all ethical agreements (such as altering germ cells in order to alter the genes of the offspring).

Similar issues arise with nanotechnology – especially when we are talking of self-replicating nano-systems things may get quickly out of control. The Science Fiction novel 'Diamond Age – Induced Nightmares' provides a great example, with the story taking place at the beginning of the 21st century in a research laboratory:

David Stanton, who works on his thesis, has been able to construct the first carbon-based nanomachine by using a Scanning Tunnelling Microscope (STM). The story starts with Mr. Stanton calling for his thesis advisor, Dr. Sarah Latkins, explaining her how he has achieved this breakthrough and how to control the nanomachines. Two types of nanomachines exist, the duplicator and the builder. While the first one is being used to construct copies of builders and duplicators, the builders are the workhorses, and cannot make any copies of themselves. Telling the duplicators, whether they should produce builders or more duplicators is achieved by changing the conductivity of the solution in which the nanomachines are dispersed. If the conductivity is increased the duplicators start to produce duplicators. The builders are shut off by either withholding iron or boiling off the water. Both types of machines do automatically destroy themselves if not immersed. The tragedy starts as Dr. Latkins learns that David has cut one of his fingers, with the wound being

exposed to the "nano-liquid". In the following minutes both the student and his thesis advisor evaluate the consequences if only one of the duplicators has got into the bloodstream of David. Although the odds are astronomically small that a duplicator has entered David's body (the nano-liquid has 156.000.000 builders vs. 58 duplicators), the consequences are enormous. Carbon is anywhere in the human body, and of course the environment inside the bloodstream is of liquid nature. As Dr. Latkins realises that there is a significant danger, she calls on the police. The military isolates her, David and eight other students as well as the equipment from the laboratory in Cheyenne Mountain. The incubation period is ten days and during that time everyone from the laboratory resides in an absolute dry room, isolated from the others. At the last day, all of the 10 persons are linked together in a videoconference, already on the verge of leaving the isolation quarter. It is then, when the "nano-chain reaction" starts within David's body. As the builders inside David's bloodstream could not find any iron they shut themselves off and disintegrated, releasing iron (that was used beforehand to "feed" them), thus increasing the conductivity. The increased conductivity was the trigger for the duplicator(s) to construct even more duplicators, using the carbon supply nearby. Within a few minutes after the process had started within David's leg, the chain reaction reaches every atom in David's body, creating enormous heat, burning him alive from inside out while incorporating every of his body's atoms into duplicators. While the others watch David's agony, they are aware that the process will only stop as soon as David's body has dried out – the nanomachines will only destroy themselves in the absence of liquid - tragic for David, but the only hope for all carbon-based life forms in the vicinity. But even this last hope is smashed as the huge flame that consumes David's body triggers the sprinkler system of the military base…[56]

Information may not be as dangerous as bio or nanotechnology as it is not that closely connected to living organisms; still it has a great

[56] Vader, Paul. n.a. "Diamond Age – Induced Nightmares".

potential to alter things simply because of the vast number of systems that will exist and will be interconnected – eventually the IoT and M2M will be like a beehive, possibly representing some kind of swarm and maybe one day even an artificial intelligence. Acknowledging that the DNA is nothing else but a great information storage system, one can only speculate what happens, if one day it becomes possible to handle all information stored in every device on this world. The digital age, enabling both digital storage and interconnected systems, has already made this vision possible. What is missing are some clever big data algorithms to find and exploit so far hidden structures within the data chaos.

Obviously, bio-, nano-, and information technology have a great sinister potential of their own. Is this risk even more elevated by technological convergence? Digital convergence, which aims to integrate four industries into one, ITTCE (Information Technologies, Telecommunication, Consumer Electronics, and Entertainment), is a fact like media convergence, the interlinking of computing and other information technologies, media content, media companies and communication networks. As of 2014, another convergence, NBIC (Nanotechnology, Biotechnology, Information technology and Cognitive science), was put on the table. Will it improve human performance or will it make us obsolete and lead machines to overtake us to rule the world? No one can tell now, as humanity seems to be able to master information technology and, to a certain extent, cognitive science. However, as far as the capabilities of bio and nano technology are concerned, we are still in an infant stage. Once humanity masters bio- and nanotechnology, it remains to be seen what humans will do with it, as these technologies may potentially be abused. The movie

'Gattaca' (1997) and the SF novel 'The Diamond Age'[57] provide an insight into the pros and cons of a world where human capabilities are altered at will and where systems that manipulate matter at the atomic level have become objects of utility.

NBIC may be an opportunity and a potential sinister problem in the future, but today's interlinked world offers already enough sinister potential for those who are willing to seize the opportunities that exist. There is no discussion that in a globally interlinked industry scenario, failures in cybersecurity become a GLOBAL threat, providing for a means to attack and stop vital processes. In the years to come, the data on our computers, mobile phones and in the cloud may be readily accessible for everyone who has a quantum computer at his disposal. On the other hand, quantum cryptography may serve as the best option to ensure secure data transmission.

Wherever technological progress may finally take us, all technologies will have a positive and a negative potential and, consequently, emerging risks will appear in several forms and with different time scales. The figure below aims to list but a few, putting them in the context of time and technology domains:

[57] Stephenson, Neal. 1995. The Diamond Age. Bantam Dell, New York.

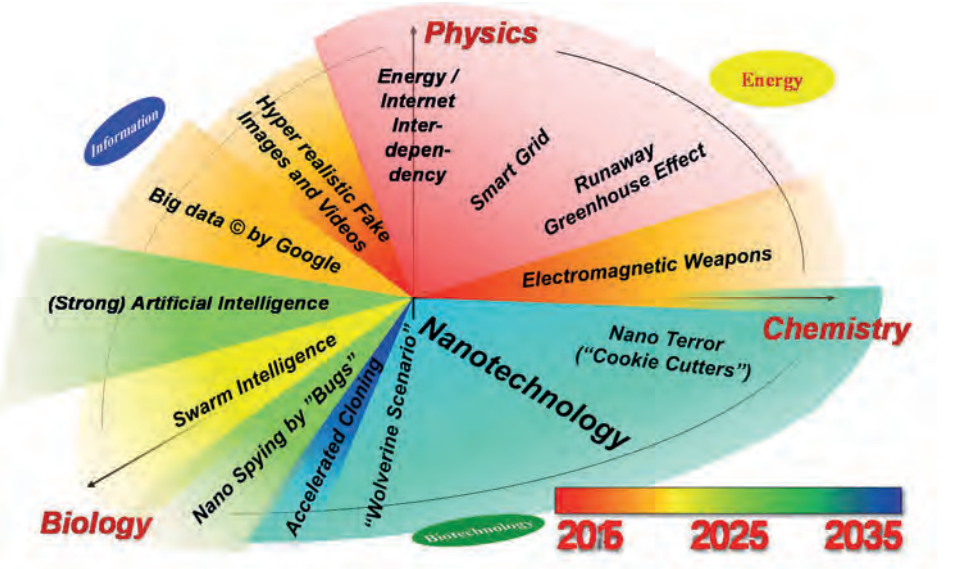


Figure 6: Overview of emerging risks sorted by technology domain and time of potential occurrence[58]

Should a new technology appear within the next 5, 10 or 20 years, whether driven by progress in physics, biology or chemistry, it is clear that it is in our responsibility to make the best use of it. Since we humans are both the driving force and the users of the overall progress – with all our flaws and virtues and – we should be on constant watch regarding what is going on out there. As Thomas Jefferson put it: "Eternal vigilance is the price of liberty"[59]. Although this statement is nearly 200 years old, it is still very modern – especially in the light of the upcoming converging technologies and the associated emerging risks.

---

[58] Copyright Norbert Frischauf.

[59] Jefferson, Thomas. 4th July, 1817, 42nd year,. Bennington: Vermont Gazette. July 8, 1817, p. 2 "...let your motto be 'eternal vigilance is the price we pay for liberty'."

Pandemic and Bioterrorist Threats – Risk Assessment

Wolfgang Schallenberger

Bioterror means the deliberate release of highly pathogenic biological agents (bioagents). Pathogenic biological agents comprise bacteria and viruses as well as biological toxins. These agents are considered to be potentially used by terrorists to cause death and illness or disrupt food and water supply.

Since at least the anthrax letter attack shortly after 9/11 increased efforts have been made to improve preparedness as well as the prevention and counteraction against possible threat of bioterrorism (i.e. bio-preparedness). This holds true for many industrialized countries, particularly for the U.S. government, while e.g. bioterrorist threats have not been perceived as an urgent national security issue in Austria.

As mentioned before, bioterror is the deliberate misuse of biological knowledge and technology. However, the spectrum of biological risks also encompasses naturally occurring (e.g. emerging pandemics) and unintended risks (associated with dual use research or accidental release of pathogens). Therefore, efforts to improve bio-preparedness need to address the full spectrum of biological risks. Thus, advances in biotechnological sciences and their possible misuse for terroristic objectives are a serious concern.

A comprehensive and objective assessment or ranking of biological risks should be in place as an essential prerequisite for organizing preventive actions, prioritizing countermeasures and supporting rapid decisions in case of an emergency situation. Furthermore, risk ranking crucially supports decision-making in the area of regulations concerning the identification of suspicious actions like loss or theft of bioagents and of identifying research and development needs.

In October 2015, the 'Kuratorium Sicheres Österreich (KSÖ)'[60] initiated a process to evaluate chemical, biological, radiological and nuclear (CBRN) threats to establish an objective risk assessment. This assessment was intended as a basis for appropriate national security policies and standards. Experts from different sectors, such as life sciences, health, national security and the military gathered in multiple workshops to design the project outline and then to work out the risk assessment for a selected number of agents[61]. The results, potential consequences and conclusions presented below focus on biological risks.

Risk assessment and risk management - background

The purpose of risk management is to ensure that adequate measures are taken to protect people, environment and infrastructure from harmful consequences of human activities and natural events[62]. As discussed earlier, risk management includes all measures that help to avoid the occurrence of biological threats or to reduce their potential harm. Regarding the extent of risk reduction measures the costs and likely benefits of these measures in terms of safety gains have to be weighed against each other. Therefore, an objective risk and threat assessment is a prerequisite for all rational approaches to risk management. This holds true for industrial risks, natural disasters or, as discussed in this article, for bio-preparedness.

Such comprehensive biological threat assessment requires the evaluation of the risks posed by bioweapons, deliberate or accidental release of bio-pathogens, and potential pandemics. The inclusion of naturally occurring

[60] Kuratorium Sicheres Österreich (KSÖ), cf. https://kuratorium-sicheres-oesterreich.at.
[61] Kuratorium Sicheres Österreich. 2016. Contribution to the nation-wide risk analysis for Austria: biological, chemical, radiological and nuclear threats. Vienna.
[62] Aven, T. & Renn, O. 2009. The role of QRA for characterising risk and uncertainty with emphasis on terrorism risk. In: Risk Analysis, Vol. 4: 587-600.

diseases and emerging pandemics is a pragmatic approach that recognises the synergy of pandemic and biodefense preparedness. A disease outbreak can be caused by bio-terroristic action or can emerge naturally. However, both events require many of the same preventive measures, surveillance routines, diagnostics, healthcare operations and risk communication.

A great number of rankings of bio-pathogens are available. These rankings base on qualitative or (semi-)quantitative risk assessment methods. What seems important is that they greatly differ in preciseness, complexity and effort required for elaboration, while each ranking method has its benefits and disadvantages[63]. All in all, most methods define risk as the product of probability and impact (risk = probability x impact) of agent release. In other words, risk assessment takes into account both the uncertainties and the consequences of the natural, accidental, or deliberate event considered.

The KSÖ working group decided to use a semi-quantitative way of assessment instead of conducting a full quantitative risk assessment (QRA). This approach was chosen for several reasons. First, a stringent QRA (cf. Tomuzia et.al.[64], Radosavlevic et.al.[65]) depends on the quality of the underlying data. However, sufficiently precise and quantitative data is not, or not always, available for bioterrorist incidents or rare pathogens. Furthermore, QRA can be misleading in the case of terrorism, particularly

[63] Menrath, A. et al. Survey of systems for ranking of agents that pose a bioterroristic threat. In: Zoonoses and Public Health, 157-166.
[64] Tomuzia, K. et al. 2014. Development of a comparative risk ranking system for agents posing a bioterrorism threat to human or animal populations. In: Biosecurity and Bioterrorism, Vol. 11: pp. 53-66.
[65] Radosavlevic, V. & Belojevic, G. &Jovanovic, L. 2012. A Mathematical Model of Bioterrorist Attack Risk Assessment. In: J. Bioterror Biodef, Vol. 3(1):3.

bioterrorism, because expected values do not adequately capture events with low probabilities and high consequences. Traditionally, QRA are useful to manage the risk of industrial technologies and plants (e.g. nuclear power, oil, gas). In those cases historic data, causal modelling and computer simulations are available to derive probabilities with some level of significance. However, tools such as expected values or probability distribution are ill-suited for complex and uncertain risk situations such as terrorism and do not provide useful pictures of risk.

Semi-quantitative risk assessment

Semi-quantitative risk assessment is a compromise between the preciseness of the result and complexity and the duration of the work required. With a multidisciplinary group of experts it is possible to compensate for lacking data and to build a sufficiently strong knowledge base, including phenomena, processes, activities and systems being analysed.

QRAs depend on detailed and rigorous risk quantification, but quantification not only demands a quality database but often also requires strong simplifications. This might result in important factors being ignored or given too little weight in complex, uncertain and ambiguous risk situations such as terrorism. Therefore, introducing expert judgement could prove a tool to reduce uncertainty[66]. It allows for specifying context determinants as well as their likely changes, and for deriving motivations of potential terrorists. In a qualitative or semi-quantitative analysis a more comprehensive risk picture can be established by building scenarios,

[66] Renn, O. & Walker, K. Lessons learned. 2008: A re-assessment of the IRGC framework on risk governance. In: O. Renn & K. Walker (eds.). The IRGC Risk Governance Framework: Concepts and Practice. New York: Springer, 331-167.

assessing uncertainties beyond probabilities, and providing subjective scores of importance.

Moreover, experts from different institutions (health system, security authorities, emergency services) and multidisciplinary scientific background are able to develop a common understanding and language, which, in case of an emergency, will help to improve cooperation between decision-makers and stakeholders.

Semi-quantitative risk assessment based on expert judgement, particularly related to terrorism risk, has proven to be a useful method to achieve useful results in situations that require efficient and time saving analysis[67].

The risks of pandemics and emerging infectious diseases seem to be more calculable in terms of statistic probabilities. Nevertheless, also for these events semi-quantitative assessment is still appropriate because expert judgement can additionally include quantitative data as available. A coherent and comparative assessment of infectious disease threats assist risk managers in making robust and legitimate decisions for the whole spectrum of biological risks. This holds true, regardless of cause, for bioterrorism or natural epidemic emergence as well.

Semi-quantitative assessment of bioterrorist and pandemic risks

As mentioned above, the most frequently used form of risk definition is the product of probability and impact:

[67] Aven, T. & Renn, O. 2009. The role of QRA for characterising risk and uncertainty with emphasis on terrorism risk. In: Risk Analysis, Vol. 4:587-600.

Risk ~ Probability x Impact

For semi-quantitative assessment, the term 'probability' is not meant in a strictly statistical sense (as it is for QRA). It rather indicates the likeliness that an agent will appear as a biological threat. Therefore, the expert group decided to use the term 'plausibility' instead of 'probability':

Risk ~ Plausibility x Impact

For the assessment, the two criteria (or dimensions) of risk – plausibility and impact – are each considered to consist of sub-criteria. There are many ways to define sub-criteria and, of course, many more possibilities to further divide into sub-sub criteria. Therefore, a short description of the method chosen by the KSÖ expert is given below.

Impact comprises the sub-criteria infectiousness, method of delivery or transmission, lethality and vulnerability. Probability or plausibility incorporates parameters such as terroristic intention, technical or synthetic availability and access, natural re-emergence or accidental outbreaks and global transit of bioagents.

In addition, every sub-criterion itself is composed of multiple considerations. As an example, the key assessment issue, 'terrorist intent' encompasses several aspects. These aspects are the motivation (of a terrorist) to use a disease as a weapon, the technical capability to do so, the availability of a high impact agent, combined with an appropriate attack scenario and a high chance of success. 'Technical availability' considers possible access to a bioweapon from existing bioweapon stocks, rogue states, malevolent researchers and/or whether it could be reconstituted by means of biotechnology. 'Vulnerability' does not only reflect how the outbreak of a disease might impact health systems, social institutions and infrastructure. It also includes the

availability and effectiveness of countermeasures as well as the dimensions of robustness and resilience of health systems and of society.

Again, each of these sub-parameters of vulnerability can (and should) be split into subcategories of influence factors. For example, countermeasures comprise the availability of (early) diagnostics, the options of containment (disinfection, quarantine), prevention in humans (vaccines), and the treatment of humans (medicines) among others.

The method allows for a simple and quick reconsideration of single parameters or to include additional or emerging aspects when the context is changing. However, an interdisciplinary expert group has to agree upon a rationally structured and well-organized working process, in order to value a multitude of differing influence parameters in an efficient and productive way. In a series of workshops the KSÖ expert group first decided on a limited number of agents and diseases.

Subsequently, the selected agents and scenarios were discussed step by step. Finally, for each sub-criterion a value from zero to ten on a risk rating scale was assigned to each agent or disease as exemplified by the table in Fig. 1.

Criteria	Sub-Criteria	Influenza	Influenza*	SARS	Polio	Smallpox	Ebola	Anthrax	Anthrax*	VBD	Blister WA*	Nerve WA*
Impact	Infectiosity/ *contamination and spreading	7	7	3	7	9	5	6	6	2	3	3
	Dispersal/ transmissibility	9	9	3	6	9	3	1	1	2	2	2
	Lethality/ Morbidity	4	9	3	2	9	10	8	10	5	2	7
	Vulnerability	4	9	2	0	5	2	4	9	1	4	4
Plausibility	Intended/ terrorist/ -motivated release**	4	9	1	2	9	3	6	9	3	10	8
	Synthezising / *technical availability	9	9	3	7	8	7	8	8	1	10	10
	Natural recurrence/ mutation/ *technical failure	10	10	3	8	5	6	1	1	10	0	0
	Transit	10	10	6	6	3	2	1	1	2	9	9

Fig. 1: Risk rating scale (Kuratorium Sicheres Österreich)[68]

Ebola, as an example, is undoubtedly very lethal for any infected person. However, transmissibility is limited to direct contact or body fluid

[68] Kuratorium Sicheres Österreich. 2016. Contribution to the nation-wide risk analysis for Austria: biological, chemical, radiological and nuclear threats. Vienna.

exchange. The same applies for anthrax, whereas influenza, as a counterexample, combines a moderate lethality with high transmissibility and quick global transit.

This assessment results in a two-dimensional risk matrix with plausibility and impact. Importantly, the maximum risk is located in the right upper corner (Fig. 2).

At first glance, most risks lie somewhere in the middle of the risk matrix with influenza and smallpox more on the right upper side. The threat imposed by influenza is obvious, even though it is not widely noticed. Influenza emerges every year in the influenza season and causes several hundreds of thousands cases of disease. Several thousand of these infections result in patient death, mainly older and immunocompromised persons are affected.

The case of smallpox poses a special situation. After the eradication of smallpox in 1980, the vaccination programmes were discontinued. Therefore, the immunity of the population against smallpox has vanished in most countries. This could have dramatic consequences in case of a re-emergence of the smallpox virus. Even though all known smallpox stocks around the world were destroyed or transferred in one of two WHO reference labs in the US and Russia, the threat still persists. Apart from forgotten stocks that resurface in labs from time to time, it is theoretically possible to reconstruct the smallpox virus by means of modern biotechnology. Therefore, the threat of smallpox to public health, naturally occurring or deliberately released, must be considered high.

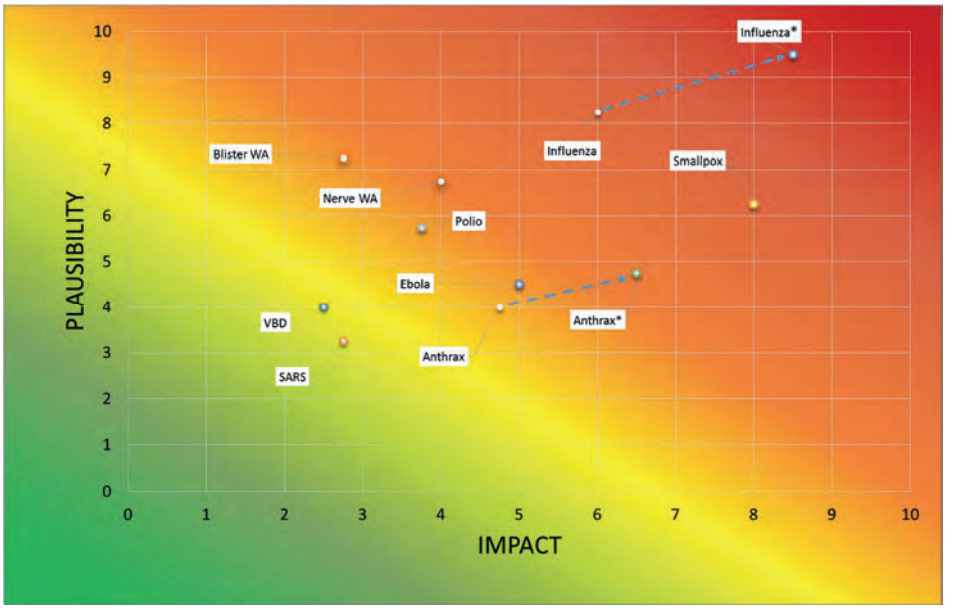


Fig. 2: Risk matrix for biological agents of natural or deliberate origin. The chemical agents Nerve WA and Blister WA are included for reason of comparison. Influenza and Anthrax* indicate increased risk presented by these agents after pathogenicity has been enforced by means of modern biotechnology (Kuratorium Sicheres Österreich)*[69]

To date, all known bioterrorist attacks have involved classical bacterial or toxin agents. Fortunately, the combination of motivation and capability that is required for a successful bioterrorist attack is rare.[70] For the foreseeable future, mass casualty threats with high level bioweapons (as described below) are not likely to arise from terrorist attacks. Therefore, the KSÖ report in a first step focuses on those well-known, classical bioagents for deliberate release or terrorist use as well as on known pandemic threats.

[69] Kuratorium Sicheres Österreich. 2016. Contribution to the nation-wide risk analysis for Austria: biological, chemical, radiological and nuclear threats. Vienna.
[70] Schallenberger, W. 2014. Bioterrorismus - eine aktuelle Gefahr?. In: R. Ö. f. L. u. Sport (ed.).: Biologische Bedrohungen: Gefahren aus Natur und Retorte. Korneuburg, 61-74.

Current technological advances – a future security challenge

Nevertheless, the advances in the life sciences trigger the question, whether and how the wide accessibility of knowledge and technologies will create new dual use and deliberate or terroristic risks. It is necessary to reassess the possible impact of the so-called new biotechnologies on biological threats. A few examples of recent and unanticipated science and technology achievements illustrate the situation. These examples of technological breakthroughs include DNA sequencing, synthetic biology, gene editing.

Today, DNA sequencing technologies allow reading a human genome sequence – 4-5 billion of nucleotides - for €1.000. Ten years ago the cost amounted to € 25.000.000. Genomic sequences of any organism – animals, plants, bacteria or viruses – are accessible in public data collections. The function of genes and gene complexes - including pathogenic ones – is increasingly known and ready to use in order to alter properties and metabolic products of microbes.

Based on sequence information, a master copy or blueprint, advanced DNA-synthesizing technology enables the reconstruction of entire viral genomes. Furthermore, it is possible to design new properties or to engineer altered pathways by means or synthetic biology. There are many threatening examples of how synthetic biology creates and modifies pathogenic organisms.[71+72]As early as 2002, the construction of a 'live' poliovirus using synthetic DNA segments and the available viral genome sequence was reported.[73] In 2005, the virus that caused the 1918 Spanish

[71] Casadevall, A. 2012. The future of biological warfare. In: Microbial Biotechnology, Vol. 5: 584-587.
[72] Tucker, J. B. 2011: Could Terrorist exploit Synthetic Biology? In: The New Atlantis - A Journal of Technology and Society, Vol. 31: 69-81.
[73] Cello, J. & Paul, A. & Wimmer, E. 2002. Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template. In: Science,Vol. 297:

influenza pandemic was reconstructed.[74] The most advanced techniques fifteen years ago are routine methods in today's laboratories. Currently, huge efforts are underway to advance sequencing technology from scientific research into a true manufacturing tool.[75]

Gene editing became another public buzzword. It describes the ability to target, study and change particular DNA sequences in any specific position in the vast expanse of a genome. Ever since the first genetic engineering experiments 40 years ago, 'actual' gene editing was a dream pursued by generations of life scientists. Some ten years ago, a technology named "zinc finger nuclease" emerged as the result of a breakthrough in research. Only a short time later it was followed by an even smarter technology named TALEN.

In 2012/2013, the so-called CRISPR technology emerged as a real game changer in the field of gene editing. The details of this technology would surpass the scope of this article. However, a few figures illustrate the drastic changes caused by CRISPR. To conduct one specific mutation, either the deletion or the insertion of genetic information, TALEN requires on average chemical assays costing some € 3.000 and 2 or 3 months of hard work on the lab bench. Finally, the method will deliver a success rate of 1 %. With CRISPR about € 50 for chemicals, 1-2 weeks of work in the laboratory result in a success rate 50% and more.

Just a few years ago, gene editing was exclusively accessible to a few high competence centres with huge financial funds. Today it is accessible to almost any lab and even interested students. It is available in the form of

---

2016-2018.

[74] Tumpey, T. et al. 2005. Characterization of the Reconstructed 1918 Spanish Influenza Pandemic. In: Science, Vol. 310:77-80.

[75] Leake, D. 2016. DNA synthesis steps up. In: Genetic Engineering & Biotechnology News April 2016:14-15.

commercial reagents, kits, and services. There is no need for expensive equipment and people do not need many years of training to do this.

These facts lead to the important issue of 'de-skilling'. Spread and advancement of enabling technologies could not only increase the risk of misuse, but also reduce the level of knowledge and skills required to perform biological attacks. However, whether this de-skilling process is or will be sufficient to make possible effective bioterrorist attacks by non-state actors is highly controversial.[76]

There is no doubt that the dramatic advances of modern biotechnologies are no longer material-based but information-based. Another trend is the convergence of biological and chemical production methods that could be misused to produce highly toxic chemicals in bacteria.

The danger of dual use research

The rapid pace of technological advances suggests that new technologies are likely to modify the range of biological weapons (and, of course, for biodefense) in coming years. In this context 'dual use research' leading to 'dual use risks' is of particular interest. Such research can be anticipated to provide knowledge, products, or technologies that could be directly misapplied by malevolent individuals or groups to pose a threat to public health, plants, animals, and the environment.[77]

The scientific community (and biosecurity experts) should give particular attention to 'experiments of concern'. This includes demonstrations on

[76] Jefferson, C.& Lentzos, F. &Marris, C. 2014. Synthetic biology and biosecurity: challenging the "myths". In: Frontiers in Public Health, Vol. 2:1-15.
[77] NSABB, N. S. A. B. f. B. 2007. Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information. Maryland: National Institutes of Health.

how to render a vaccine ineffective; conferring resistance to antibiotics or antiviral substances; enhancing virulence of a pathogen or rendering a non-pathogen virulent; increasing the transmissibility of a pathogen; altering the host range of a pathogen; enabling the evasion of diagnostic and detection modalities; enabling the weaponisation of a biological agent or toxin.[78]

But, and this could emerge as historic irony, the huge investments in biodefense research since 2001 have enormously expanded the number of scientists in such research fields with clear dual-use potential. Of course, the now large number of scientists with dual-use knowledge has not only increased our biodefense capabilities but also the statistical risk of misuse.

Today, there is an overall agreement that dual use research could pose a serious threat to public health.[79] Countries need to work on biosecurity strategies and to implement biodefense measures on national and international levels.[80] The EU Council adopted a first programme for improving cooperation in the European Union in order to prevent and limit the consequences of CBRN terrorist threats and renewed this effort by launching the so-called 'EU CBRN action plan' in 2009.[81] Today, just a few member states have already implemented appropriate and comprehensive steps to comply with this initiative.

Examples of potential for misuse

As mentioned before, many experts claim that the risk of novel bioagents being created by malevolent people experimenting with synthetic biology is

[78] NRC, N. R. C. 2004. Biotechnology Research in an Age of Terrorism. Washington, DC: National Academies Press.
[79] Lentzos, F. 2016. Biology´s Misuse Potential. In: Connections QJ, Vol. 15:48-64.
[80] Vogel, K. M. & Ozin, A. J.& Suk, J. E. 2015: Biosecurity and dual use research: gaining function - but at what cost? In: Frontiers in Public Health, Vol. 3:1-2.
[81] EU Council 2009. EU CBRN action plan, l.

very unlikely. However, the technology for significantly enhancing the lethality of existing biological weapons already exists.[82] More than just a few 'experiments of concern' were successfully undertaken in the past and they will more common in the future. A few examples of such 'high end' bio agents point in this direction and to how they could alter the risk compared to conventional pathogens:

The introduction of antibiotic resistance genes into bacterial agents could significantly enhance their lethality by reducing treatment options. In this regard, it is relatively simple to generate anthrax bacteria resistant to first line antibiotics. By assessing the potential impact of such an 'enhanced' microbe and the increased possibility of their deliberate use the position of 'Anthrax' will move to 'Anthrax*' (Fig. 2).

In 2011 two research groups[83] independently announced that they have created an aerosol transmissible variant of the H5N1 avian influenza virus. To date, the lethal avian influenza virus is known to be transmissible only through direct, physical contact with infected animals. Therefore, by combining high lethality with high transmissibility they created an influenza virus that could cause a deadly, global pandemic. The increased biological risk posed by such an influenza virus is illustrated in Fig. 2 by 'Influenza*' as compared to 'Influenza'. Of course, the threat posed by this mutation type could arise from natural emergence as well.

[82] Tucker, J. B. 2010. The Current Bioweapons Threat. Belgrade.
[83] Herfst, S. et al. 2012. Airborne transmission of influenza A/H5N1 virus between Ferrets. In: Science, Vol. 336: 1534-1541.

Another possibility was demonstrated unintentionally by genetically modifying viruses to express immune modifiers such as interleukins to block the efficacy of vaccines.[84]

Assessing the risks imposed by such 'high end' bioagents such as antibiotic resistant anthrax or airborne transmissible avian influenza will lead, not very surprisingly, to a significantly increased risk of each of the altered bioagents, as shown in Fig. 2.

Actually, the value of such assessment tools does not only lie in the visualisation of relative risks. It also helps to derive conclusions that affect preventive and countermeasures. For example, antibiotic resistance would increase the lethality of anthrax but also the motivation of terrorists to use it and the vulnerability of health systems. The semi-quantitative assessment tool makes it possible to differentiate the influences of contextual changes on relative risks. Therefore, asking the right questions might lead to a better preparedness. Therefore, in case of a future presumptive anthrax attack, it will not be important to know whether there is anthrax but whether there is genetically altered anthrax. Should antibiotic resistant anthrax be found by using quick and precise diagnostics, appropriate measures to treat and isolate infected individuals, protect first responders and uninfected persons can be taken in time.

In this context, it is important to emphasize that technological advances will not only change the scope of application for deliberate biological agent release or bioterror but also increase the defensive capabilities to prevent, detect and counter new biological threats.

---

[84] Jackson, R. J. et al. 2001. Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox. In: Journal of Virology, Vol. 75: 1205-1210.

Concluding remarks

Risk assessment is a tool useful for a broad range of decisions and activities to increase biopreparedness. However, it does not predict when, where and what disease will break out or whether accidental or deliberate misuse will occur. Given the different nature of the risks across the spectrum, a common approach incorporating specific scenarios coupled with an overarching model can be used for a unified risk assessment.

Naturally occurring pandemics, be it emerging (e.g. SARS, Ebola) or re-emerging (Influenza) have been continuing and will continue to be a real threat to public health. Health systems on a national and international level have successfully established pandemic preparedness and are steadily optimising prevention and healthcare measures to meet these challenges. However, naturally occurring diseases pose the greatest risk. Therefore, a focus on public health and health systems that encompass surveillance, detection, prevention, treatment is the most sensible way to address the full spectrum of biological risks.

No matter how likely bioterror might be, in the age of terrorism biological weapons are perfectly suited for asymmetric warfare, given their relatively low costs combined with potentially strong effects, both physiological and psychological, on targeted populations. Thus, in the near future we should continue to be concerned about classical biological weapons with limited efficacy. However, even if the absolute number of casualties is likely to be low, the impact of a bioterrorist attack can still be high.[85]

There is broad agreement between many international experts that the risk of 'high end' bioterrorism might be exaggerated, particularly in the United

[85] Janssen, H. & Breeveld, F. & Stijnis, C. & Grobusch, M. 2014: Biological warfare, bioterrorism, and biocrime. In: Clinical Microbiology and Infection, Vol. 20:488-496.

States. However, given the trends of technological advances and deskilling, it would be unwise to be too easy going and to ignore them completely. The dramatic advancement of biotechnologies with a potential for misuse increases the likeliness that more sophisticated bioterrorist attacks occur. At least, there should be a continuous observation and a regular re-assessment of associated risks to enable early detection of looming threats.

When considering bioterrorist risk, the key issues are intent and capability to use biological weapons. However, bioterrorist intent and capability pose the highest levels of uncertainty and, therefore, they are the most difficult parameters in any rational assessment. For this purpose, new forms of intelligence analysis will be required[86] to detect and identify them as early as possible.

The people most capable of harnessing advanced biotechnologies for harmful purposes are life scientists working in academic and industrial laboratories. The sole perpetrator of the 2001 anthrax attack was a respected microbiologist working in a biodefense laboratory of the United States Army. Since 2001, the number of researchers with relevant dual use knowledge has expanded enormously not least due to the public funding of biodefense research.

Contrary to nuclear or chemical agents, dual use risks in biotechnology are very high. With respect to all facets such as organisms, manufacturing devices and so on, there is a lack of unambiguous technical 'fingerprint' of bioweapon related activities.

The ultimate purpose of biological risk assessment is to show the best way of how to protect society. The sheer number of different threats suggests

[86] Vogel, K. M. 2013. The Need for Greater Multidisciolinarity, Sociotechnical Analysis: The Bioweapons Case. In: Studies in Intelligence, Vol. 57(3):1-10.

that attempts to achieve defence using microbe-to-microbe approaches to biodefence are impractical and inefficient. While no single countermeasure can be a 'silver-bullet', there is a need to prioritise responses that will have the most impact on the full spectrum of biological risks.[87] Assessing the risk reducing potential of different countermeasures and performing cost-benefit analysis could be used as a feedback for the assessment process and allow for strengthening overall bio preparedness.

[87] Royal Society. 2009. New approaches to biological risk assessment. London.

Emerging Security Challenges in Biology[88]

Filippa Lentzos

Key points

- Assessments of contemporary misuse risks in biology must have 1) a realistic understanding of the emerging technologies and the scientific practices surrounding them, and 2) a nuanced consideration of who the potential threat is coming from.
- The most significant risk of misuse of scientific advances in biology comes is state or state-supported use of sophisticated biological weapons.
- Another significant concern is the 'insider threat' from well-resourced biodefence programmes.
- Heavy military investments in emerging biotechnologies for defence purposes pose a final major risk of misuse serving as a cover-up for an offensive program or, more likely, being perceived as such.

Twenty-first century biology

Twenty-first century biology has been characterized by rapid advances and an increasing convergence of biology, chemistry, engineering, mathematics, computer science and information theory. There is also an increasing spread of capacity in biology around the world, particularly in emerging economies such as China and India, as well as increasing international collaborations, not only among researchers in scientifically developed countries and between researchers of developed and developing countries,

[88] Acknowledgment: This chapter has been adapted from Lentzos, Filippa. 2016: Biology's misuse potential. In: Connections – The Quarterly Journal, Vol.15(2):48-64.

but also among regional networks and, increasingly, among scientists within developing countries. The increasing transparence of science with new tools like wikis, blogs and microblogs is altering the way information is collected, handled, disseminated and accessed. All these developments increase the challenge for those tracking and assessing contemporary misuse risks of biology.[89]

The most recent assessment by the global network of science academies concludes that technological barriers to acquiring and using bioweapons have been significantly eroded over the last few years.[90] It is now easier to acquire both natural and synthetic pathogens. It is also easier to produce biological agents, and lab equipment can be fabricated using 3D-printing technology – though this is by no means easy. Less space and time are also required for scale up, and it is easier to conceal nefarious activities. Advances in nanotechnology and aerobiology, along with the use of chemical co-factors to increase uptake and formulations to improve absorption from the gastrointestinal tract, are making the dispersal and delivery of biological agents easier too. In short, the global network of

[89] IAP Global Network of Science Academies conference. 13–15 September 2015. The Biological and Toxin Weapon Trends Symposium. Warsaw: Polish Academy of Sciences.
IAP Global Security Working Group Meeting. 16 September 2015. Assessing the Implications of Advances in Science and Technology for the BTW 2016. Warsaw :Polish Academy of Sciences. (A summary is available under www.iapbwg.pan.pl).
Organisation for the Prohibition of Chemical Weapons. 2014. Convergence of Chemistry and Biology: Report of the Scientific Advisory Board's Temporary Working Group. The Hague.
National Research Council. 2011. Life Sciences and Related Fields: Trends Relevant to the Biological Weapons Convention. Washington, DC: National Academies Press.
The Biological Weapon Convention Seventh Review Conference. 5–22 December 2011. New Scientific and Technological Developments Relevant to the Convention. Geneva.
[90] IAP Global Network of Science Academies conference.13–15 September 2015. The Biological and Toxin Weapon Trends Symposium. Warsaw: Polish Academy of Sciences.

science academies argues that scientific advances "could facilitate almost every step of a biological weapons programme."[91]

Not all biological research causes concern. Various efforts have been made, particularly in the United States, to characterize biological research with high potential for misuse.[92] Examples of such 'dual use research of concern' include experiments that increase capacity to manipulate the pathogenicity, virulence, host-specificity, transmissibility, resistance to drugs, or ability to overcome host immunity to pathogens; to synthesize pathogens and toxins without cultivation of microorganisms or using other natural sources; to identify new mechanisms to disrupt the healthy functioning of humans, animals and plants; and to develop novel means of delivering biological agents and toxins. Early high-profile experiments that raised concern aimed at making mouse pox more deadly, synthesizing poliovirus from scratch and reconstructing the extinct 1918 flu virus.[93] More recently, entire fields of biological research have raised concern. These include synthetic biology and neurobiology.

---

[91] Ibid.

[92] For example: National Research Council. 2004. Biotechnology Research in an Age of Terror- ism. National Washington, DC: Academies Press.
National Science Advisory Board for Biosecurity. 2007. Proposed Framework for the Oversight of Dual-Use Life Sciences Research. Washington; US Government Policy for Oversight of Life Sciences Dual Use Research of Concern; March 2012; US Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern; September 2014. Available at http://osp.od.nih.gov/office-biotechnology-activities/biosecurity/ dual-use-research-concern:

[93] Jackson, Ronald J. et al. 2001: Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox. In: Journal of Virology 75.1205–1210; Wimmer, Eckard. 2006. The Test-tube Synthesis of a Chemical Called Poliovirus. The Simple Synthesis of a Virus Has Far-reaching Societal Implications. In: The European Molecular Biology Organization Reports – Special Issue 7:3–9; Tumpey, Terrence M. et al. 2005. Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus. In: Science 310:77–80.

Synthetic biology

Synthetic biology is an emerging field in life sciences that is often identified as the most susceptible one to misuse. The field aims at engineering biology, or "to designing and engineering biologically based parts, novel devices and systems, as well as redesigning existing, natural biological systems."[94] The aspirations and pace in the advance of synthetic biology have raised a number of security concerns. Some of these are legitimate, others less so.[95]

One of the most frequently cited concerns is that synthetic biology is making it easier to create dangerous pathogens from scratch. The claim is that well-characterised biological parts can be easily obtained from open-source online registries and then assembled by people with no specialist training outside professional scientific institutions, into genetic circuits, devices and systems that will reliably perform desired functions in live organisms. The assumption that synthetic biology makes it easy for anybody to 'engineer biology' is, however, not true. Academic and commercial researchers are still struggling with every stage of the standardisation and mechanisation process. More than a decade in, the translation of proof-of-concept designs into real-world applications is still a major challenge. As recently noted in the scientific literature surveying the progress in synthetic biology: "The synthetic part is easy, it's the biology part that's confounding."[96] And, even if the engineering approaches offered by synthetic biology make processes more systematic and more reproducible, skills do not become irrelevant, and all aspects of the work

---

[94] The Royal Academy of Engineering. 2009. Synthetic Biology: Scope, Applications and Implications. London:The Royal Academy of Engineering.
[95] Jefferson, Catherine &Lentzos, Filippa &Marris, Claire. 2014. Synthetic biology and biosecurity: Challenging the 'myths'. In: Frontiers in Public Health, Vol. 2: 115.
[96] Gardner, Timothy S. et al. 2014. Synthetic Biology: From Hype to Impact. In: Trends in Bio- technology 31(3):123–125 (quoted in Nature Reviews Microbiology 12(5):309).

do not become easier. In fact, 'easier' does not mean 'easy.' Aeronautical engineering provides a useful analogy: Planes are built from a large number of well-defined parts in a systematic way, but this does not mean that any member of the general public can build a plane, make it fly and use it for commercial transportation. Thus, advances in synthetic biology do not make it easier for just anybody to engineer biological systems, including dangerous ones.

This leads to the often raised second concern that synthetic biology is breaking down the boundary between experts and non-experts. In other words, the growth of a do-it-yourself biology (DIY bio) community, along with the fact that DNA synthesis is becoming cheaper and easily outsourced, could make it easier for terrorists to obtain the basic materials to create biological threat agents. However, the link between synthetic biology and DIY bio, as well as the level of sophistication of the experiments typically being performed, are grossly over-stated. There are also several challenges increasing the misuse potential offered by inexpensive DNA sequencing. While the "technology for synthesizing DNA" is readily accessible, straightforward and constitutes a fundamental tool used in current biological research, "... the science of constructing and expressing viruses in the laboratory is more complex and somewhat of an art. It is the laboratory procedures downstream from the actual synthesis of DNA that are the limiting steps in recovering viruses from genetic material."[97] Again, it is the biology and not the synthetic part that is complicated, and DNA synthesis requires extensive training in basic techniques of molecular-biology, such as ligation and cloning, including

[97] National Science Advisory Board for Biosecurity (NSABB). 2006. Addressing Biosecurity Concerns Related to the Synthesis of Select Agents. Bethesda, MD: National Institutes of Health, 4.

hands-on experience that is not "reducible to recipes, equipment, and infrastructure."[98]

A third frequently voiced concern is that synthetic biology may enable the design of radically new pathogens and that synthetic biology could be used to enhance the virulence or increase the transmissibility of known pathogens, creating novel threat agents. It is not that simple: Even experts have a hard time enhancing disease pathogens.

In sum, it is likely, in the near future, that synthetic biology will make it possible to create dangerous viruses from scratch. However, while synthetic biology is 'deskilling' science, it is not doing this to the extent that people with no specialist training operating outside professional scientific institutions can assemble biological parts into circuits, devices and systems that will reliably perform the desired functions in live organisms, and even professionals will have a hard time creating radically new pathogens or synthetic 'super-pathogens.'

Neurobiology

Neurobiology is another emerging area with high potential for misuse.[99] Military interest in neurobiology mainly relates to enhancement, involving efforts to improve the operational performance of national forces, and to

---

[98] Vogel, Kathleen. 2006. Bioweapons Proliferation: Where Science Studies and Public Policy Collide. In: Social Studies of Science 36(5):676.

[99] National Research Council. 2008. Emerging Cognitive Neuroscience and Related Technologies. Washington, DC: National Academies Press; The Royal Society. 2012. Neuroscience, Conflict and Security. London (http://royalsociety.org/ policy/projects/brain-waves/society-policy, accessed 20 January 2016) Requarth, Tim. 2015. This is Your Brain. This Is Your Brain as a Weapon. In: http://foreignpolicy.com/2015/09/14/this-is-your-brain-this-is-your-brain-as-a-weapon-darpa-dual-use-neuroscience/, accessed 20 January 2016.

degradation, involving efforts to diminish the performance of the enemy. There are security concerns about both enhancement and degradation.

There are various ways neurobiology might confer performance advantages in a military context.[100] One of these is through the use of neuro-pharmacological agents to enhance cognitive functions like perception, attention, learning, memory, language, thinking, planning and decision-making. There has been significant military interest in cognitive enhancement. Modafinil, for instance, is thought to have been used by the French army in Iraq in the early 1990s to combat fatigue, and by the US Air Force in 2003 to improve alertness and concentration during long flights. Military interest in sustaining and enhancing brain function and performance continues, as demonstrated by the large number of DARPA projects devoted to this goal. Neurobiology has also been identified by the UK Ministry of Defence as an important and rapidly developing field with potential relevance to defence and security.

Degrading enemy performance through neurobiology has focused particularly on the development of incapacitating biochemical agents or so-called non-lethal weapons. Incapacitants generally target the central nervous system to reduce alertness and, as the dose increases, produce sedation, sleep, anaesthesia and death; these are distinct from riot control agents, such as tear gas, which cause local irritation to eyes, skin and the respiratory tract, and have long been used by police forces around the world. There are indications of continued interest in incapacitating biochemicals among a number of states.

---

[100] The Royal Society. 2012. Neuroscience, Conflict and Security. London. (http://royalsociety.org/ policy/projects/brain-waves/society-policy, accessed on 20 January 2016). See: Chapter 4 "Performance Enhancement".

Concern over state interest in incapacitants was heightened following a case of actual use by the Russian Federation in October 2002. A group of armed Chechen separatists raided the Dubrovka Theatre in Moscow and took approximately 800 hostages. They demanded the withdrawal of Russian troops from Chechnya and threatened to kill the hostages if their demand was not met. Russian Special Forces disseminated an incapacitating chemical agent—reportedly a mixture of derivatives of the synthetic opiate fentanyl—through the ventilation system of the theatre, rendering both the hostages and the hostage-takers unconscious. Shortly afterwards, the troops stormed in, killing all of the hostage-takers and bringing the siege to an end. 129 of the hostages died from use of the incapacitant and many others suffered serious and long-term injury. The refusal of the Russian Special Forces to disclose the identity of the incapacitating agent at the time of the siege prevented emergency medical personnel from responding effectively.

Developments in anaesthetics and neuro-pharmacological drug research, coupled with developments in drug delivery, are making precise manipulation of neurological function increasingly feasible, and there are concerns about the risk incapacitants pose to the international ban on chemical weapons. Particularly relevant in the biological field are bioregulators and their synthetic derivatives. Bioregulators are special chemicals that carry messages from the brain to the rest of the body, between neurons or within cells, and modulate the function of the target cell or organ. They are naturally occurring biochemical compounds, such as hormones, neurotransmitters or signalling factors that control vital homeostatic systems, like temperature, sleep, blood pressure, heart rate and immune response. However, while they occur naturally in the body at low concentrations, they can be extremely toxic at higher concentrations or if the molecular structure is changed. While many bioregulators tend to be unstable in aerosolised form and are rapidly broken down by enzymes in the body, engineered variants could be synthesised, and considerable developments have taken place in the *in vitro* synthesis of bioregulators for

pharmaceutical purposes. Aerosol technology is also advancing rapidly and is already in use to deliver effective inhaled drug therapy for the treatment of disease. With advances in neurobiology, it may eventually become possible to develop modified bioregulators that can be disseminated over large crowds of people and that will cross the blood-brain barrier to induce states of sleep, confusion, placidity, fear, addiction or aggression.

The potential for misuse

There is a range of actors that could potentially misuse the new knowledge and tools gained through advances in science. These include national militaries, international terrorist networks, criminal groups, religious extremists, disgruntled or mentally ill scientists, or even biohackers, who are not necessarily motivated by politics or religion, but by curiosity, exacting revenge, payment or their own entertainment. However, not all of these actors are equally likely to take advantage of scientific advances.[101]

Few—if any—terrorist groups have the knowledge or scientific resources to create biological weapons. The number of attempts by terrorists to acquire and use these types of weapons is exceptionally small compared to the overall number of attacks that terrorists have conducted. Terrorists tend to be conservative and use weapons that are readily available and have a proven track record, not something like biological weapons that are more difficult to develop and deploy. While there is a risk of crude bioterrorist attacks or the use of 'scruffy' bioweapons, the likelihood that scientific advances—both generally and more specifically within synthetic biology and neurobiology—will be used to 'enhance' these attacks is relatively low. Many of the cutting-edge developments are expensive and/or complicated to acquire and deploy successfully.

---

[101] Koblentz, Gregory D. 2010. Biosecurity Reconsidered: Calibrating Biological Threats and Responses. In: International Security, Vol. 34(4):96-132.

Instead, the most significant security threat from the misuse of advances in the biological sciences is the potential for state or state-supported use of sophisticated biological weapons. There has been no state party use of biological weapons over the forty plus-year life span of the Biological Weapons Convention (BWC), which, together with the 1925 Geneva Protocol, 'forms' the biological cornerstones of the rules of war. Most experts agree that the potential for state use is very low, and there are good reasons for this: Biological weapons are not considered 'good' weapons. It is difficult to produce sophisticated and reliable biological weapons, and it is not politically viable to use them, because the norm against biological warfare—encoded in law through the BWC—is exceptionally strong. Yet, while the norm against biological weapons *is* strong, and the potential for state use *is* low, we cannot assume that biological weapons will not be used in the future. The likelihood that they will be used is not zero—and this is now coupled with the erosion of technological barriers and the possibility to acquire and use biological weapons. Synthetic biology and neurobiology could be used as means to create and deploy new and sophisticated biological weapons for new types of warfare.

Also of significant concern is the insider threat from well-resourced biodefence programmes. These programmes frequently focus on studying the characteristics of biological agents such as infectivity (the ability of a microorganism to infect a host), pathogenicity (the ability of a microorganism to cause disease), virulence (severity of the disease caused by the organism), and transmissibility (ability of the pathogen to spread from person to person)—all areas of biological research considered to have high potential for misuse. According to the Federal Bureau of Investigation, Bruce Ivins, a scientist at USAMRIID, the U.S. military's premier biodefense facility, was the sole perpetrator of the 2001 anthrax

letter attacks that sickened 17 and killed five.[102] *The World at Risk* report, released in December 2008 by the US Commission on the Prevention of WMD Proliferation and Terrorism, recommended that efforts to prevent bioterrorism focus less on the risk of terrorists becoming biologists and more on the risk of biologists becoming terrorists.[103] The report failed to emphasize, however, that not all biologists are of concern. It is the scientists working in areas of 'dual use research of concern' that are in the centre of interest.

Current military investments in synthetic biology and neurobiology are significant.[104] The majority of these funds is for basic science and do not come with security classification or publication restrictions. Indeed, many scientists view their defense-sourced funding on par with their other funding from, for instance, the National Institutes of Health or the National Science Foundation. From an international security perspective, however, the extensive influx of military funding is often perceived as a threat by analysts in other countries who are following these developments. Part of their concern is the military agenda behind the copious funding, and the purposes which the technology and its applications might serve, including the development of sophisticated biological weapons. A final major risk is that heavy military investments in emerging biotechnologies for defensive purposes are misused as a cover for an offensive programme, or, more likely, are perceived as such. The perception that another country

---

102 Department of Justice. 19 February 2010. Amerithrax Investigate Summary. Washington, DC: Department of Justice.

103 Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism (WMD Commission). 2008. World at Risk. New York: Vintage Books.

104 Lentzos, Filippa. 24 December 2015. Synthetic Biology's Defence Dollars: Signals and Perceptions'. In: http://blogs.plos.org/synbio/2015/12/24/synthetic-biologys-defence-dollars-signals-and-perceptions/, accessed on 14 September 2016.
The White House. 2 April 2013. Fact Sheet: BRAIN Initiative. In: https://www.whitehouse.gov/the-press-office/2013/04/02/fact-sheet-brain-initiative, accessed on 14 September 2016.

is using its biodefence programme to disguise an offensive programme may provide justification for initiating or continuing an offensive biological warfare programme.

Conclusion

Concluding, the assessment of threats from emerging biotechnologies, like synthetic biology and neurobiology has often taken place without a realistic understanding of the technology and the scientific practices surrounding it. What has also often been missing is a nuanced portrayal of who the potential threat was coming from. We must not present the results of horizon scanning exercises as present-day possibilities; we must not conflate the intentions of terrorists with the potential capabilities of state or state-supported programmes; we must not ignore the very real insider-risk from defensive military programmes; and we must be conscious of perceptions and signals in international relations.

4 Implications for Robotics/Cognition/ICT Technology

Artificial Intelligence and Cyber-Physical Systems: A Dangerous Mix?

Robert Trappl

The discipline 'Artificial Intelligence' was established in 1956 in a conference in the USA, it got its name from John McCarthy, an American mathematician. The papers presented at this conference were mainly about knowledge representation, logical reasoning, search algorithms, elements of learning and language understanding. AI developed more and more through faster and cheaper computers. But the breakthroughs has just recently come in the last ten years, when totally different methods were made possible by these fast computers. One of them is deep learning, which enabled computer programs like Watson or AlphaGo to compete and beat human champions in games like Jeopardy! or even Go.

What does this mean for us? First, it means better control. You have more chances to find information as soon as these programs are connected to the World Wide Web. For example, they can find information on court decisions, for which Watson is now being used, and they are better at tracing medical articles in different journals. They can also aid physicians in decision-making to an extent that was considered impossible a few years ago. It is very interesting that the first thing that springs to mind is *not* the possibility to control people better. It was already mentioned that Google collects an enormous amount of information.

Ten years ago the Austrian Research Institute for Artificial Intelligence (OFAI) co-developed a filter for postings with an Austrian newspaper. Before comments submitted by people are put online, a computer program checks them and determines which ones you can put online with certainty

and which ones should be rejected. Only between twenty and thirty per cent need human intervention to decide if putting them online could lead to legal problems.

In 2015, Google started the so-called Digital News Initiative, in which publishers of European online journals were invited to submit proposals for new projects to improve the distribution of news by new intelligent methods. Out of the about 1,200 proposals submitted, OFAI's proposal with an Austrian online-newspaper was among the 128 selected for funding. The idea was, rather than looking at the text in a rational, more formal way, to look for emotions. In recent times, online fora are increasingly flooded with insults is taking place, especially in the statements sent to news fora. Therefore, it became increasingly time-consuming to moderate the fora, to detect when this emotion-loaded situation reaches a stage in which it is necessary to intervene. OFAI proposed the development of a de-escalation bot that checks the discussion groups and as soon as a specified emotional level is surpassed, there will be an intervention. However, such a program could also be used to check emails for emotional content.

Furthermore, OFAI was a partner in a EU project called 'Emotions in Cyberspace', in which we developed a virtual barman with who it was possible to have discussions. The intention of the barman was to influence the mood of the person with who he had the conversation; for example, if the emotions of the person were at a medium level, to reduce it (to sadder) or increase it (to happier). Though the persons who interacted with this program knew that it was a computer program, it nevertheless had an impact on the mood of these persons. For example, with such programs it would be possible to influence newsfeeds that go to journals or newspapers. With such activities one could attempt to change moods, opinions, and decisions, in practically real-time.

One of the risks to be expected possibly earlier than 2025 is that hackers will not only be attempting to get codes or bank account numbers, but trying to influence opinions via such methods. It would be very difficult to detect this.

Robots are, at present, the most important cyber-physical systems. They are machines able to move, sense and interact. They come in different sizes, from very small – the size of a big fly- which is very difficult to detect, to very big ones. Surprisingly, some drones do not only have radars or ultra-sound devices or cameras, there are also drones that can 'hear'. One of the developed drones has directional microphones. It can fly over forests and detect and distinguish between the sounds of different kinds of guns (big guns, machine pistols etc.). And since it can locate the sound, even under trees, it can give information on where enemy forces strike.

Self-driving cars, tanks and trucks will very soon be common, animal-like robots that can creep through forests during the night are being developed. Flying robots, called 'drones', are now controlled in their actions by humans thousands of miles away from their targets. However, there are plans to give them some kind of autonomy of decision. And what about robot soldier? Are they being developed? The important question is: What should these robots be allowed to do autonomously? What about equipping them with an ethical system? In December 2015, I edited a book[105] that is essentially a construction manual for ethical systems for robots.

Many people are afraid that, in the long run, AI-systems and robots could become so smart that they can govern the world, including us humans. The British philosopher Nick Bostrom discussed this possibility in 2014[106].

---

[105] Trappl, Robert (ed.). 2015. A Construction Manual for Robot´s Ethical Systems. Switzerland: Springer International Publishing.

[106] Bostrom, Nick. 2014. Superintelligence: Paths, Dangers, Strategies. Oxford: Oxford University Press.

Several years before, in 2005, Daniel H. Wilson, a US-American AI researcher, also wrote a book, in which he deals with this question very humorously;[107] since then, the technology has been improved dramatically, and clearly not all of his tips would work today.

What has been missing in the development of artificial intelligence for a long time was the emotional dimension. Only the rational aspect of the human mind was dealt with, and the language. In the mid-1990s, psychologists found that, contrary to our assumption that having emotions is bad for rational decision-making, people who have weaker emotions or none emotions at all make worse rational decisions than persons who have emotions. Rationality and emotionality are not contradictory but mutually dependent.

Some experts say that the U.S. is planning to substitute about one third of their army with robots by the year 2020. However, it is more likely that this may happen in 2025 or 2030. The reason for this is very simple: For most politicians in democratic states the arrival of dead soldiers in coffins is one of the most horrible ideas! Therefore, most of them try to avoid military interventions, especially with land forces. Robot soldiers would enable states to be by far more offensive and to intervene much more often than now. Whether or not this is preferable is left to the reader.

Performing the complex tasks of soldiers, robots cannot be stupid mechanisms limited to shooting about. They need some kind of personality or character. One of several possibilities to program them to that end is the so-called Beliefs-Desires-Intentions (BDI) model. First, a robot has to have a belief system regarding how the world is constructed. It does not make sense to have only cameras if nobody sits in Texas and sees the pictures and then

[107] Wilson, Daniel H. 2005. How to Survive a Robot Uprising: Tips on Defending Yourself Against the Coming Rebellion. US: Bloomsbury Publishing.

acts. The robot has to have knowledge about the outside world, for example, about very simple physical facts. For example, a liquid object may be a wet spot on a pavement or deep water, so the robot might have to turn around etc. We have to provide the robots with common knowledge as we do with small children, but with children that takes years. Therefore, we have to develop a system of beliefs, which we then can transfer to every robot. Since we do not know exactly how 'the real world' really is and humans also act according to their beliefs of the real world, the term 'belief' is a better expression than 'fact', at least from a constructivist point of view. Among the beliefs that robots need to have is the information on how humans react or act under specific circumstances; furthermore, what human needs and desires are and how they are expressed in reactions and actions. Psychologists and AI researchers call this a 'Theory of Mind'. They also need it because they must be able to interact and coordinate their actions with human soldiers. The 'Theory of Mind' encompasses more than a system of beliefs; it also contains Desires and Intentions. Robots, too, need to have desires. An important one for robot soldiers will have to be the disabling of enemy soldiers, making PoWs, and protecting civilians. Depending on the actual beliefs about a situation, different desires will lead to different intentions and acts—a very complex structure, also known to us humans, who served as basis for this model.

A specific problem not only for robots but also for humans is the fact that beliefs and desires and the resulting intentions and acts are, to some extent, culture-specific. An example is the challenge we Austrians faced when in 2015 about 90,000 refugees from various different cultures asked for asylum, which meant that most of them would stay in Austria for shorter or longer periods or even forever. Bearing in mind that many conflicts arose when human soldiers ignored culture-specific behaviour in foreign countries, the belief base of soldier robots has to take care of these differences from the beginning.

Finally, I would like to mention a book that was one of the results of more than ten years' work by several scientists. This book, which I published in 2006, has the title 'Programming for Peace: Computer-Aided Methods for International Conflict Resolution and Prevention'[108]. Having experienced the horrors of the second world war as a child—I was born in 1939—and having read about war games in the 1990s, my primary idea was: If AI can be used to enable more 'efficient' warfare, could AI not also be used to prevent the outbreak of wars or, if armed conflicts are already going on, aid decision-makers in trying to end them? My group at the Austrian Research Institute for Artificial Intelligence (OFAI), in cooperation with scientists from the University in Heidelberg, Germany, and the University of Canterbury, New Zealand, used their databases to compare the new conflict or war with many other conflicts to find the most similar one (case-based reasoning) and see what has helped to end this conflict. The other approach developed decision-trees starting from a large conflict-management database with detailed descriptions of several thousand conflict management attempts and their results. These decision-trees were the bases for finding the conflict management method for a new conflict or war that had the best chance to end this situation peacefully.

As already mentioned, the book was published ten years ago. There has been huge progress in the field of AI since then. In addition, the structure of most armed conflicts today is different from those 10 or 20 years ago. Maybe similar attempts are undertaken somewhere else. I have not consulted the literature for some time; any such references are most welcome. I personally think that the situation we have now would justify using current AI-methods and databases that are non-classified to give this idea another try, with hopefully even better results.

---

[108] Trappl, Robert. 2006. Programming for Peace: Computer-Aided Methods for International Conflict Resolution and Prevention. Netherlands: Springer Verlag.

Multinational Robotic Wars –The Increasing Use of Unmanned Systems by State and Non-State Actors in Current and Future Conflict Zones

Markus Reisner

With the start of the 21st century, autonomous, unmanned and unarmed systems operating from the sky as well as robots operating on the ground or on water became indispensable assets for modern violent warfare.[109] Their deployment varies depending on the broad range of scenarios and tasks. Such systems enable real-time insight on the situation on the ground or disablement of dangerous bombs, but also targeted destruction and killing. Carrying weapons they are used more and more for the latter. The high functionality and ability to carry weapons lead to a high dependence of the military on the availability of such systems.[110] More and more terrorist groups as well as non-state organisations (with doubtful interests) are discovering the use of those systems. Therefore the deployment of drones is not restricted to industrialised countries. On the contrary: Easily operable technologies constitute a tool for the common man. Few simultaneously deployed *Quatrocopters* with minimal capacity but loaded with explosive material might be sufficient to destroy a target, there being no need for a sophisticated armed drone.

On 16 February 2001, a surface-to-air missile, type *AGM-114 Hellfire,* was fired for the first time successfully by an American drone

[109] King, Anthony. 2011. The Transformation of Europe´s Armed Forces: From the Rhine to Afghanistan. Cambridge University Press. 5.
[110] Scahill, Jeremy. 2013. Dirty Wars: The World is a Battlefield. New York: Nation Books. 48.

(Unmanned Aerial Vehicles, UAV) type *MQ-1 Predator*[111]. In the year 2001, responsible technicians and constructors of the US-Airforce as well as General Atomics were not aware of the ground breaking importance of this event[112], but the terror attacks of 11 September 2001 were followed by fast developments in this field. Already in October 2001 the first armed mission of a *Predator* was launched over Afghanistan. On 4 March 2002 a *Predator* was used for the first time to support U.S. ground troops in the U.S. operation *ANACONDA*. From 2001/02 onwards *Predator* was used in Iraq and Yemen as well as in 2003 in Pakistan. The attack in Yemen in November 2002 by a *Predator* was the first attack by a drone in the course of the *Global War on terror* outside Afghanistan.[113] In June 2004, the first targeted killing by a *Predator* was carried out on Pakistani national territory. [114] More operations with *Predator* followed in Somalia (2011 against the terror organisation *Al-Shabaab*) and on the Philippines (2006 and 2012 against the terror organisation *Abu-Sayyaf*). As of 2007, the first UCAVs of the type *MQ-9 Reaper* are successfully operating. It is capable of transporting significantly more weapons than *Predator*.[115]

As for the development of unmanned flying systems, it was the events of 11 September 2001 and the following interventions of international

---

111 *Unmanned Aerial Vehicles (UAV), t*ype *Predator,* are operated as an unarmed intelligence version (RQ-1 = *UAV*) and an armed version (MQ-1 = *UCAV*). *UAV* or *UCAV* of this size are called *Medium Altitude / Long Endurance* (*MALE*) systems.

112 Dusseault, Christopher G. (Program Director Predator XP, General Atomics Aeronautical Systems): Defining the Future of Innovation – Taking a Deliberate and Integrated Approach to Unmanned Systems Acquisition and Technology Development. Panel discussion at the Conference & Exhibition for Unmanned Systems 2016 (UMEX 2016). Abu Dhabi (VAE) 6 March 2016.

113 Whittle, Richard. 2014. Predator – The Secret Origins of the Drone Revolution. New York: Henry Holt and Company. 302-303.

114 Ibid. 232.

115 Ibid. 299.

coalition forces in Afghanistan and Iraq that also lead to significant developments and a wider range of deployment of Unmanned Ground Systems (UGS). International troops in Afghanistan and Iraq were confronted with Improvised Explosive Devices (IED). *UGS* were employed as a first reaction to this kind of threat. After a short time, a whole family of such systems, of different sizes and specialised in different tasks, emerged. At the peak of the international operation in Afghanistan in 2010, an average of one *IED* incident occurred out of seventeen conducted supply convoys. [116] *UGS* were recognised as possible solutions; on the one hand for intelligence about suspicious objects and recognition and disarmament of an *IED*, on the other hand for the transportation of military supply through unmanned vehicles. [117]

In some fields of operation the special conditions on the ground demand for a higher degree of autonomy of those systems; i.e. unmanned maritime systems deployed under water. Remote control is very limited because of the medium water. Some scientists therefore expect the first fully autonomous systems to be deployed under water.[118] Not to be forgotten in the list of unmanned systems in the air, on the ground and under water is the cyber space as a possible conflict zone. Operations at the speed of light require software that can operate highly autonomously. Therefore, partly autonomous programs are being developed in the cyber domain as well, which are expected to be used especially in the conduct of Computer Network Operations (CNO). Due to information leaks by Edward Snowden, employee of a company working for the American National Security Agency (NSA), it became

[116] Mets, David R. 2009. Airpower and Technology, Smart and Unmanned Weapons. In: US Department of Defense (ed.). Unmanned Systems Integrated Roadmap FY2013-2038. 6.
[117] Ibid. 15, 19.
[118] Tucker, Patrick. 2015. Will Subdrones Cause World War III? In: http://www.defenseone.com/technology/2015/09/will-subdrones-cause-world-war-iii/120383/?oref=d-topstory, accessed on 08 February 2016.

public that the NSA is working on a programme called *MonsterMind*. The purpose of this program should be the early detection and neutralisation of cyber-attacks on the U.S. Because of the high speed with which such operations are conducted the goal is to deploy the program in a fully autonomous mode.[119] These examples show how highly capable troops and weapons companies that also have the required resources are already working with high pressure to further develop the degree of autonomy of unmanned systems. The battlefield of the future is reserved for *this* robot.

Drones in particular have been the focal point of public discussions over the past few years. During the Bush Administration, end of 2001 to the end of 2008, 48 targeted killings through American drones became publicly known. Between 2009 and 2013, during the Obama Administration, 307 operations in total were documented, 122 only in the year 2010. This represents an enormous increase.[120] More U.S. drone bases were established in the Middle East and Africa. UCAV attacks have been expanded over Pakistan, Yemen and Somalia. Terror organisations, like the Somali *Al-Shabaab* militia were targeted and it became less and less important for a strike whether the target person was clearly identified. Also, civil victims, so called collateral damage, were knowingly tolerated. Furthermore, the conduct of 'signature strikes' was mentioned. In the year 2012, former U.S. president Obama authorised the fight against targets based on their 'signatures', the behavioural patterns of a target person that is derived from intercepted phone calls, open information sources and targeted aerial intelligence.

---

119 Zeter, Kim. 2014. Meet MonsterMind, the NSA Bot That Could Wage Cyberwar Autonomously. In: http://www.wired.com/2014/08/nsa-monstermind-cyberwarfare/, accessed on 10 February 2016.

120 Rudolf, Peter. 2013. Präsident Obamas Drohnenkrieg. In: Stiftung, Wissenschaft und Politik (SWP), SWP-Aktuell, Vol. 37. Berlin: Deutsches Institut für internationale Politik und Sicherheit, 5.

This information constituted the basis for intelligence regarding the probability that a specific person was at a specific location at a defined time.[121]

The United States of America, Israel and Great Britain are most certainly the most advanced in the deployment of armed drone systems. Nevertheless, other states keep up in development and procurement. France, Italy, Morocco and the United Arab Emirates employ U.S. MALE drones[122] in their operations or are close to employing them. Since 2015, for example, the Italian Air Force has been employing armed *Predators* in the fight against the IS. France uses unarmed drones of the type *EADS Harfang,* amongst others. Also, France successfully procured the American *Predator* and employed it in Mali. Especially in the uneven terrain of the desert region in the north of Mali the armed drone of the type *Reaper* was very successfully operated by French troops. [123] Germany, on the other hand operates leased Israeli unarmed intelligence drones of the type *Heron* in Afghanistan. Apart from western industrialised nations, other states are keeping up. Turkish troops, for instance, possess a MALE drone *TAI Anka*, which was developed and produced in Turkey. As concerns small drone systems almost all modern industrialised nations and their troops have different systems at their disposal, so do Austrian troops. [124]

---

[121]Miller, Greg. 2010. US citizen in CIA´s cross hairs. In: http://articles.latimes.com/2010/jan/31/world/la-fg-cia-awlaki31-2010jan31, accessed on 12 November 2015.

[122] Medium Altitude Long Endurance (MALE).

[123] Colonel Fontaine, Christoph (Direction du Renseignement Militaire, Ministére des la Défense, République Francaise): Defining the Future of Innovation – Taking a Deliberate and Integrated Approach to Unmanned Systems Acquisition and Technology Development. Panel discussion at the Conference & Exhibition for Unmanned Systems 2016 (UMEX 2016). Abu Dhabi (VAE) 6 March 2016.

[124] The Austrian military already has intelligence drones, types *Tracker* (French production), *Huginn* (Danish production), demining robots, type *DOK-Ing* (Croatian production), as well

Drones seem to be the perfect tool for the military and for politics in the fight against *asymmetric* and *irregular* warfare. [125] Consequently, the U.S. troops' inventory of UAV increased to almost 11,000 of different categories in ten years. [126] Most of the systems deployed in 2013 (almost 9,800) are UAV (or UAS) of the first class *Group 1*, smaller type, with up to nine kilogrammes total weight. Nevertheless, in the year 2013, 237 UAV/UCAV of the types *RQ-1/MQ-1 Predator* or *Grey Eagle* (class *Group 4,* total weight over 600 kilogrammes) and 112 UAV *of the* type *MQ-9 Reaper* (class *Group 5,* total weight also over 600 kilogrammes) have been in operation. Globally deployable and armed with air and ground rockets those almost 350 UAV or UCAV represent an enormous potentiation of the force and capacity of U.S. troops.[127] In Afghanistan and Iraq (but also in Yemen, Pakistan and Africa) it was possible, via deployment of unmanned systems, to compensate for capacity gaps and a shortage of soldiers. [128]

Russia and China are also in possession of their own systems and development programs. China's military forces, for example, are already using MALE UAV of the types *CH-4* and *HALE*[129]. The UAV of the type *Soar Dragon* successfully developed by the Guizhou Aviation Industry Group (GAIC).[130] Russia's military forces especially have a

---

as *tEODor* (US production), at its disposal. Also, the Lower Austrian company Schiebel is a potential actor in the developing of helicoptor drones, type *S-100 Camcopter* (cf. www.schiebel.com). The Upper Austrian company Rotax is producing engines, type *Rotax 914 TC*, i.e. for the UAV, US type *MQ-1 Predator* (see www.rotax.com).

125 Martin, Matt J.2010. Predator: The Remote-Control Air War over Iraq and Afghanistan: A Pilot's Story. Minneapolis: Zenith Press. 5.

126 Mets, David R. 2009. Airpower and Technology, Smart and Unmanned Weapons. In: US Department of Defense (ed.). Unmanned Systems Integrated Roadmap FY2013-2038. 7.

127 Ibid.

128 Gates, Robert M. 2014. Duty. Memoirs of a Secretary at War. Alfred A. Knopf, Inc. 125.

129 *High Altitude Long Endurance (HALE).*

130Fisher, Richard D. 2016. Guizhou unveils box-wing UAV concept. In: http://www.janes.com/article/62178/guizhou-unveils-box-wing-uav-concept, accessed on 10 August 2016.

number of different operational small drone systems at their disposal. Furthermore, small drones of Russian production (type *Forpost* und *Orlan-10*) were captured in summer 2014 in the Donbass region by Ukrainian military forces.[131] Subsequently, since 2015, different small drone systems have been purchased and employed by Ukraine. The Austrian company Schiebel leased drones of the type *S-100 CAMCOPTER* to the OSCE (Organisation for Security and Co-operation in Europe) in the course of their monitoring mission in the Donbass region. Unfortunately, they became victim of successful counter measures. [132] On 7 September 2015 Pakistani military forces announced the firing of a surface-to-air missile of the type *Barq* from a UAV/UCAV of the type *Burraq* for the first time. The detonation of the missiles is believed to have killed three Taliban fighters in Shawal valley in the border region between Pakistan and Afghanistan.[133]

Iran probably also has armed drones. An Iranian UAV of the type *Shahed*-129 was presented to the public for the first time in 2012. Only one year later, a video was published that shows a *Shahed*-129 firing a surface-to-air missile. In 2015 Iraq successfully deployed armed Chinese UAV/UCAV of the type *CH-4B* against IS targets. Apart from Iraq, Egypt, Qatar and Nigeria possess the Chinese UAV type, which is another good example of the increase in the export of drone systems of different types and sizes.[134] It is only a matter of time until rebel or

---

131 Krushelnycky, Askold. 2015. Ukrainian Forces recover downed Russian Drone. In: https://theintercept.com/2015/02/17/russian-drone-shot-ukraine, accessed on 13 March 2016.

132 Mader, Georg. 2016. UAV losses to hostile fire leave OSCE without eyes over eastern Ukraine. In: http://www.janes.com/article/65139/uav-losses-to-hostile-fire-leave-osce-without-eyes-over-eastern-ukraine, accessed on 3 November 2016.

133 Bokhari, Farhan. 2015. Pakistan claims first airstrike with indigenous UAV. In: IHS Jane´s Defence Weekly, Vol. 52 (37):5.

134 Binnie, Jeremy. 2015. Iranian Shahed-129 UAV crashes. In: IHS Jane´s Defence Weekly, Vol. 52 (34):18.

terrorist movements will have potent unmanned systems at their disposal. Comparably small drones of different types have, for example, been repeatedly operated by Hamas and Hezbollah over Israel, by the *IS* in Iraq and Syria and by pro-Russian separatists in eastern Ukraine since 2012. [135] In 2012, Hezbollah started an Iranian MALE UAV of the type *Shahed-129* from Lebanon, which flew successfully across Israeli territory. Only then the Israeli Air Force was able to take it down. The operation of such systems by Hezbollah represents an unpleasant surprise for the Israeli Defence Forces (IDF). [136] Two years later, several drones of Hamas were successfully taken down during the IDF operation *PROTECTIVE EDGE* in Gaza. [137] The IS heavily wounded two French soldiers by deploying a drone equipped with explosives in October 2016. [138] In December 2016, *Quatrocopter* drones were found in the possession of the *IS* in the fight of Mosul in Iraq, provisionally equipped with explosives of anti-tank missiles of the type *RPG-7*. Not only small drones were deployed, also remotely controlled cars equipped with explosives were operated by the IS. [139]

---

135 Zucchino, David &Vartabedian, Ralph. 2014. Hamas drone injects new element into Arab-Israeli conflict. In: http://www.latimes.com/world/middleeast/la-fg-hamas-drone-20140715-story.html, accessed on 13 November 2015.

136 Ryan, Missy. 2015. U.S. drone believed shot down in Syria ventured into new area, official says. In: https://www.washingtonpost.com/ world/national-security/us-drone-believed-shot-down-in-syria-ventured-into-new-area-official says/ 2015/03/19/891a3d08-ce5d-11e4-a2a7-9517a3a70506 _story.html, accessed on 13 March 2016.

137 Bregmann, Ahron. 2016. Israel´s Wars – A history since 1947. New York: Routledge. 326.

138 Schmidt, Michael S.& Schmitt, Eric2016. Pentagon Confronts a New Threat From ISIS: Exploding Drones. In: http://www.nytimes.com/2016/10/12/world /middleeast/ iraq-drones-isis.html?_r=2, accessed on 12 October 2016.

139 Capaccio, Anthony. 2016. Extensive Islamic State Drone Use Raising Risks in Mosul Battle. In: https://www.bloomberg.com/news/articles/2016-10-26/extensive-islamic-state-drone-use-raising-risks-in-mosul-battle, accecssed on 26 October 2016.

Almost 15 years after the deployment of the first armed drone type *Predator,* deployment of unmanned systems became an undeniable fact in the present theatres of war. Not merely operated by military troops and secret service of powerful Industrial Nations but also rebel and terrorist movements. The possibility to globally and in real time kill by pressing a button renders the use of drones more and more an accepted political measure of demonstration of military power of potent military nations. The life of national soldiers can be spared by the deployment of surface-to-air systems. The presumed terrorist or undercover operating opponent is forced to seek 'protection' under civilians on the other hand. He takes cover in the population where he, at least to some parts, is supported. Even with the most precise weapons he is very hard to fight without taking into account civilian victims and even a high flying armed drone cannot ensure the desired result. Moreover, additional civil victims encourage counterinsurgency or people joining terror networks, therefore generating more opponents.[140]

The deployment of unmanned weapons systems makes tactical and operational success possible; however, strategically the opposite might be the case. As it is not possible to identify every single opponent or completely avoid civilian casualties - not even via thoroughly prepared safety measures - the death of every innocent person might have far-reaching consequences. This leads to a dilemma, which is not totally solvable by unmanned weapons systems. A targeted killing of the leaders of rebel movements or terror groups is most likely to turn out as a pyrrhic victory. Unmanned systems are more and more used by the opponents, too. They do not possess the capacity to use a technologically highly complex MALE drone system.

---

[140] Corthright, David & Fairhurst, Rachel &Wall, Kristen (eds.). 2015. Drones and the Future of Armed Conflict – Ethical, legal and Strategic Implications. Chicago: University of Chicago Press.

However, as it can be observed in Iraq, there is sufficient capacity to operate a *Quatrocopter* drone of a few kilos equipped with explosives. Irregular forces and terrorists do not fight according to determined norms or processes, but in view of the constraints imposed by the surroundings and the opponent (the international military forces).[141]

Since the crisis in Ukraine in summer 2014, a new term has become popular in security policy and military discourse: rather than talking about *irregular* or *asymmetric* warfare, the term *hybrid* warfare has been used. Initially, William J. Nemeth used this phrase for the first time in 2002; in 2007 American political scientist Frank G. Hoffman coined the term more precisely.[142] Hybrid warfare describes a combination of procedures and resulting events that have been attributed in particular to the developments in Ukraine.[143] Any military strength or superior weapon system of the opponent is countered by an unconventional solution based on available resources (i.e. self-made booby traps, suicide bombers). Autonomous unmanned systems represent a viable multiplier for both sides, with unlimited possibilities of deployment. Unmanned systems offer a variety of possibilities for all actors: modern

---

141 Stahel, Albert A. & Geller, Armando. 2004. Asymmetrischer Krieg: Theorie – Fallbeispiel – Simulation. In: Schröfl, Josef & Pankratz, Thomas (eds.): Asymmetrische Kriegführung – Ein neues Phänomen der internationalen Politik. Baden-Baden: Nomos Verlagsgesellschaft. 95.

142 Hoffmann, Frank G. 2009. Hybrid vs. Compound War. In: Armed Forces Journal, October 2009. http://armedforcesjournal.com/hybrid-vs-compound-war/ accessed on 23 November 2015. Hoffmann defines *hybride* warfare as: "Any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives." See also: European Union Institute for Security Studies (EUISS): What we talk about when we talk about "Hybrid Threats". Paris 2015.

143 Schröfl, Josef & Rajaee, Bahram M. & Muhr, Dieter (eds.). 2011. Hybrid and Cyber War as Consequences of the Asymmetry: a Comprehensive Approach Answering Hybrid Actors and Activities in Cyberspace. Political, Social and Military Responses. New York: Peter Lang.

international military forces, national police forces, but also terrorists. Human inventive spirit knows no limits. First signs already point to the beginning of a technology race. The weapon industry advertises newly developed defence systems of small drones that can be used universally by the military, the police, abroad and on national territory. Therefore, unmanned systems, drones and robots will play a huge role in *irregular, asymmetric* and *hybrid* warfare in the future.

Internet Use in Times of Change – Demand for Innovative Security Measures

Reinhard Posch

The way that people use the Internet has significantly changed over the past years. Compared to the situation of only a few years ago, users' communicative behaviour, devices, but also the entire field of data storage have greatly changed. Usually, the security issue is added to a scenario only later on. However, we urgently need a forward-looking security system that is integrated into the systems from the very beginning.

On the European level, both the NIS Directive[144] and the eIDAS Regulation[145] have contributed significantly to this new awareness. In this sense, it will hinge not only upon the rapid and comprehensive implementation of these regulations, but also on the take-up by the member states and especially by the private sector.

Another significant aspect of change in this respect is the headway made in the field of the 'Internet of Things'. Not only communication intensity, but especially the new security issues will force us to face new risks in an ever-growing volume of data, which in the future will be many times larger than today. However, we must also see the remarkable chances inherent in this development, be it in the field of critical infrastructure or in situations of emergency.

---

144 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

145 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

We shall have to pay special heed to ensuring that communication increasingly adheres to the respective statutory norms, thus avoiding critical situations from the outset. Our general aim must be to strengthen proactive security measures, also on the basis of cryptographic processes strong enough to withstand any attempts to breach them.

Why do we need change?

The security landscape has not only become more differentiated, but also much more complex. In general, we have to assume increasingly complex technologies. However, we will have to pay even more attention to limit the effect of disruptive changes with security assumptions.

Different communicative structures and thus much more complex security processes have become necessary as people's use of information and communication technologies has changed dramatically over the past years. Not only has the significance of text compared to that of spoken discourse decreases considerably, but people are also using different structures today, replacing one-to-one with a more open one-to-many communication. For the first time ever, the private sector has been a pioneer in the utilisation of innovative communication infrastructures. Nevertheless, the underlying contracts are usually quite complicated and mostly unknown to users, who rarely make an effort to keep track of all these continually changing contractual provisions and amendments prior to use.

Not only have people's communicative behaviour and habits changed dramatically over the years, but also the technical structures are completely different these days. The path of change wound its way from the large mainframe computer – whose entire system was familiar to the system administrator, who also knew how to adapt it, via the so-called

PC, uniting a variety of different software programmes in a single and naturally unsafe system – to the now predominant and popular mobile devices. In this sense, the development can be characterised by changes in proprietary standards, apps in containers, and thus by a loss of control and influence on the end user's part. This development is still continuing, culminating in the fact that with the Internet of Things, the boundaries between hardware and software are becoming blurred.

Likewise, this lack of transparency from the point of view of the end user can also be extended to the field of data itself. A good example of the fact that end users are only vaguely aware of such developments are push notifications, which are mostly conveyed via third countries and often communicate personal data which is then stored there. Thus it is extremely difficult to ascertain, both in legal and technical terms, where data is stored or processed. If, for the sake of self-protection and for sustaining regular business operations the provider uses data encryption, the user is normally unaware of the encryption key and the organisations or staff who use, manipulate or pass this key on.

At this point, the question of trustworthiness arises; does the system ensure data protection and privacy in the long run?

Worldwide Smartphone Sales to End Users by Operating System in 1Q16 (Thousands of Units)

Operating System	1Q16 Units	1Q16 Market Share (%)	1Q15 Units	1Q15 Market Share (%)
Android	293,771.2	84.1	264,941.9	78.8
iOS	51,629.5	14.8	60,177.2	17.9
Windows	2,399.7	0.7	8,270.8	2.5
Blackberry	659.9	0.2	1,325.4	0.4
Others	791.1	0.2	1,582.5	0.5
Total	**349,251.4**	**100.0**	**336,297.8**	**100.0**

Fig.2 : world wide smartphone sales[146]

NIS proactive security as the optimum solution

When observing the developments in the sector, we inevitably come to the conclusion that the only sustainable strategy is long-term proactive security. Ideally, we would be able to do away with CERTs (Computer Emergency Response Teams) – but unfortunately we are miles away from that. Rather, the opposite is the case. So far the number of CERTs increased continuously and this trend will go on.

[146] Gartner 2016. Gartner Says Worldwide Smartphone Sales Grew 3.9 Percent in First Quarter of 2016. In : http://www.gartner.com/newsroom/id/3323017, accessed on 19 January 1017.

However, we will not be able to sustain this development very long, which is why we need a forward-looking, proactive approach to IT security in the very near future.

In this respect, the NIS Directive has made a significant contribution to the way we have been coping with security incidents, especially in recording, evidencing and communicating IT security breaches across the member states. Thus, we have gained the ability to react to such incidents swiftly and with limited effort. Nevertheless, in the course of the discussion the Directive has slowly given priority to reporting, thus nearly neglecting other measures of equally high importance.

The Directive, which was passed on 6 July 2016 by the European Parliament, aims to put common network and information security on an unprecedentedly high level of priority. This means that the member states will have to prepare themselves accordingly.

Mainly, such preparations include the establishment of a Computer Security Incident Response Team (CSIRT) and a NIS authority in each member state. On the European level, this will be complemented by a cooperation group intended to facilitate the exchange of information and to enable its members to learn from each other's experience. The national Computer Security Incident Response Teams will be supported and supplemented by a European network.

This urgency is also reflected by the fact that at the time the Directive was passed, it was already permitted to start actual projects on the European level, especially within the general framework of the Connecting Europe Facility Programme (CEF). With the SMART programme, common tools are being developed that will be put at the disposal of all member states (CSIRTs) to facilitate their work in the field. These measures are especially supported by the Commission, also with regard to financing.

eIDAS identity and a lot more

Internet security without identities is unthinkable. To access the Internet for the purpose of online shopping or communicating, users are required to identify themselves. However, this aspect, which, unless handled with sufficient care, can easily become a point of weakness, is often sorely neglected. As has been shown again and again, activities of a certain type require more than a user ID and a password to protect citizens. Through the eIDAS regulation, this element of security and at the same time liability has been considerably strengthened.

A first central element of the Regulation is the electronic signature along with its twin, the electronic seal, for legal entities. Here, the Regulation resorts to the Electronic Signatures Directive. However, we hope and expect that being based on the Directive, it will lead to a better harmonisation on EU level and thus to a wider range of use of electronic signatures, but first and foremost, that it will be widely acknowledged and recognised. The Regulation also clearly regulates the subject of the remote signature, which in the shape of the mobile signature ('Handy-Signatur') has been successfully used in Austria for quite some time. Even though there is little difference compared to the previous situation, this will be especially helpful in gaining international acceptance and acknowledgement.

The second main point of the Regulation refers to electronic identities. At least in the administrative field, the recognition of qualified identities is clearly regulated, a fact which will also greatly benefit the private sector. The most significant advantage compared to previous offers and characteristics is the possibility to assign responsibility for the quality and, thus, for the use of electronic identities beyond geographical borders. However, technologies used and offered nationally by either public or private service providers are only subject to regulation with regard to

quality, not to type. This fact accommodates the demands of the free market.

A third element of the Regulation deals with the so-called timestamp authorities. Especially combined with other elements, timestamps serve to enhance the quality of, for instance, a delivery.

The authentication of websites contributes significantly to a secure Internet environment and can be regarded as the counterpart of server identification. In order for this extremely valuable element to be able to take its effect, system- and especially browser manufacturers will have to implement the underlying technology actively and responsibly, in a way that is visible to the user. Only then will this technology serve to benefit us more than it currently can. However, this also hampers implementation since actually all browser manufacturers are non-European and have therefore so far refused to take this aspect into consideration with regard to implementation. This may also be due to the fact that a region which grants legal validity to such technologies would have an advantage over regions which do not. Thus it remains to be seen whether and to what extent this element of the Regulation will actually be implemented in practice. This could be compared to a situation where Europeans are legally required to wear a seatbelt while the manufacturers from another region would not offer cars with seatbelts. In the car industry, though, the monopoly is not as strong yet to render such a scenario realistic; however, it shows that in the case of general IT, Europe has become extremely dependent, especially where the sector of critical infrastructure is concerned.

The final aspect addressed by the Regulation is electronic delivery using send-and-receive services. Here, the structure differs significantly from the current situation in Austria. This means that it will take a considerable amount of time before national users will be able to make use of this part in actual applications.

The Internet of Things is at the root of fundamental change

Become an insider for only €2! Processor, storage, WIFI – regardless of whether you have a battery or power supply. Delivered from the Far East, free of charge to your door. Such low-threshold access is essential, especially for small and new enterprises. Currently, though, this means that anyone, regardless of their qualifications, is able to introduce critical software. Just think of energy supply, medical informatics (e.g. cardiac pacemakers) and many more. In practice, we are miles away from a formal examination of the quality of critical systems, although it would be technically possible in the case of a few thousand lines of code.

Way too often we substitute trustworthiness with trust, which is often blind. The dilemma here is the fact that the general certification of, for instance, a mobile phone will inevitably lead to technically outdated devices and applications, since with the change from large mainframes to mobile gadgets, innovation concerns less and less big companies and professional systems but, increasingly, applications in the consumer sector. Indeed, it would be a grave mistake to underestimate the innovative force of Google, Facebook etc., and particularly their economic power and strong urge to push innovation. The problem is, however, that in practice this often leads to an innovation monopoly. Europe's economic structure, and that of its member states, will only be able to cope with this situation, if at all, by promoting open innovation that arises from scientific research and its advancement. Establishing a sustainable kind of competitiveness takes some time and, as we have also seen in Europe, is often politically unattractive. Transferring scientific innovation to the industrial sector too early and too strongly especially constrains small and new commercial fields through a gradual loss of any right to the respective know-how, and thus through the lack of possibility to continue research.

Austria is the innovative 'birthplace' of 85% of all IoT/NFC technologies used worldwide. This is a very promising start, which, however, is not

adequately reflected in the innovation for the final products using these technologies. In fact, the competition on and the demand of the market is huge and has thus led to the rather unsatisfactory security situation described earlier.

The aspects of IoT and Artificial Intelligence (AI) are increasingly combined, which has given rise to enormous technical potentials. Assisted driving is but one of them, which has, however, already become a household name for the majority. Unfortunately, the public memory (and, alas, too often that of the decision-makers) tends to retain only the hypes and incidents, such as the hacking of a Jeep. This is probably due to the fact that many regard an understanding for technology as necessity rather than as part of culture and education since, historically, we are more steeped in the humanities. Here, the security factor is sorely neglected, as is the fact that with the increasing use of AI, decisions are made elsewhere. Sometimes, this applies to decisions humankind is incapable of making, due to its limited capabilities, or to decisions it should not take in the first place.

If we look at self-driving cars, for instance, we will find that an AI system realises in an instant that damage or injury are inevitable. If a playing child suddenly jumps onto the street from behind a tree, a human driver will, after the initial moment of shock, randomly decide whether to hit the aged person on the pavement or the child. An AI system, on the other hand, makes active decisions in such situations — and somebody programs them to do just that. Possibly, such situations reach far beyond the scope of product liability or disclaimers.

In the case of the systems mentioned, the classic terms of hard- and software are becoming blurred. What remains are inadequately defined aspects of security, a fact which is intensified by the lack of formal verification combined with short lifespans. Let me give you another example from the field of Assisted Driving and AI. Police officers could make use of any vulnerability of a hardware / software system, maybe even

of knowledge only available to the manufacturer, to minimise their risk when chasing a speeding offender and to bring the latter's vehicle to a halt or at least to make it slow down. This could be done by having the autonomous sensor of the tyre pressure report a significant pressure drop and put the vehicle into a conservative mode. Of course we can expect many such 'weak points', which gives rise to the commercial and, in such cases, also the political issue of weighing up interests.

Looking at the numerous apps installed on most mobile phones these days — regardless of the respective sector or manufacturer —, one will find that the number of potentially vulnerable points or points that pass on data without the user's knowledge is huge. The pressure to swiftly implement such innovations seems to make this inevitable.

Sufficient encryption without any loopholes or weak points that could be hacked is but one consideration in this respect. We are in need of far more robust communication able to master a vast variety of situations. Let me give you a few examples to illustrate my point.

Localisation services have been discussed at length and are familiar to most. A device that communicates where it 'goes to sleep', where it is during working hours etc. will identify its owner without any previous knowledge being required. But what happens if this device suddenly changes its 'behaviour'? Who is to receive this information — Google? The respective app? The authorities...? Should your bank keep a closer eye on your account in case of atypical behaviour? We can safely assume that such information will simply be used — no questions asked.

By controlling certain devices in their home via app, where the home router is required to allow a certain port, the individual unwittingly becomes a 'server operator' and is thus usually unable to cope with this chance with regard to applying IT security. Would it be better to pass the data on to a third party, i.e. the manufacturer of the device, in such case? What would

happen if the latter terminated the service contract, and you could not open your garage door any longer?

A person's communicative behaviour per se already gives away a lot of information. Somebody with the intention to burgle your house could thus 'lose' an inconspicuous battery-driven two-Euro device which is camouflaged as a windfall. This device then informs them when exactly you are at home or on holiday, thus 'helping' the burglars do their work.

This calls for communication structures that are robust enough to withstand most types of attack, which in turn calls for professionalism.

Chances for critical infrastructure

The change in technology also brings with it a plethora of chances. Let me just give you an example.

Take an incident inside a tunnel, for instance, in a remote valley or the like. Now let us assume that this incident has shut down any means of communication, including mobile communication. In today's infrastructure, calling for help would thus become extremely difficult, if not downright impossible. Mobile phones in their 'power save mode' could 'survive' for a considerable length of time, though.

In cooperation with other universities, scientists at the University of Luxembourg are currently developing such emergency protocols. By applying AI methods and irrespectively of any provider the latter try to 'leap' from one device to another, thus transmitting at least very short messages, in this case, calls for help. Once the path or the possible paths — the batteries can be assumed to fail at some stage — have been learnt, Voice over Data communications would also be thinkable. All this must operate irrespectively of the Internet, since the infrastructure is not available.

Proactive security using the example of Jurisdiction Awareness

Europe has very strict anti-spam laws. Still, they are not effective, which means that in practice we have more spam in Europe than in the US, for instance.

Looking at harmful communication, we will find in many cases that it travels along winding paths and passes through legal space that is very unlikely to provide legal assistance or support.

If tomorrow — which is not altogether unrealistic — a provider from a remote region offers switchboard services to a provider in Europe at half the usual price, the temptation for the latter to make use of these services definitely exists, as most have an eye to their own competitiveness.

Any prohibitions or restrictions in the field of communication, but also in IT security, are usually unrealistic or ineffective, due to the dynamics involved. If a solution is required in certain fields of qualified communication (banks, e-commerce, medicine, critical infrastructure, also e-mailing...), this will rather have to be provided on a voluntary basis, possibly by offering certain features, and the progressive change in communication and IT will be quite challenging.

Past experience has taught us that solutions that merely consist in surveillance or restriction are difficult to sell to the end user, and that they are inefficient in view of the increasing liberalisation beyond the scope of the EU. Moreover, criminals intending to commit felonies will always find a way, which makes this race of technologies difficult to win.

It seems feasible for providers to offer a certain quality, which commits them to keeping to the conditions defined therein — and the possibility to verify whether they are actually being kept to.

Jurisdiction-Aware Communication, i.e. communication offers that enable the user or their application and programme sphere to know in which way (to which country or jurisdiction) the communication flow is directed, could be made a mandatory part of the offer made by a provider or even implemented as a dial-up requirement ('country/jurisdiction badge'). If it is restricted to 'own jurisdiction', 'EU', and 'unknown', two Bits would be sufficient.

The effect could be useful. For instance, in the case of 'unknown', banks could demand additional securities for transactions exceeding a specified amount. The same holds true for other areas.

It would also be potentially applicable to a comprehensive implementation of the eIDAS Regulation and the consequent use of qualified server certificates, in the course of which, however, the aspect of private communication and the Internet of Things will raise a host of new questions.

Summary

Owing to the drastic changes in services and technologies, IT security must be subjected to some serious rethinking and become considerably more proactive in order to be able to cope with the extremely dynamic situation. The current approach, which lays great store by communicating, reporting and rapidly handling incidents, makes sound sense. The Internet of Things, especially when combined with Artificial Intelligence, will pose an enormous challenge to us, also with regard to AI-supported 'malicious software'. Formal verification can make significant contributions in some areas. What we need most, however, is the transparency of all aspects of quality, which includes the legal spheres or jurisdictions involved.

5 Implications in the Field of Nano Materials Technology

Session on Nanotechnology

René Fries

More than ten years ago, in 2004, the report of the British Royal Society and Royal Academy of Engineers on 'Nanoscience and Nanotechnologies - Opportunities and Uncertainties', pointed out that significant advances and advantages in defence capability are expected from the application of nanotechnologies:

"[T]he main initial defence impact is predicted to be in information systems using large numbers of new and cheap sensors, as well as in information processing and communications. These developments might enable pervasive nanosensors to contribute to national defence capability through early detection of chemical or biological releases, and increased surveillance capability. In addition, 'a whole range of military equipment including clothing, armour, weapons, personal communications will, thanks to low cost but powerful sensing and processing, be able to optimise their characteristics, operation and performance to meet changing conditions automatically'."[147]

On the other hand, it has been mentioned that developments in nanotechnology could entail specific dangers. A contribution by Jürgen Altmann in March 2004 in 'Security Dialogue' dealt with military use of nanotechnologies. The consequences for arms control and the stability that may arise from new military technologies are discussed:

---

147 Royal Society and Royal Academy of Engineers. 2004. Nanoscience and nanotechnologies - opportunities and uncertainties. In: http://www.raeng.org.uk/publications/reports/nanoscience-and-nanotechnologies-opportunities, accessed on 04 September 2016, 55.

"[T]he potential of mistrust is expected to be particularly high in areas where revolutionary changes are foreseen and the speed of those changes can change rapidly. Thus, transparency about national nanotechnology initiatives is of immense value and can significantly contribute to building confidence. [...]

Nanotechnology R&D should be extensively published, in both the civilian and the military realms. In particular, states that are traditionally less open about their military R&D should increase their transparency to avoid creating unnecessary mistrust. The nanotechnology initiatives of various nations should work together to build confidence and to address concerns such as arms control and safety protocols [...]." [148]

Therefore, it is very valuable that experts contributed to this book to share their profound state of the art knowledge of military nanotechnology and of future developments in this area.

Earlier this year, the *New York Times*[149] highlighted the dangers resulting from the development of a new generation of smaller weapons systems and quoted President Obama's remarks at the 'Nuclear Security Summit' in Washington D.C. concerning the fear that warhead miniaturization and the development of more effective weapon systems could lead to a new escalation of the arms race. The revolutionary changes brought about by nanotech and other 'disruptive technologies' (such as the enrichment of isotopes by pulsed laser) result in new dangers and a growing mistrust. It is of utmost importance that transparency and international cooperation in the field of military applications of nanotechnology will be improved.

---

[148] Altmann, Jürgen. 2004. Military Uses of Nanotechnology: Perspectives and Concern. In: Security Dialogue, Vol. 35 (1): 61-79.

[149] Broad, William J. & David E. Sanger. 2016. Race for Latest Class of Nuclear Arms Threatens to Revive Cold War. In: The New York Times, 16 April 2016.

Nanomaterials Technology: Convergence between Nanotechnology and Materials Science and Engineering

Michael Fredholm

This chapter will describe the implications for security forces of the convergence between nanotechnology and materials science and engineering. It will aim to investigate what can be expected in the medium term, until 2025, by examining U.S. and Russian efforts in nanomaterials, with a focus on security forces applications. It will also suggest a few scenarios in which nanomaterials are likely to be misused against individuals or societies, states, and their security apparatuses. What are the challenges? What should we expect in this field in the medium term, that is, by 2025?

This chapter will not cover the convergence of nano/bio/info technology or robotic/cognition/info technology, since these will be described elsewhere in this volume.

How will we predict the implications of future technology? We need to distinguish between Early Warning, Situational Awareness, and Forecasting. Which is our focus? Forecasting may be impossible, so Early Warning and, whenever possible, Situational Awareness with regard to new technology and its implications may be better options. Most studies extrapolate from the past, but this may not be enough.

The current trend in technology threat forecasting is to use tweets (and, for some, RSS feeds). However, tweet logs lag behind social media and real events but they do mirror them (RSS feeds also suffer from time lag). There is a more serious time lag as well, since open-source information appears later than real events. There are also time gaps, due to a limited availability of data. Algorithms can be used to address these problems,

although the enthusiasm with regard to potential success seems bigger than the actual results.

The trend in horizon scanning for emerging technology is to scan open source scientific literature. Early indicators are likely to appear in open source specialised literature. Key discoveries are relevant for various scientific disciplines, therefore key scientific technical journals should be added to watch lists for emerging technologies. Analysis of publications, conference proceedings, and tweets can be also used to keep track of developments in science and technology.

However, this methodology will not work well for military technologies, since not all achievements are published. Automated data mining can reduce human 'blind spots' but will produce many false positives/false negatives. Data mining can find 'nearest neighbours' to known technologies, but no actual black swans. Besides, the current data mining trend is to rely on Google search for patents, which is insufficient since potentially adversarial countries do not publish their scientific results in this way.

For this reason, a qualitative rather than quantitative study is necessary. Furthermore, the study must be based in a broad understanding of not only the subject area but also of the wider societal and technological trends. For this reason, the present chapter will begin with an outline of the background of current and projected military and security applications of nanomaterials, then go on to focus especially on U.S. and Russian efforts, since these will illustrate the difficulties of solely relying on open-source specialised literature. Finally, a number of misuse scenarios will be described, again with an emphasis on those for which open-source information may be insufficient for forecasting.

Origins

The concepts that inspired nanotechnology were first discussed by physicist Richard P. Feynman in his lecture 1959 with the title "There's Plenty of Room at the Bottom", in which he described the possibility of synthesis via direct manipulation of atoms.[150] The term 'nanotechnology' was first used by Norio Taniguchi in a conference paper in 1974.[151] However, K. Eric Drexler made the term 'nanotechnology', which he used in his 1986 book *Engines of Creation: The Coming Era of Nanotechnology,* popular.[152] As a result of these works, nanotechnology emerged as a scientific field in the 1980s. Commercialisation of products based on advances in nanoscale technologies finally began in the 2000s.

Although nanotechnology is an emerging technology, defined as a technology which is not necessarily new but not widely used, it is likely to result in significantly more advanced science-based innovations in the near future. Moreover, it has the potential to create a new industry or transform an existing one, having already moved beyond the purely conceptual stage. In short, the defining characteristics of an emerging technology are neither commonplace science-based innovations or industrial usage nor concrete, as opposed to theoretic, application. Other characteristics of emerging technologies, as identified by Mohanad Halaweh, are uncertainty, network

---

150 Feynman, Richard P. 1959. Plenty of Room at the Bottom. Transcript. Pasadena: American Physical Society.

151 Taniguchi, Norio.1974. On the Basic Concept of 'Nano-Technology'. In: Proceedings of the International Conference on Production Engineering. Part II. Tokyo: Japan Society of Precision Engineering.

152 Drexler, K. Eric. 1986. Engines of Creation. The Coming Era of Nanotechnology. New York: Anchor Books.

effect, unseen social and ethical concerns, cost, limitation to particular countries, and a lack of investigation and research.[153]

The sub-field of nanomaterials technology is a converging technology. The term, which was introduced by Mihail C. Roco and William Sims Bainbridge, refers to the "synergistic combination of four major 'NBIC' (nano-bio-info-cogno) provinces of science and technology," that is, (a) nanoscience and nanotechnology; (b) biotechnology and biomedicine, including genetic engineering; (c) information technology, including advanced computing and communications; and (d) cognitive science, including cognitive neuroscience.[154] Nanomaterials are the result of the convergence between nanotechnology and materials science and engineering.

Materials science, also commonly known as materials science and engineering, is an interdisciplinary field which involves the discovery and design of new materials, with an emphasis on solids.[155] Intellectually, the origin of materials science was the Age of Enlightenment, when researchers began to use analytical thinking from chemistry, physics, and engineering to understand ancient, phenomenological observations in metallurgy and mineralogy. Materials science thus incorporates elements of chemistry, physics, and engineering.

Nanotechnology is the manipulation of matter resulting in the engineering of functional systems at the atomic, molecular, and supramolecular scale

---

[153] Halaweh, Mohanad. 2013. Emerging Technology: What is it? In: Journal of Technology Management & Innovation 8(3):108-115.

[154] Roco, Mihail C. & Bainbridge, William Sims 2002. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation.1-2.

[155] Science Journal of Chemistry, Research Topic #2, Materials chemistry; http://www.journalchemistry.org/index accessed on 04 December 2017.

and implies a projected ability to construct items from the bottom. Nanotechnology is not a single technological field but encompasses all types of research and technologies that deal with the special properties of matter below at a certain scale, which is usually interpreted between 1 and 100 nanometres.

Nanomaterials research takes a materials science-based approach to nanotechnology, in effect being a convergence between traditional materials science and the emerging potential of nanotechnology. In this way it is possible to create many new materials – nanomaterials – and devices with a vast range of applications, for example in medicine, electronics, biomaterials energy production, and consumer products. Materials whose structure can be found at the nanoscale often have unique optical, electronic, or mechanical properties. Many lend themselves to dual use application, for example, in construction materials, consumer products, and military/security equipment. At the same time, there is a significant potential for the abuse of consumer products that include nanomaterials.

The field of nanomaterials is, like the traditional field of chemistry, loosely grouped into organic (carbon-based) nanomaterials, such as fullerenes, and inorganic nanomaterials, based on other elements, such as silicon. Examples of nanomaterials include fullerenes, carbon nanotubes, nanocrystals etc.[156] Nanomaterials have an impact on metals, alloys, fibres, ceramics, and composites.

Major benefits of nanotechnology include improved manufacturing methods, leading, for instance, to vehicles, energy systems, and detoxification systems with a better performance. Purification and

[156] Everipedia.org, Materials science, https://everipedia.org/wiki/Materials_science/, accessed on 11 December 2017.

environmental clean-up applications include the desalination of water, water filtration, waste-, and groundwater treatment. Future benefits may include better food production methods, nutrition, physical enhancement, nanomedicine, and eventually large-scale automated fabrication infrastructure. Due to the scale on which it operates, nanotechnology may allow for the automation of tasks that were previously impossible due to physical restrictions.

Our focus here will be on applications in technology and the security forces. In modern history, military needs have often pushed technology, particularly in situations when countries are faced with existential threats as, for example, during World Wars I and II as well as the Cold War. However, it will be shown that this is not necessarily the case with nanomaterials, since nanomaterials technology really only emerged in the early 21st century, when no existential military threat remained. Then, the focus was on low-intensity conflicts and counterterrorism in remote countries. This situation is unlikely to change in the short term.

Moreover, the implementation of nanotechnology will necessarily include an economic parameter, which is difficult to forecast. Will the gains produced be regarded as motivated by the higher costs? Furthermore, the organisational culture must be receptive to the adoption of new technology, even if it disrupts existing traditions and doctrine.

Perhaps, for this reason, results have so far been incremental. It will be shown that existing nanomaterials technology provides gradual, not revolutionary advantages. Underlying the age of nanotechnology from the beginning was the belief in the revolution in military affairs (RMA) hypothesis, which claimed that new technology would enable radically new military hardware and operational concepts, making high technology the key arbiter on the battlefield of the future. Information processing, communications, robotics, and other advances in technology would lead to major advances in military affairs. Sensors would develop until the

battlefield essentially became transparent, and the fog of war would become a problem of the past. Vehicles of all kinds would become lighter, faster, and stealthier. Finally, new types of weapons would emerge, among them advanced biological agents and directed energy beams. However, sceptics such as Michael O'Hanlon argued that although advances in information processing and communications were real, the other projected developments were at least overstated by their proponents, and the RMA hypothesis was unconvincing, at least in the near future. Environments such as forests and cities would remain significant obstacles to high-technology warfare. Most trends in military technology were not as impressive as RMA proponents argued. While new tools and weapons would change tactics, they would not change the basic nature of armed conflict. In 2000, O'Hanlon concluded that "even if a contemporary revolution in military affairs may eventually be possible, it does not appear within reach today."[157]

Almost two decades later, the RMA hypothesis still appears to be beyond our reach, despite the limited benefits for military hardware provided by developments in nanotechnology. As for the incremental advances provided by nanomaterials, most are indeed visible in consumer goods.

Current consumer applications

Several products that contain nanomaterials are already in use. Nanomaterials may be found in a variety of items, which people are not aware of since they cannot be seen with the naked eye. At present, simple nanoparticles are the most widely used nanomaterials, used in coatings, paints, sensors, chemical catalysts, and food packaging.

---

[157] O'Hanlon, Michael. 2000. Technological Change and the Future of Warfare. Washington, DC: Brookings Institution Press. 193.

Nanomaterials are already common in products, especially in the field of cosmetics, pharmaceuticals and consumer chemicals. For example, a sunscreen based on mineral nanoparticles such as titanium oxide offers several advantages, including higher radiation resistance than conventional sunscreen. Zinc oxide nanoparticles let light of some wavelengths through while blocking the rest, which makes them useful for certain sunscreen products. Silver nanoparticles with antimicrobial properties are added to laundry detergents. The use of engineered nanofibers in textiles enables wrinkle-resistant and water- and stain-repellent clothing, and such textiles need to be washed less frequently and at lower temperatures. Silver nanoparticles with antimicrobial properties are added to washing powder. They can also be woven into socks, where they kill bacteria. Nanotechnology also allows the introduction of full-surface protection from electrostatic charges by the integration of carbon particle membrane in fabrics. It may also be applied in food packaging. Clay nanoparticles improve barrier properties and are used in some plastic food packaging to increase shelf life, for instance in glass packaging for drinks. Perhaps most importantly at present, the use of nanomaterials enables lighter and stronger products. Clay nanoparticles are used to make lighter, stronger, and more elastic composites, and therefore are used in some car bumpers and composite bicycle frames. They also make cell phones lighter in weight and enable the production of harder synthetic bones. Even balls for various sports are made more durable. Recent generations of semiconductors can also be included in the field of nanotechnology.[158]

Nanotechnology thus already provides existing types of consumer products with incrementally better, but not revolutionary, functions. Nanomaterials can be used to produce more lightweight products. Surfaces and coatings

[158] Manyika, James et al. 2013. Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy. McKinsey Global Institute. 114, 118.

on ceramics and glasses become easier to clean or even self-cleaning, and more scratch-resistant.

Nanotechnology also has applications in heavy industry, particularly in construction. Lighter and stronger materials enable the construction of vehicles that are faster and safer. This is particularly useful for aircraft manufacturers, since it leads to significantly increased performance. Such materials also reduce the size of equipment thereby reducing fuel consumption. Existing types of combustion engines benefit from parts that are more heat-resistant and hard-wearing.

Projected consumer applications

The dilemma is that many types of nanomaterials are already available, but a high production price makes them uncompetitive. Graphene, which is composed of one-atom-thick sheets of graphite – carbon hexagons – is already being produced but the cost remains high compared to other materials and thus uncompetitive. Being one sixth the weight of steel per unit of volume and more than a hundred times as strong, it has huge potential. It can also be compressed without fracturing and has 35 per cent less electrical resistance than copper and ten times the conductivity of copper and aluminium, and thus would be an excellent choice for electrical circuits. Nanotubes (tubular graphene) are perhaps best known and show great potential, if production processes can be scaled up cost-effectively.[159]

Projected consumer applications include 'smart' materials, nanosensors, and miniature power generation.

Smart materials are any kind of material designed and engineered at the nanoscale for a specific task. This includes a wide variety of possible

[159] Ibid.118.

commercial applications. Clothes could become 'smart' through embedded wearable electronics. Fabrics and other materials could be designed to respond differently to various molecules. Artificial drugs could recognize and render inert specific viruses. Self-healing structures could naturally repair small tears in a surface in the same way as self-sealing tires or human skin.

A nanosensor would resemble a smart material in that it that would react to its environment and change in a fundamental, intentional way. A photo-sensor might passively measure incident light and discharge its absorbed energy as electricity when the light passes above or below a specified threshold, in effect sending a signal to another and larger machine. Such a sensor would likely cost less and use less power than a conventional sensor, yet function in the same applications.

Miniature power generation systems would generate the energy needed to power other miniature systems through the wearer's normal body movements. Improvements in battery and solar power technology and increased energy efficiency will also enhance the use of energy.

While nanomaterials can be expected to result in many improvements in existing products, nanomaterials are not generally believed to be a disruptive technology, that is, one which will have major implications for individuals and societies. Yet, this field will result in new products and services. It will result in changes in quality of life, health, and the environment, but it will likely not change patterns of consumption, the nature of work, or bring changes in the organisational structures of corporations or states.[160]

[160] Ibid. 20.

Current and projected military and security applications

Certain military products too have appeared with incrementally better, but no revolutionary, functions. However, comparatively few have entered service. Far more are projected. These can be grouped into communications and sensor applications, defensive applications, and offensive applications, in roughly this order of apparent importance. Applications for homeland security and policing would be a fourth category, even though it would overlap with the others in significant ways.

Communications and sensor applications

The use of nanomaterials will enable high-performance information technology with a performance improved by several orders of magnitude as compared to present technology. Small but powerful computers will be built into weapons, uniforms, and vehicles. Batteries and similar power sources will have an improved efficiency as compared to conventional technology, since nanoenergetic materials can store more energy than conventional energetic materials. The produced goods will be smaller, lighter, cheaper, and more efficient.

Nanomaterials allow the replacement of several present-time bulky and energy-intensive sensors with far smaller ones with far lower energy requirements. An example would be a cheap array of microsensors with the ability to detect chemical and biological warfare agents on a single chip or flexible, textile-embeddable, nanofiber-based sensors capable of being mounted on more solid garment or used in a pocket as a wearable sensor. Cheap miniature sensor systems could be scattered in high numbers, including miniature drones, some of which may be very small, perhaps centimetres, later millimetres, and even below. Low-cost miniature satellites can be built for low- orbit deployment, for the collection of data emitted by unattended ground sensors, such as GPS beacons, cameras, microphones,

vibration detectors, or other sensors. Such technology has already been announced by several U.S. firms.[161]

Communications between soldiers can be improved by the use of nanoparticles to create coated polymer threads woven into soldiers' uniforms, allowing protected communication between the soldiers. The system of threads in the uniforms could be set to different light wavelengths, eliminating the ability for anyone else to listen in.[162]

The use of nanomaterials will also enable further miniaturisation of the technology used for unmanned vehicles including combat vehicles – drones. Unmanned Aerial Vehicles (UAVs) will have greater range and endurance, due to the lighter payload and smaller size. Unmanned Underwater Vehicles (UUVs) will have better performance characteristics, due to the miniaturisation of navigation and guidance electronics.

Despite the advantages, a challenge for miniature UAVs will be survivability in an electronic warfare environment. Enemy jamming is likely to be an efficient countermeasure, since, due to its small size, a miniature UAV close to the enemy is unlikely to have sufficient inherent power to transmit through enemy jamming without losing its communications line. It must then be completely autonomous and, if designed as a sensor platform, able to return home or at least to report within communications range of a swarm of other miniature UAV sensor platforms.

Developments in nanomaterials will of course also benefit manned flight. The use of nanomaterials may eventually lead to integrated health-

[161] n.a. 2014. Nano-Satellites, the Future of Interception. Intelligence Online. Issue 726.
[162] Everyipedia.org, Industrial applications of nanotechnology, https://everipedia.org/wiki/Industrial_applications_of_nanotechnology/, accessed on 11 December 2017.

monitoring systems for airframe and engine, and advanced sensors that would allow fully integrated exterior-interior flow control and continuously deformable wings constructed of nanomaterials for better aerodynamic characteristics, manoeuvrability, and range.[163]

Finally, nanotechnology could be used for implants in soldiers' bodies in the form of neuron contacts, small computers, bio-compatible materials, and power supplies, which would be used for monitoring, communication, expanded senses, or drug release. However, this capacity would reach beyond that of nanomaterials and enter other fields of convergent technologies.

Even so, there seems to be a key threshold that needs to be overcome. This particularly concerns information technology and is indeed exemplified by software complexity. Moore's well-known law suggests a doubling of computer power every 18 months, and indeed computer power has hitherto increased exponentially. However, this doubling of computer power has not automatically led to a doubling of human capacity to write significantly more complex software. Jordan Pollack has observed that "faster and faster computers seem to encourage software companies to write less and less efficient code for the same essential functionality" which suggests that there are limits to the complexity of achievable design.[164] The human cognitive ability to remember, not to mention improve, millions of lines of code remains limited. When nanotechnology enables the self-

[163] Venneri, S. & Hirschbein, M. & Dastoor M. 2002. A Vision for the Aircraft of the 21st Century. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 313-317.
[164] Pollack, Jordan (Brandeis University). 2002. Breaking the Limits on Design Complexity. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 161-164.

replication and indeed self-improvement of design, that is, evolutionary design, a true breakthrough will take place. But this seems increasingly unlikely to happen in the medium term.

Defensive applications

The use of nanomaterials will reduce the volume and weight of the combat equipment carried in the field. This characteristic can in itself be regarded as a defensive application. But there are others, which may prove even more important.

For instance, uniform fabrics can include high-performance fibres in which special nanoparticles group together when something strikes the fabric, in order to stiffen the area of impact. This stiffness helps lessen the impact of blunt force. By reducing the force of the impact, the nanoparticles protect the soldier from injury. One such development is the so-called liquid armour, which consists of several layers, with a thick fluid between each layer. Upon impact, the fluid solidifies, thus absorbing the impact over a wider area.[165] Nanoparticles functioning as ballistic resistance also make the fabrics flame-retardant. This will shield soldiers from both kinetic energy and high temperatures. Moreover, the fabrics become more durable. The latter can also be made to shield soldiers from chemicals and biological warfare agents. Selectively permeable membranes could provide an outer layer for uniforms that would prevent aerosols and liquids from penetrating. Integrated decontamination activity and cooling or heat-resistant properties are feasible too.

---

[165] By an odd coincidence, this function corresponds to the protection provided by a legendary suit of living chain-mail armor in Georgia, worn by the hero Torgva. When hit by a sword, arrow, or bullet, all the loops of the chain-mail gathered and piled up in that very spot, protecting its wearer. (cf. Hunt, David. Legends of the Caucasus. London: Saqi.159.).

Surfaces of many different military items including uniforms and vehicles can be designed so electromagnetic radiation reduces the infrared signatures of the object's surface. This will improve stealth in the form of thermal camouflage, protecting soldiers from being seen with night vision devices and enabling better protection from infrared guided weapons or infrared surveillance sensors. Indeed, surfaces with locally variable colour – for example, through the use of phase-change materials, such as mobile pigment nanoparticles injected into the material – can be used for camouflage, enabling uniforms to change its colour according to the surroundings. By combining these methods dynamic multispectral camouflage can be created to protect against visual, infrared, and eventually radar observation.

Beyond the field of mere nanomaterials, converging technologies that include nano-scale applications can reach yet further.

Nanotechnology makes a biomedical, health-monitoring system worn by soldiers possible, able to watch over health and stress levels. Such systems would use sensors for vital signs, stress hormones, and physical activity, and could sense the state of health of the wearer. They would react by releasing drugs or, using smart materials, by compressing wounds until further medical treatment can be applied. This would reduce casualties, due to heat stress and dehydration, performance failure due to sleep deprivation (sleep time being determined by the lack of motion of the sensor), certain wounds, and combat stress. Detecting chemical and biological warfare agents, through the appropriate sensors would be also possible.

The system would also be able to release drugs into the soldiers' bodies, such as pain killers in case of injuries. The system would be able to inform the medics of the base of the soldiers' health status whenever they are wearing the system and are within communications range. The energy needed would be generated through the soldiers' normal body movements.

Yet another development could consist in improving human performance, including compensation for sleep deprivation and enhancement of survivability in case of physical injury.

Offensive applications

In nanomaterials, there is a higher focus on communications, sensor, and defensive applications than on offensive ones. However, better sensors and higher performance in weapons systems is a characteristic that in itself may be regarded as an offensive application. Besides, weapons can of course be improved as other forms of industrial applications. So far, most attention has been on explosives. Fast-release explosives, and incidentally slow-release propellants as well, must have high energy density while retaining stability, and nanoenergetic materials show greater power density than those in conventional explosives, thus can store more energy than conventional energetic materials.[166]

Nano-sized thermic materials could be used for new types of bombs several times more powerful than conventional explosives. A thermobaric weapon is a type of explosive that utilizes oxygen from the surrounding air to generate an intense, high-temperature explosion. The fuel-air bomb is one of the most well-known types of thermobaric weapons.

Nano-sized materials would also enable miniature munitions, including missiles that could be equipped with guidance systems, even though their explosive power may not reach that of conventional missiles.

---

[166] Lau, Clifford 2002. Nanotechnology and the Department of Defense. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 349-351.

For clandestine special operations, nanofiber composites could enable metal-free small arms and ammunition.

Unmanned Combat Aerial Vehicles (UCAVs), that is, armed drones, will have greater aerial combat capabilities, in part for the same reasons as UAVs (lighter payload and smaller size) but also because there is no pilot on board, there will be no g-force limitations and no need for life support, armour, or evacuation systems. Again, even more can conceivably be achieved through other converging technologies, including fully autonomous systems, known as Lethal Autonomous Weapons Systems (LAWS). If the latter remain unfeasible, it may be possible to modify or implant the desired systems in small animals such as rats or even insect.

Genetic engineering enables targeted chemical and biological warfare agents, including through nanotechnology. The development of biological agents that will not be detected or affected by known countermeasures can be expected. An inorganic nanomaterial would then be used to mask a biological material, for instance, the anthrax toxin could be bound to a nanoparticle that is used to transport the toxin across the cell membrane. Current vaccines would then not function. Second, nanotechnology could be used to disrupt the immune system, through either suppression or overstimulation, and prevent it from functioning. Certain nanoparticles can trigger an immune response, and delivery enabled by nanotechnology can again be used to overcome existing medical countermeasures.[167]

[167] Kosal, Margaret E. 2014. Anticipating the Biological Proliferation Threat of Nanotechnology: Challenges for International Arms Control Regimes. In: Nasu, Hitoshi &McLaughlin, Robert (eds.): New Technologies and the Law of Armed Conflict. The Hague: Asser Press.159-174.

Homeland security applications and policing

The terrorism threat that heralded the 21st century also brought home the potential for nanotechnology in homeland security, specifically sensors for chemical/biological/radiological /explosive detection. Sensor systems can be expected to be installed in all sorts of facilities, including but not limited to transportation nodes (airports, railway and subway stations, and others), border crossing points, government offices, public water supplies, chemical industries, and schools.[168]

Nano-materials also present significant opportunities for policing. Again there will be an emphasis on sensors, but this time used in police investigations. For law enforcement agencies, a key benefit of the improved sensory capacities of scientific instruments would be the ability and the speed with which forensic scientists will be able to examine crime scenes and traces left by criminals. Nanotechnology is expected to allow for faster DNA analysis and an improved examination of fingerprints and blood samples.[169]

Nano-materials may also play a major role in the use for the policing purposes of Big Data and, soon, the Internet of Things (IoT). Devices such as telephones and personal computers are already used by law enforcement to determine the whereabouts of individuals. With the increasing connectivity of a wide range of goods, such as clothes, jewellery, and footwear to the nearest wireless network, for commercial or entertainment purposes, it will become easier to pinpoint the whereabouts of a person at a

[168] Murday, James. 2002. NBIC For Homeland Defense: Chemical/Biological/Radiological/Explosive (CBRE) Detection/protection. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 341ff.

[169] Europol. 2015. Exploring Tomorrow's Organised Crime. The Hague. 22.

certain time and in fact investigate the movement patterns of a suspect. If such data becomes available – and privacy concerns will no doubt form obstacles to the imminent use of these methods – Big Data analytics will facilitate predictive policing.

The potential role of Big Data, or better, Big Data Analytics, in policing and other types of intelligence collection is not yet properly understood. Big Data represents information assets characterised by high Volume (quantity), Variety (type of content), Velocity (speed at which the data is generated), and Variability (inconsistency of the data and its accuracy). Big Data Analytics can be defined as the specific technology and analytical methods for its transformation into Value. This working definition of Big Data is derived from its various characteristics, which has been referred to as the four Vs:[170]

Volume: The amount of data in datasets is very large, requiring multiple petabytes of storage.

Variety: Data is generated and collected from a number of distinct sources and more than one dataset is integrated and analysed.

Velocity: Data is being added to, deleted from, and/or transferred into datasets at different speeds and times depending on the type of data and collection methods.

---

[170] AAAS-FBI-UNICRI. 2014. National and Transnational Security Implications of Big Data in the Life Sciences. Washington, DC: American Association for the Advancement of Science. 21. Cf. also Kosal, Margaret E.& Preston, Thomas. 18-21 February 2015. Contagion: The Peril and Promise of Big Data Analytics and Technological Advances in the Life Sciences for Biological Security. Paper prepared for International Studies Association Meeting. New Orleans. 5.

Variability: Datasets are incomplete, imperfect, and error-prone, and the data collected in these repositories is not standardised (also referred to as the veracity of data).

Big Data represents the information assets, while Big Data Analytics constitute the specific technology and analytical methods for the transformation of these assets into value, that is, intelligence products.[171] Such products will no doubt be increasingly common in a variety of situations in which intelligence is needed.

However, a major difficulty in implementing Big Data Analytics is the likely result of spurious correlations, that is, correlations without causal connection. Big Data Analytics will not reduce the need for experienced intelligence analysts in the loop.

A particular application of Big Data Analytics will no doubt be opinion mining, which could be used as a means to identify and prevent emerging riots and public unrest. If the data is made available to law enforcement, this would enable a potential revolution in policing and fighting serious and organized crime. Its adoption would allow law enforcement agents to prioritise their efforts and engage in truly intelligence-led policing. Big Data analytics would then reveal patterns in criminal activity and identify links between ostensibly unconnected events or criminal actors to an extent currently difficult or impossible, especially with regard to decentralised criminal networks and online networks.[172] It is indeed envisaged that accelerated developments in machine learning, algorithms, and sensors that track individuals, for instance through IoT, eventually will enable datasets,

---

[171] De Mauro, Andrea & Greco, Marco & Grimaldi, Michele. 2015. What is big data? A consensual definition and a review of key research topics. http://dx.doi.org/10.1063/1.4907823, accessed on 29 September 2017.

[172] Europol. 2015. Exploring Tomorrow's Organised Crime. The Hague. 43.

at first used for marketing purposes, that can be used to create profoundly powerful models capable of predicting human behaviour, including individual behaviour. If used for policing purposes, this would greatly increase capabilities for crime prevention.[173]

Case Study: U.S. efforts in nanomaterials

Nanotechnology in the United States

The U.S. Department of Defense has stated that it began to sponsor research in nanoscience already in the early 1980s, since that was the time when research in this field began. It soon identified nanoscience and nanotechnology as one of six strategically important research areas. Several federal agencies, including the Department of Defense, joined the Interagency Working Group on Nanotechnology to evaluate and support research, and defence funding was organised to focus on three areas of nanotechnology deemed to be of critical importance: nanomaterials by design, nanoelectronics/magnetics/optoelectronics, and nano-bio devices. From a defence viewpoint, the Department of Defense regarded the areas of nanoelectronics, chemistry, and materials as most important to enhance warfighting capabilities.[174]

In 2000, the U.S. National Nanotechnology Initiative (NII) was launched by President Bill Clinton as an interagency programme to coordinate federal nanoscale science, engineering, and technology research and development (R&D) activities and related efforts among participating

---

[173] Center for Long-Term Cybersecurity. 2016. Cybersecurity Futures 2020. Berkeley: University of California. 29-34.

[174] Lau, Clifford . 2002. Nanotechnology and the Department of Defense. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 349-351.

agencies.[175] From FY2001 through FY2014, Congress appropriated approximately $19.4 billion for nanotechnology R&D. President Barack Obama proposed $1.5 billion in NNI funding for FY2015.[176] The NII was formed as a broad-based programme in nanoscience. It was intended to couple that programme with information technology and biotechnology. As a result, the coordinating offices for both the NII and the U.S. Information Technology Initiative (ITI) were co-located in order to encourage collaboration. The NII aimed to support progress in key areas of research, yet the funding depended on congressional decisions and was generally regarded as insecure.[177]

In fact, in the United States, commercial actors are the principal ones in nanotechnology. As a result, most developments so far have taken place regarding civilian applications and consumer products. However, some have dual-use applications.

When the NII was launched, it was envisioned that in twenty to thirty years' time, nano-bio-info-cogno (NBIC) technology would mature. Several Department of Defense programmes were then envisioned to integrate biomedical status monitoring technology, among them the ambitious 1991 Land Warrior programme.[178] In addition, NBIC technology would enable

---

175 Interagency Working Group on Nanoscience, Engineering and Technology, National Nanotechnology Initiative. February 2000. Leading to the Next Industrial Revolution. Washington, D.C.: Committee on Technology, National Science and Technology Council.

176 Sargent, John F. Jr. 16 December 2014. The National Nanotechnology Initiative. Overview, Reauthorization, and Appropriations Issues. Congressional Research Service, Report RL34401. 1, 7.

177 Murday, James. 2002. NBIC For Homeland Defense: Chemical/Biological/Radiologi cal/Explosive (CBRE) Detection/protection. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 352-355.

178 Etter, Delores M. 2002. Cognitive Readiness: An Important Research Focus For National Security. In: Roco, Mihail C. & Bainbridge, William Sims. Converging

the replacement of fighter pilots, either by autonomous systems or with the pilot-in-the-loop.[179] And indeed, drone technology has already changed the nature of low-intensity air power. The use of nanomaterials is very likely to continue the trend of the miniaturisation of sensors, electronics, information processors, and computers. This will reduce the weight, size, and power of UAVs. Since removing the pilot from combat aircraft will not only reduce the risk of death or injury but also further reduce weight, since devices, such as oxygen system, ejection system, or personal armour, will become unnecessary. Furthermore, combat UAVs will become more manoeuvrable and capable of more extended missions as well, and tasks, such as take-off and landing, navigation, and target identification, will be done autonomously. An autonomous situation awareness capability may become possible too. Of course, surface warships, submarines, tanks, and other combat vehicles may experience similar development. However, despite advances so far, there is still a long way to go for all these developments to take place.

State-of-the-art technology

Although nanotechnology deals with very small structures, nanomaterials can and will perhaps most often be employed in the construction of large, and indeed very large, platforms. Already at the beginning of the 21st century, the U.S. military services were looking into the use of nanoparticles in high-performance platforms and weapons. The idea was to

---

Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 330-337.

[179] Lau, Clifford. 2002. Nano-Bio-Info-Cogno as Enabling Technology for Uninhabited Combat Vehicles. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 359-360.

embed small structures consisting of nanomaterials with special properties into larger structures, that is, warships, combat aircraft, and combat vehicles. Nanotechnology would thus enable combat equipment of greater stealth, higher strength, and lighter-weight structural materials. In addition to enabling higher performance, the use of nanomaterials would provide higher reliability and lower life-cycle cost.

The U.S. Department of Defense regards coatings, thin films, and advanced surfaces as particularly important aspects of systems, devices, and technologies critical to the services' warfighting mission.[180] Already in the early 2000s, the U.S. Navy was in the process of testing the use of nanostructured coatings in warships that were expected to dramatically reduce friction and wear. At the time, the U.S. Navy also was testing nanocomposites in which clay nanoparticles were embedded in polymer matrices for shipboard use, since such composites had been shown to have greater fire resistance.[181]

New coatings were also developed for the Air Force. By 2015, a plasma electrolytic oxidation (PEO) nanoceramic coating that provided an at least tenfold improvement of corrosion and wear resistance in missile launchers had been introduced following research by IBC Materials and Technologies Inc., who were under contract with the Air Force Research Laboratory's Materials and Manufacturing Directorate. The coating also resulted in a 27-percent improvement compared to current coatings concerning fatigue, and was announced to utilise green technology contrary to the current

---

[180] McQuade, Tyler. 2016. Local Control of Materials Synthesis (LoCo). Defense Advanced Research Projects Agency (DARPA). In: https://www.darpa.mil/, accessed on 29 March 2016.

[181] Lau, Clifford. 2002. Nanotechnology and the Department of Defense. In: Roco, Mihail C. & Bainbridge, William Sims. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 349-351.

coating scheme, which includes anodisation, a primer, and a solid film lubricant (anodising has been the standard protective coating for aluminium and other light alloys but uses chromic and sulfuric acid, which produces hazardous byproducts, such as sulfuric acid fumes and aluminium hydroxide). Using only water-based, low-concentration electrolytes, which produce a significantly harder, denser and lower-friction ceramic coating with high corrosion resistance, the PEO coating was not only environmentally better but allowed for higher performance. The PEO coatings were thus qualified for the LAU-12X Advanced Medium Range Air-to-Air Missile (AMRAAM) missile launchers on F-15, F-16, F-18 and other combat aircraft platforms.[182]

Already in 2011, Lockheed Martin announced that its F-35 fighter jets will use carbon nanotube composite plastics – nanocomposites – in some structural parts, beginning with wingtip fairings.[183] Since then, nanocomposites are being increasingly used. Silicon carbide particulate-reinforced aluminium is used for F-16 ventral fins and as fan exit guide vanes for large turbofan engines on the 777 commercial aircraft. In situ metal matrix composites are used for the compressor inner shroud of the F-22 fighter's engine. Advanced super alloy materials are used in the engine of the F-15 and F-16 aircraft. Precision, high-performance ceramic bearings are used in gyros for F-18, AV-8, F-16, several helicopters, and in the bearings for IR seekers for the Navy Missile Homing Improvement Programme. The use of armour plates made of nanomaterials is also increasingly common. Ceramic composite armour was used to protect

---

[182] Air Force Office of Scientific Research (AFOSR). 2015. Wright-Patterson Air Force Base. Press release of 20 April. In: www.wpafb.af.mil/news/story.asp?id=123445595, accessed on 29 March 2016.

[183] Trimble, Stephen. 2011. Lockheed Martin reveals F-35 to feature nanocomposite structures. In: Flight Global, 26 May (www.flightglobal.com/news/articles/lockheed-martin-reveals-f-35-to-feature-nanocomposite-357223/), accessed on 29 March 2016.

flight crews in C-141 transport aircraft in Bosnia against small arms fire and, on the ground, for light armoured vehicles.[184]

A new battle dress was expected to be launched in 2015. It is based on Second Skin (a responsive uniform made of new fabrics, with aerosol protection and self-detoxifying characteristics), but has been delayed and therefore will be postponed for several years. The project was started with high ambitions. In addition to Second Skin, the new battle dress was to have chemical and biological (CB) protection with reduced thermal burden, to be based on multifunctional materials for protection, and to have integrated protection characteristics with active cooling and physiological monitoring.[185]

Another key project underway is the Uniform Integrated Protection Ensemble (UIPE), which concerns CB protective garments. Its objective is the transition to new fabrics and garment designs. This will include improved aerosol protection, a reduction in the logistical burden, and the increase in the physical and cognitive performance of the war fighter in Mission Oriented Protective Posture (MOPP) gear, that is, protective gear used in toxic environments. The plan encompasses characteristics, such as liquid shedding fabric to reduce agent load, self-detoxifying materials to minimise risks from agent residuals, and high-performance selective permeable membranes and absorption layers.[186]

---

[184] Defense Advanced Research Projects Agency (DARPA). 2015. Materials Science: Advancing the Next Revolution of 'Stuff'. In: www.darpa.mil/news-events/2015-08-14, accessed on 29 March 2016.
[185] Cf. Presentation of Robert Botto, Chief, Physical Sciences and Technology, DTRA, at the 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.
[186] Ibid.

Yet another key project underway is Enhanced CB Survivability Coatings. Its objective is to develop an improved acceptance standard for chemical agent resistance, investigate new and more resistant, potentially reactive coatings, and develop a coating for aircraft with improved capabilities. The plan encompassed an update of the Chemical Agent Resistant Coating (CARC), a paint commonly applied to military vehicles to provide protection against chemical and biological agents, to a relevant acceptance standard for chemical resistance and the development of permanent or at least more durable coatings that also have reactive moieties to reduce residual risk.[187]

By 2015, there still remained doubts on when these projects would mature. Besides, ambitions remained high, possibly too high for easy implementation. Half serious, half in jest, a representative of the USAF concluded that, despite the high hopes for Second Skin, what the U.S. military really needed was the fictitious suit of the animated movie superhero, Mr. Incredible. That is, a bulletproof and flame-resistant protective suit that can be worn indefinitely under any climatic conditions.[188]

With such high ambitions, the possibility remains that research and development programme specifications and requirements are set unrealistically high. Scientists and the military have perhaps felt free to add too many improvements to the original needs. This is a well-known dilemma; one can always find new ways to improve the original plan, but as a result, the project is repeatedly delayed and takes years to mature. Besides, a personal observation is that, in the United States, cooperation between the Defense Threat Reduction Agency (DTRA) and the services, and

---

[187] Ibid.

[188] Cf. Presentation of Billy Mullins (USAF) at the 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.

between DTRA and the intelligence community, remains limited.[189] This is also a factor that keeps U.S. research and development from achieving its full potential in military and security applications based on nanomaterials.

In addition, scientists have observed that methods that enable atomic through millimetre-scale control over structure and properties of materials deposited on surfaces remain underdeveloped.[190] Furthermore and as a result, many of the expected improvements have not yet matured, despite a belief in the early 21st century that they would be in use by now (that is, within 10 to 20 years from 2001). For instance, in 2001 one such forecast assessed that, by now, national security would be "greatly strengthened by lightweight, information-rich war fighting systems, capable unmanned combat vehicles, adaptable smart materials, invulnerable data networks, superior intelligence-gathering systems, and effective measures against biological, chemical, radiological, and nuclear attacks."[191] While superior intelligence-gathering systems have emerged, in particular for counterterrorism, the rest still remains a forecast only.

Outlook for the year 2025: research and development potential and challenges for security forces

Although an early leader in nanotechnology, when it comes to practical applications, the United States – perhaps surprisingly – lags behind its own projections.

---

189 Roundtable on Threat Forecasting, Technology Watching, and Horizon Scanning. 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 13 May 2015.

190 McQuade, Tyler. 2016. Local Control of Materials Synthesis (LoCo). In: https://www.darpa.mil/ Defense Advanced Research Projects Agency (DARPA). accessed on 29 March 2016.

191 Roco, Mihail C. & Bainbridge, William Sims. 2002. Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Arlington, Virginia: National Science Foundation. 4-5.

For instance, the United States had expected to launch its new battle dress in 2015. Based on Second Skin (a responsive uniform made of new fabrics, with aerosol protection, self-detoxifying characteristics, and so on), and for this reason presumably far more advanced than the equivalent new Russian battle dress (see below), it has been delayed and will have to be postponed several years.[192]

The United States has fallen behind in capability because since 2001 or 2003, depending on whether Afghanistan or Iraq is taken as starting point, the security focus was on counterinsurgency in these two countries and elsewhere. Thus, there was no necessity for a plan to fight in a contaminated environment or against a high-technology opponent.[193]

Some in the United States now believe that Early Warning technology for contaminated environments will have matured by 2020. Self-contained and wearable and/or disposable diagnostic systems, with no need for calibration or maintenance, will then be available to all personnel. However, others do not agree and believe that the introduction of mature warning technology will be postponed several years beyond this date.[194]

Concluding, in the short term (until 2020), applications of nanotechnology for security forces will remain incremental. However, in the medium term (until 2025), it is possible that one or more ground-breaking developments will have taken place, in particular with regard to operations in contaminated environments. In addition, nanotechnology will lead to

[192] Presentation of Robert Botto, Chief, Physical Sciences and Technology, DTRA, at the 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.
[193] Special Panel: Science and Technology (S&T) Meets the Warfighter. 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.
[194] Presentation of Rich Schoske on Diagnostic Detection Diseases at the 2015 Chemical & Biological Defense Science and Technology Conference, St. Louis, Missouri 12 May 2015.

improvements in firepower, protection, mobility, sensors, and command and control. Even so, it seems unlikely that the emergence of completely new systems will have an impact on security forces before 2025).

Case Study: Russia's efforts in nanomaterials

Nanotechnology in Russia

It was late that Russia became a major actor in nanotechnology, and then because of top-down initiative. Russia's President Vladimir Putin and especially Prime Minister Dmitry Medvedev, known for his great interest in nanotechnology, singlehandedly began the process. On 24 April 2007, President Putin presented a strategy for the development of nanoindustry.[195] In his annual address to the Federal Assembly two days later, Putin singled out nanotechnology as the locomotive of Russia's scientific and technological development strategy.[196]

The Russian Corporation of Nanotechnologies (Rusnano) was established in July 2007 by federal law to improve Russia's science and industry in the field of nanotechnology.[197] Rusnano invests in nanotechnology inventions and also helps them become commercial enterprises. In 2008, President Putin stated that nanotechnology could lead to revolutionary changes in weapons systems.[198] While this was only one, and not a major, part of his

---

[195] Президентская инициатива – Стратегия развития наноиндустрии, № Пр-688, 24 April 2007.

[196] Putin, Vladimir. 2007. Послание Федеральному Собранию Российской Федерации. In: http://archive.kremlin.ru/appears/2007/04/26/1156_type63372type63374type82634_125339.shtml, accessed on 29 March 2016.

[197] Федеральный закон Российской Федерации от 19 июля 2007 г. N 139-ФЗ "О Российской корпорации нанотехнологий".

[198] Putin, Vladimir. 2008. Выступление на расширенном заседании Государственного совета «О стратегии развития России до 2020 года», 8 February. In: http://archive.kremlin.ru/text/appears/2008/02/159528.shtml, accessed on 29 March 2016.

speech, it shows that the military potential of nanotechnology had not been forgotten.

However, the 2008-2009 global financial crisis had a severe impact on the Russian state budget. Besides, the sanctions imposed against Russia in 2014 and the falling oil price made it difficult to acquire international funding for major projects.

State institutions have remained the principal actors in Russian nanotechnology.[199] The dominant subject area of Russian nanoscience is physics, followed by chemistry and materials.[200] This is hardly surprising, since fundamental research and applicable science were strongly supported in the Soviet period. Besides, the generation of nanoparticles and nanostructured materials has a long tradition in the country, which makes this field an important part of current Russian nanotechnology programmes.[201] The Soviet Union also witnessed rapid development in the field of biotechnology,[202] including that of military applications. However, following the end of the Cold War, Russia's then President Boris Yeltsin (1991-1999) privatised the national biotechnology industry, which almost resulted in a near-collapse of the support for research and development and in the emigration of many leading scientists.[203] Moreover, Russian

---

199 Westerlund, Fredrik. 2011. Russian Nanotechnology R&D: Thinking Big about Small Scale Science. Stockholm: FOI. 13.
Karaulova, Maria et. al. 2014. Nanotechnology Research and Innovation in Russia: A Bibliometric Analysis. Project on Emerging Technologies, Trajectories and Implications of Next Generation Innovation Systems Development in China and Russia. Manchester Institute of Innovation Research, University of Manchester: Working Paper 2014.
200 Ibid. 23.
201 Swiss Business Hub Russia: Russia Nanotechnology. OSEC Business Network Switzerland, Moscow 2011.
202 "'Biotechnology' means any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use." UN Convention on Biological Diversity, Art. 2 (1992).
203 Roffey, Roger. 2010. Biotechnology in Russia: Why Is It Not a Success Story?

investments in nanotechnologies remained below those of the United States even before sanctions were imposed.[204]

By 2011, examples of Rusnano projects included Connector Optics, which was expected be a base for high-speed fibre optics production in Russia, producing fibre with a capacity of 80 gigabytes per second; Sitronics-Nano, which would produce 90-nanometer chips which, although not a world record, was the norm for microchips used in most modern electronic devices; Pruzhina, which produced springs far superior to others currently produced in Russia and with a projected lifespan close to 30 years, first intended for use in railway carriages where present springs had a lifespan of a few years only; and Danaflex, which would produce food packaging film with a coating that reduced the amount of air and moisture that could penetrate through the film, helping to preserve the food longer.[205]

State-of-the-art technology

The influence of nanotechnology on Russian military technology has, so far, been incremental. Besides, there is some doubt whether all of the announced projects in fact make use of nanotechnology.

Already in 2007, only months after President Putin had presented the strategy for the development of nanoindustry, Russia introduced and demonstrated the 'father of all bombs', claimed to be the world's most

---

Stockholm: FOI. 7.

[204] Harper, Tim. 2011. Global Funding of Nanotechnologies & Its Impact. Cientifica (July). 3-4.

[205] Dulnev, Nikita. 2011. Rusnano's big nanotechnology secrets revealed. In: http://rbth.com/articles/2011/08/03/rusnanos_big_nanotechnology_secrets_revealed_13216.html, accessed on 29 March 2016.

powerful thermobaric bomb, with a reported power equivalent to 44 metric tons of TNT. It was claimed that nanotechnology was a key element.[206]

Yet there were without doubt real results. For instance, at the Oboronekspo-2014 defense technology exhibition, RT-Khimkompozit, owned by the state corporation Rostekh, announced a cockpit window coating made of nanomaterials that would improve visibility by reducing disturbing light reflections, thus enabling better vision for the pilot; moreover it would reduce UV radiation, and thus cockpit temperature.[207]

Another example, which was Ukrainian but which was noted by Russian media, was an armoured fighting vehicle of the type BTR-3E1, which in 2014 was advertised as having a coating of nanomaterials that protect it from corrosion.[208] Military technology research and development until recently followed the same trajectories in Russia and Ukraine, with many cooperative efforts.

The new Russian multifunctional battle dress Ratnik ('combatant') was expected to be the standard from 2015 onwards. The Ratnik system is reported to incorporate improved Russian military/tactical 6B43 model ceramic hard armour plates (to chest and back) and tactical armour plate carriers (tactical vests). The 6B43 model plates are reportedly a titanium/boron carbide ceramic composite. Ratnik was already used in the

---

206 Reuters. 2007. Самая мощная в мире вакуумная бомба: российские испытания. In: www.1tv.ru/news/techno/67699, accessed on 29 March 2016.

207 На ОБОРОНЭКСПО-2014: РТ-Химкомпозит" представит новые уникальные разработки. In: http://vpk.name/news/115381_na_oboronekspo2014_rthimkompozit_predstavit_novyie_unikalnyie_razrabotki.html, accessed on 29 March 2016.

208 Харьковские ученые разработали нанопокрытие, благодаря которому БТР не "съест" коррозия. 2014. In: http://vpk.name/news/118088_harkovskie_uchenyie_razrabotali_nanopokryitie_blagodarya_kotoromu_btr_ne_sest_korroziya.html, accessed on 29 March 2016.

2014 annexation of Crimea.[209] The exact details of Ratnik remain unknown, but fabrics and composite materials would seem to be in part based on nanotechnology. Ceramic armour plates, manufactured by using boron carbide powder, and already used in the United States, were announced in 2013 by NEVZ-Soyuz, based in Novosibirsk. The company claims that the effectiveness of protection is five to six times higher, and the weight four times less than that of existing armour. Production costs are reportedly lower as well. Indeed, the same type of ceramic armour plates might be used to ensure anti-bullet protection on combat transport helicopters without sufficient original armour protection and combat vehicles.[210]

NEVZ-Soyuz is also reportedly developing ceramic bullets that would cost a fraction of lead-based ones. Ceramic bullets would also be ten times stronger than steal.[211]

Russian scientists claim to have developed highly durable materials, including liquid armour, which is developed by, among others, OAO NII Stali in Zelenograd.[212] Further developments using nano-materials are regularly reported as well in specialist forums.[213]

---

[209] Crane, David. 2014. Russian Nano-Armor Coming in 2015 for Future Soldier 'Warrior Suit', and Russian Spetsnaz (Military Special Forces) Already Running Improved 6B43 Composite Hard Armor Plates, New Plate Carriers and Combat Helmets, AK Rifle/Carbines, GM-94 Grenade Launchers and other Tactical Gear in Crimea, Ukraine. In: www.defensereview.com/russian-nano-armor-coming-in-2015-and-russian-spetsnaz-military-special-forces-already-running-improved-6b43-composite-hard-armor-plates-new-plate-carriers-ak-riflecarbines-gm-94-grenade-launch/, accessed on 29 March 2016.

[210] RIA-Novosti. 13 August 2013. Defense Review. 23 April 2014. In: www.defensereview.com. NEVZ-Soyuz Website. www.ru.nevz.ru

[211] DefenseReview. 23 April 2014.

[212] Разработки XXI века: "жидкая" броня. 2013. In: https://wf.mail.ru/news/407640.html, accessed on 29 March 2016.

[213] See, e.g., Новости ВПК. In: http://vpk.name/news/nano/new_dev/, accessed on 29 March 2016.

Outlook for the year 2025: Research and development potential and challenges for security forces

Despite great hopes, when it comes to practical applications in nanomaterials, Russia has not yet caught up with its competitors, nor lived up to its own projections. Even so, there have been some developments. For instance, the new Russian multifunctional battledress Ratnik became standard from 2015 onwards. While a less ambitious project than its U.S. counterpart, it had entered service already by 2014.

State institutions have remained the principal actors in Russian nanotechnology. As a result, Russia has lagged behind because of an emphasis on state-funded nanotechnology research programmes and financial difficulties directly caused by the Russian state's economic and other policies.

Concluding, in the short term (until 2020), Russian applications of nanotechnology in the Russian security forces will remain incremental, as will American applications. However, in the medium term (until 2025), it is possible that one or more ground-breaking developments will have taken place, again, in particular with regard to operations in contaminated environments. In addition, nanotechnology will lead to improvements in firepower, protection, mobility, sensors, and command and control. Even so, it seems unlikely that the emergence of completely new systems will impact security forces before 2025).

Scenarios regarding the misuse of nanomaterials technology against individuals or societies, states, and their security apparatuses

Toxic nanomaterials accidentally released during armed conflicts

There is no provision in current nanomaterials technology for self-replication, so there is little opportunity for misuse that would actually entail disruptive consequences.

However, some nanomaterials are highly toxic. They could thus cause environmental damage, in particular during battlefield usage or after being decommissioned. Products that contain nanomaterials may accordingly require special end-of-life recycling procedures.[214] It has also been noted that nanomaterial coatings containing nanoparticles release a certain amount of the latter over time. However, the volume released depends on the type of nanoparticle. While, for example, only a very small amount of titanium dioxide nanoparticles would be released, as much as 30 per cent of silver nanoparticles may be lost, in comparison. The release follows from normal usage. For instance, nanoparticles in textiles are released through washing.[215] It follows that special cleaning and detoxification procedures will have to be conducted. However, it cannot be taken for granted that the armed forces of great powers would see this as an imperative in times of emergency.

Moreover, under the conditions of armed conflict, the imperative will always be on winning the conflict and saving the lives of friendly soldiers.

---

214 Manyika, James et. al. 2013. Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy. McKinsey Global Institute.122.

215 Part, Florian & Greßler, Sabine & Huber-Humer, Marion & Gazsó, André. 2015. Umweltrelevante Aspekte von Nanomaterialien am Ende der Nutzungsphase – Teil I: Abwässer und Klärschlamm. NanoTrust-Dossiers 43.1-6.

As a consequence, there will be less emphasis on recycling procedures, and toxic materials will be lost, abandoned, or dumped.

This is a 'known known' scenario and assessed as very likely.

Opportunistic use of nanomaterials by groups of organised crime

In the same way military and law enforcement benefit from applications which include nanomaterials, it must be expected that groups that are part of organised crime will also find ways to take advantage of them. As in all types of emerging technologies, the technology barrier will gradually be eroded, as deskilling takes place. Deskilling is the process by which skilled labour within an industry is eliminated by the introduction of technologies operated by semiskilled or unskilled workers. Within organised crime, deskilling can be said to take place when technology allows semiskilled members of the group to carry out work which formerly could only be handled by highly skilled personnel, such as laboratory technicians.

Currently a number of territories exist in which organised crime has access to advanced technology and communications networks as well as sufficient freedom of action to make full use of technological advances. Contested parts of the industrialised regions of Central Asia and the Caucasus come to mind, as well as the tri-border region of Argentina, Brazil and Paraguay, major parts of Pakistan, including urban areas with advanced research institutes, and Ukraine, a country which until recently shared a military nanotechnology base with Russia.

Organised crime will no doubt find numerous uses for nanomaterials. First, it can be expected that nanomaterials will be used to develop or alter drugs and psychoactive substances. Second, organised crime groups can be expected to take advantage of the developing market in nanotechnologies

to produce counterfeit versions of legal pharmaceuticals and devices.[216] While designer drugs are likely to remain a lucrative market, the trade in counterfeit drugs and devices may become the more important criminal activity, since the trade is lucrative while the risk of prosecution and imprisonment is significantly lower.

But the key advantage of nanotechnology for groups of organised crime, compared with that of conventional technology, would be the possibility of committing complex and sophisticated identity frauds at a scope yet unprecedented.[217] A key cause is the increasing exploitation of Big Data and personal data for criminal purposes. There are already groups of cybercriminals that provide complete stolen identities to interested buyers, usually for the purpose of various kinds of fraud. In the future, it can be expected that such a data packages will consist of yet more comprehensive information, including the complete biography, personal details, photographs, credit card information, as well as the biometrical data of an individual.[218] In view of the expected developments in machine learning, algorithms, and sensors tracking individuals, for instance through IoT, models capable of predicting human behaviour, including individual behaviour, will be developed. Organised crime will find ways of using data to manipulate individual behaviour, for fraud, blackmailing, kidnapping, or other hostile purposes.[219] Terrorists would attempt to break or hack into IoT systems that handle traffic control or other critical infrastructure, in order to carry out spectacular attacks killing large numbers of people.[220]

---

216 Europol. 2015. Exploring Tomorrow's Organised Crime. The Hague. 22.
217 Ibid. 19.
218 Ibid. 20.
219 Center for Long-Term Cybersecurity. 2016. Cybersecurity Futures 2020. Berkeley: University of California. 29-34, 71-79.
220 Ibid. 83-86.

Naturally, within the broader field of nanotechnology there are additional threats. The convergence between biotechnology and Big Data Analytics will present opportunities to terrorist groups and, perhaps more importantly, lone-actor terrorists, particularly in the form of disgruntled scientists.[221] There have already been cases of insider lone-actor terrorists who managed to shut down important government institutions, which highlight the potential of advanced materials for disrupting or halting government, military, or commercial activities.[222] New forms of high-end bioterrorism might come in many shapes, including antibiotic-resistant bacteria that would interfere with first line treatment. More advanced forms of bioterrorism might involve the introduction of immune system modifiers that block vaccine efficacy, targeted modifications of existing viruses, or even the reconstitution of formerly deadly viruses such as smallpox. By such means, the introduction of diseases such as anthrax and particularly influenza would be more plausible, more effective, and thus entail higher risk.

Finally, one should bear in mind that organised crime is opportunistic and often innovative. Some envisage a new dot-com bubble burst, with the advertising-driven business model for major Internet companies falling apart. This would result in a situation in which, as companies fail, employees at risk of losing employment would be increasingly tempted to steal valuable datasets, including those that pertain to privacy and financial services. It would not only be the datasets that would be of interest to organised crime; the dispossessed employees of the tech-industry would be

---

[221] Kosal, Margaret E.& Preston, Thomas: Contagion. 2015. The Peril and Promise of Big Data Analytics and Technological Advances in the Life Sciences for Biological Security. 2015. Paper prepared for the International Studies Association Meeting, 18-21 February 2015. New Orleans. 12-13.

[222] Fredholm, Michael. 2016. Understanding Lone Actor Terrorism: Past Experience, Future Outlook, and Response Strategies. New York: Routledge. 225-226.

of interest too, since they can be put to good use in criminal schemes.[223] For instance, it can be expected that increased dependence of the manufacturing and healthcare industries on robotics will create new vulnerabilities, which can be exploited by criminals, for instance via computer-based extortion. Even small, almost undetectable degradation along a product's supply chain may cause substantial damage to a company employing robotics. Since few individuals will have the requisite technical skills to enable such exploitation, this type of crime may be the result of a convergence between organised crime and terrorism, including lone actors with the necessary expertise and a grudge against a particular employer or society as a whole.[224]

When it comes to terrorism, any technology adopted for military use will eventually also be employed by terrorists. Terrorists have already begun experiments with unmanned drones, and the eventual use of nanomaterials, pilfered or otherwise derived from industries or security forces, will become part of their repertoire. What can be built, eventually will be built.

Off-the-shelf technology is not always so difficult to counter, and toxic effects are usually anticipated. However, security forces are often unprepared for the effects of new or improvised toxic materials. Existing sensors used to detect CB agents may not be correctly calibrated against new, improvised agents, since the properties of the latter have not yet been assessed.

This is a 'known unknown' scenario and assessed as very likely.

---

[223] Center for Long-Term Cybersecurity. 2016. Cybersecurity Futures 2020. Berkeley: University of California. 51-7, 65-66.
[224] Europol. 2015. Exploring Tomorrow's Organised Crime. The Hague. 21-22.

State programmes cut corners and accidentally release toxic nanomaterials

It cannot be assumed that state programmes for research into nanomaterials for military and security forces always will behave responsibly. In fact, large government administrations tend to handle their own operational security somewhat randomly, since they often consider themselves as not subject to petty regulation. Besides, national security is often believed to surpass operational and environmental security.

As a result, accidents happen, especially when corners are cut in the name of deadlines, budget restrictions, or the perception of urgency for national security. There tends to be no warning for this kind of incident. The accident or transgression may also be hushed up, so as not to reveal what went wrong.

This is an 'unknown unknown' scenario and assessed as likely.

The remaining enigma: Chinese nanotechnology

Not all developments within state-controlled military nanotechnology programmes are released to the public. There are always a certain number of 'black' or classified programmes. For this reason, tracking actual developments in U.S. and Russian military nanotechnology programmes is somewhat difficult. However, it is even harder, at least for researchers who lack Chinese language skills, to gain an insight into the applications of nanomaterials technology in China's armed forces. China is a major centre of nanotechnology research, and much of it is not made public in foreign languages. In 2011, China surpassed the United States as the largest funder of nanotechnology research in dollars. According to Tim Harper's estimates, in Purchasing Power Parity (PPP) terms China spends US$2.25 billion in nanotechnology research while the United States spends US$2.18

billion. However, Harper argued, in real dollar terms, adjusted for currency exchange rates, China was only spending about US$1.3 billion.[225]

Even so, Chinese investments are impressive, and it could be argued that China combines the funding policies of the United States and Russia. China makes substantial state investments, but its industry is simultaneously developing nanomaterials for the consumer market. This might bring benefits also for security applications. However, little seems to be published in Western languages on Chinese applications of nanomaterials technology in the security field.

This scenario is an 'unknown known' scenario and the potential for misuse is assessed as likely, since it involves state programmes.

Conclusions

Nanomaterials have brought incremental improvements in military technology and power projection and will lead to improvements in firepower, protection, mobility, sensors, and command and control. However, when it comes to the practical application of nanomaterials technology in the military field, both Russia and the United States lag behind their own projections.

State institutions remain the principal actors in Russian nanotechnology, while commercial actors are the principal ones in U.S. nanotechnology. As a result, most developments so far have taken place regarding civilian applications and consumer goods. However, some products involve dual-use application.

---

[225] Harper, Tim. 2011. Global Funding of Nanotechnologies & Its Impact. In: http://cientifica.com/wp-content/uploads/downloads/2011/07/Global-Nanotechnology-Funding-Report-2011.pdf 3-4.

Russia has been lagging behind because of financial difficulties and an emphasis on state-funded nanotechnology research. The United States has fallen behind in capability because since 2001, the security focus has been on counterinsurgency in Iraq and Afghanistan and there was no real contingency plan to fight in a contaminated environment or against a high-tech opponent.

Some in the United States now believe that Early Warning technology for contaminated environments will have matured by 2020. Self-contained and wearable and/or disposable diagnostic systems with no need for calibration or maintenance will then be available to all personnel. However, others do not agree and believe that the introduction of sophisticated warning technology will be postponed several years beyond this date.

Concluding, in the short term (until 2020), the application of nanomaterials technology in the security forces will have an incremental impact on capabilities. However, in the medium term (until 2025), it is possible that one or more ground breaking developments will take place. Besides, the increased use of nanomaterials will likely lead to further improvements in firepower, protection, mobility, sensors, and command and control. In particular, developments can be expected with regard to operations in contaminated environments. Even so, it seems unlikely that the emergence of completely new systems will have an impact on security forces before 2025. There are no indications that any truly significant changes, such as a revolution in military affairs (RMA), will take place until several years beyond this date. Michael O'Hanlon's cautious forecast in 2000 that a revolution in military affairs does not appear within reach today remains essentially confirmed.

In modern history, military needs have often pushed technology, in particular in situations when countries are faced with existential threats, such as during the two World Wars and the Cold War. Moreover, the adoption of new military technologies can never be taken for granted,

except in times of existential threat. First, the cost of the adoption of a new technology will have to be offset by cuts in another programme. Implementing nanotechnology will necessarily include an economic parameter, which is difficult to forecast. Will the gains produced be regarded as motivated by the higher costs? Second, the organisational culture must be receptive to the adoption of new technology, even if it disrupts existing traditions and doctrine.

Nanomaterials also present significant opportunities for policing. There will be an emphasis on sensors and forensics in police investigations, but nanomaterials may also play a major role in the use for policing purposes of Big Data and, in time, the IoT. Devices such as telephones and personal computers are already used by law enforcement to locate suspects, and the ability to do so will grow. Accelerated developments in machine learning, algorithms, and sensors that track individuals, for instance through IoT, will eventually enable datasets that will greatly increase capabilities in crime prevention.

When does converging technology in the form of nanomaterials applications represent a threat or a risk for individuals or the society of a small state, as well as for security forces in the defence of the state or first responders faced with hazardous threats? There are a number of potential scenarios for which Early Warning and Situational Awareness are mandatory and preparations needed. First, toxic nanomaterials are very likely to be released during armed conflicts. Second, groups of organised crime are very likely to make use of nanomaterials for a variety of criminal purposes whenever the opportunity arises. Third, state programmes are likely to transgress rules and accidentally release toxic nanomaterials. In addition to these threats, it should be borne in mind that little information on Chinese development efforts in nanomaterials in Western languages is currently available.

In particular, the threat from organised crime is often overlooked in the assessment of military and security technology. Currently, organised crime has access to advanced technology and communications networks as well as sufficient freedom of action to make full use of technological advances in a number of territories throughout the world, including contested parts of the industrialised regions of Central Asia and the Caucasus, the tri-border region of Argentina, Brazil and Paraguay, major parts of Pakistan, including urban areas with advanced research institutes, and the Ukraine, which until recently shared a military nanotechnology base with Russia. Organised crime is opportunistic and often innovative. There is also a threat from terrorism, including lone-actor terroristic acts carried out by insiders from nanotechnology research institutes. Any technology adopted for military use will in time also be employed by terrorists. What can be built, eventually will be built.

Converging Technologies and Emerging Risks – Future Challenges for the Security Sector

Joachim Klerx

The more challenging part of writing about future developments is that these developments are in the future and thus they will happen with a typically unknown probability. This is particularly true for technological innovation. In the year 2002, the U.S. National Science Foundation and Department of Commerce sponsored report 'Converging Technologies for Improving Human Performance'[226] sponsored by the U.S. National Science Foundation and Department of Commerce was a starting point for interdisciplinary research between major contributors of nanotechnology, biotechnology, information technology and cognitive science (NBIC) to improve the human performance. The potentially useful innovations and applications for human enhancement did draw attention from the military, the health sector and other public industrial settings. Fifteen years later, in 2017, the actual research results and the actual future expectations can be used to renew the future scenarios. In the report a workshop participant was cited with the following comment:

If the *Cognitive Scientists* can think it,

the *Nano* people can build it,

the *Bio* people can implement it, and

the *IT* people can monitor and control it.[227]

---

[226] Roco, Mihail C. & Bainbridge, William Sims (eds). 2003. Converging technologies for improving human performance: nanotechnology, biotechnology, information technology and cognitive science. Dordrecht/The Netherlands: Kluwer Academic Publishers. Cf. also http://www.wtec.org/ConvergingTechnologies/Report/NBIC_report.pdf, accessed on 17 December 2016.

[227] Ibid.13.

In 2017 it turned out to be ICT, which is the science in NBIC that builds up the knowledge management infrastructure and delivers facilitating tools for data management, analytics, simulation and some specific forms of 'reasoning'. In all other NBIC technological fields (nano-, bio-, and cognitive science), as well as in research subjects, like electronics, construction, chemistry and others, innovative solutions are developed, which relate to ICT supported solutions. However, it is not worthwhile thinking about the guiding role of a single science. It is much more productive to identify linkages and synergies, which is one purpose of this publication. Technological innovation is usually not straight forward and does often come with a huge amount of additional but invisible process innovations. Therefore, it is very difficult to foresee the technological innovations of the next years. But it is very clear, that there will be a lot of different innovations and the probability is high that innovation in one technological field will support innovations in other fields.

A very reliable method to decrease the uncertainty about future developments is to understand the timely interdependence of different future developments and to understand the interaction of weak signals for anticipating emerging threats to society, for disruptive events, technological needs, capability building with research and the interaction of potential technological solutions. In this publication, all content elements from horizon scanning activities of the last years are presented in a way that the interdependence with respect to time becomes obvious.

In Chapter 2 an overview of the discussion worldwide about future emerging threats is presented. Chapter 3 deals with emerging research fronts and technologies, which might be useful to tackle emerging threats.

Finally, in Chapter 4, resulting challenges for the security sector are discussed and a model is presented of how to generate strategic knowledge as a main asset for dealing with future conflicts and future technological innovation in order to address the threats properly.

Emerging threats as sources of future conflicts

Since ancient history, societies have always had to deal with unexpected, but principally well known threats, like floods, dry periods and other natural disasters. However, due to the industrial developments of the last century and, particularly, those of the last decade, there is an increasing amount of new and emerging threats, which are not well known or even unique, like the space waste threat, which - if ever - will only happen once. As societies are not prepared for some of the new and emerging threats, the latter may be a source of future conflicts, in particular, if more than one country is affected.

Typical publications on future emerging risks[228+229] focus on identified but unexpected risk. In fact, it is very difficult to identify new and emerging threats, since they typically have not even happened yet. In the EU project ETTIS[230], software was developed to identify new threats of the Internet. The following figure summarises the results from the TIA (threat identification agent), which was used in the alpha version. In more than 200.000 Internet sources, the software identified, besides other foresight content elements, the following threat categories.

---

228 National Intelligence Council. 2017. Global Trends. Paradox of Progress. In: www.dni.gov/nic/globaltrends, accessed on 17 January 2017.
229 World Economic Forum. 2016. The Global Risks Report 2016 (11th edition). Geneva.
230 ETTIS - European security trends and threats in society. 2016. In: http://cordis.europa.eu/result/rcn/177014_en.html, accessed on 17 January 2017.

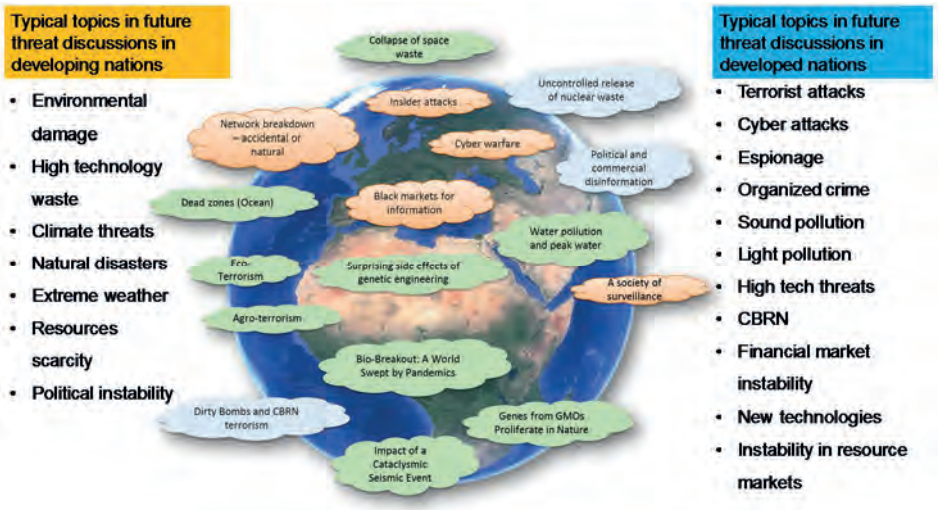


Figure 1: Emerging future threats in countries with different degrees of industrialisation[231]

The surprising result was that in different countries the discussions about future emerging risk were completely different and mainly focused on some typical local precursor for potential upcoming local threats, which might be relevant for the region or nearby regions. We found that there are typical differences in the discussion of future threats in developing and in developed nations.

Typical *developing nations* tend to have simple economic infrastructures based on low-tech solutions. They often do not have the capability or the money to deal with the consequences of climate change as a result of an increasing scarcity of resources. Thus, they fear extreme weather conditions, natural

[231] Klerx, Joachim. ETTIS Global Threat Database. Unpublished, funded 2012 under: FP7-SECURITY, Project ID: 28559, ETTIS - European security trends and threats in society, Vienna, DB Version 2016.

disasters, scarcity of resources, and other typical threats to the basic infrastructure, including political instability. In addition, they are threatened by disadvantages from global trade, like high-tech waste, as they do not have the proper knowledge or legal provisions to deal with toxic waste.

Developed nations usually have a better infrastructure, based on a knowledge-based high-tech infrastructure, which makes these nations more resilient to basic threats. However, they do fear threats to their high-tech infrastructure or threats that have consequences for their high living standard.

New types of large scale threats, such as climate change and space waste collisions are becoming increasingly interdependent and complex. These new challenges arise for the security sector, as there is a tendency to overlook spin-off impacts from the original threat that are not obvious yet. For example, one long-term consequence of climate change is a decrease in the number of different species, which causes less variance in human food and a loss of quality of life. Other threats are single events, like a space waste disaster, which might have the potential of destroying the satellite infrastructure for a very long time, entailing huge consequences. However, until a very short time before the disaster, the potential threat is not visible to the majority of people, which makes it difficult to invest in prevention.

New and emerging threats require research, technological innovation, process innovation, training and capability building to prepare for new threat events. Therefore, it is important both to gather knowledge about future threats and to research interdependences and ways of building up capabilities to address these threats. In the next chapter, emerging research fronts and technologies to address military threats are presented.

Emerging research fronts and technologies to address future threats

Typical content elements of technology foresights, like weak signals for new threats, trends, technological innovations and disruptive events can be

used to discuss the future challenges of emerging threats and emerging technologies for the security sector. The following chapter summarises weak signals from the ETTIS project, based on test results from an alpha version of the TIA software.

In the following subchapter, results for ICT and AI, biotechnologies and future materials are presented. To understand the figures it is important to notice the meaning of weak signals, trends, technological innovations and disruptive events.

Weak signals are small and often early signs of events pointing to future threats, opportunities, needs or wild cards. In particular, weak signals with a potential of being wild cards often point to future strategic discontinuity. Therefore, they have a high analytical value for strategic long-term planning.

Threats can be warnings that someone is going to hurt or punish someone else; they can be signs of something dangerous or unpleasant which may be, or is, about to happen, or they can indicate danger.

An opportunity is the positive version of a threat. It might either be a favorable or advantageous circumstance, occasion or time or a chance for progress or advancement. The advantage is usually related to a specific group. Thus, this group will consider the favorable event as opportunity.

Trend as a future-oriented concept is misleading. It is easy to discover a trend based on historical data on the stock exchange. However, it is nearly impossible to learn something about tomorrow's share prices in this way. A trend in general is a direction, derived from past data. It is usually based on a linear pattern, which only works in a specific context. Trends are usually described in terms of time horizon, impact and geographical coverage. Here, a trend is in a way the opposite of a wild card. Trends are expected events while wild cards are surprising events.

Wild Cards are high-impact events that seem too incredible to believe. Therefore, they tend to be overlooked in long-term strategic planning. Often it leads even to a decrease in reputation in the peer group, if a member of this peer group starts to discuss a wild card seriously. In futurology, 'wild cards' refer to low-probability, high-impact events, as introduced by John Petersen (1999)[232]. However, more important than probability is the fact that these topics are not well known and not part of mainstream discussion. Often these disruptive events are still too incomplete to permit an accurate estimation of their impact and to determine possible reactions. However, for strategic long-term planning and scenario development they are very important as they increase the possibility of scenario planning to adapt to surprises arising in turbulent chaotic environments. In trend analysis disruptive events point to trend breaks and tipping points.

In the following subchapter, the content elements of ICT and artificial intelligence (blue background), biotechnology and genetics (green background), and future materials (yellow background), as well as nanotechnology are presented. In each figure weak signals, trends, technological innovation and disruptive events are marked explicitly. It is very likely that some of these explicitly presented content elements point implicitly to other foresight content elements, like threats or opportunities.

If a specific content element is highlighted in another colour, this shows interdependence with the respective field of technology.

ICT and artificial intelligence

The following figure summarises the horizon-scanning results for ICT and artificial intelligence. In classical converging technologies, the artificial

[232] Peterson, John L. 1999. Out of the Blue – How to Anticipate Big Future Surprises. Madison Books.

intelligence is part of the cognitive science sector. However, for the sake of simplicity of horizon scanning, ICT and artificial intelligence are presented together.

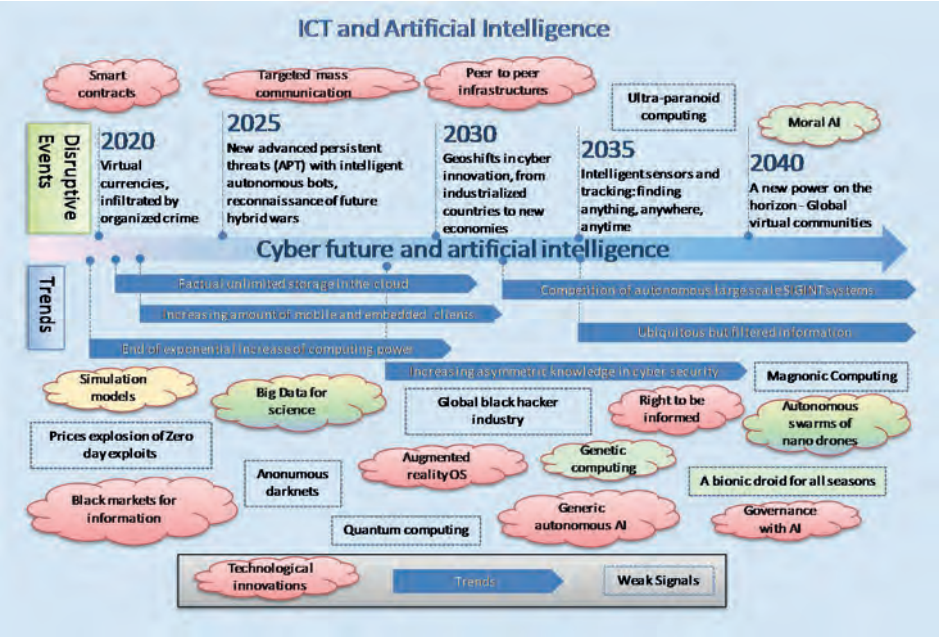


Figure 2: ICT - Emerging research fronts and technological innovation[233]

ICT and artificial intelligence is particularly difficult for horizon scanning and technology forecast. It is very likely that the timing is not precise and that some disruptive innovations are overseen, as typical in almost any past ICT technology forecast.

[233] Klerx, Joachim: "ETTIS Global Threat Database". Unpublished, funded 2012 under: FP7-SECURITY, Project ID: 28559, ETTIS - European security trends and threats in society, Vienna, DB Version 2016.

However, the main trends, the most important innovations and some disruptive technologies are presented.

It is very likely that the potential increase in calculation power of a single CPU will have reached its limit within the next years. Due to these physical limits of existing CPU technologies based on silicon it is obvious that the increasing density of transistors on a single chip will also reach its boundaries. Other technologies are not commercially available yet.

The new way of increasing calculation power is the use of large clouds in order to combine the calculation power of different CPUs. Based on this there is a huge amount of software, which needs to be redesigned and programmed in a new programming language. This process is ongoing.

In the near future, the graphical user interface of very small computers will become too complicated. New forms of user interfaces might work with language, gesture, mimics, and other verbal and non-verbal communication.

The visualisation of the user interface will be in 3D and combined with augmented reality, so that all information management services from computer are presented in the best possible way, irrespective of the hardware. As a consequent follow up from virtualization and parallelization, as well as, grid computing and cloud computing, it is very likely that at some point in the future computer, as today, will just be a virtual AI software bubble, following the person across different machines nearby. Even today it is possible to have a virtualized handy in the cloud, accessible from different devices. But the user has to orchestrate and administer this virtual computer. Starting with systems like Docker, the virtual container become smaller and smaller, integrated in a large ubiquitous cloud. Following this trend, with better administration will lead to these virtual computer bubbles.

Computers will offer an unlimited amount of calculation power to support data management, information management and knowledge management for all scientific fields, all military operations and for daily live. Military operations will be supported by ubiquitous computing without human interaction.

Biotechnologies and genetics

Over the last years, genetics and biotechnology have become very data-intensive sciences. A huge number of different databases have been created to understand the communication processes between DNA, RNA, proteins and other material of the human body with organising and communicative tasks.

The following figure presents the databases. They can be seen as a starting point of a long time research strategy, with the main purpose to understand the communication between DNA, RNA, proteins, hormones and biochemical substances in life. Understanding these processes is the first step to bioengineering, synthetic biology. This might be useful for increasing human capability in order to address future threats. In military conflicts this might involve bioweapons and biosensors for attack and response.

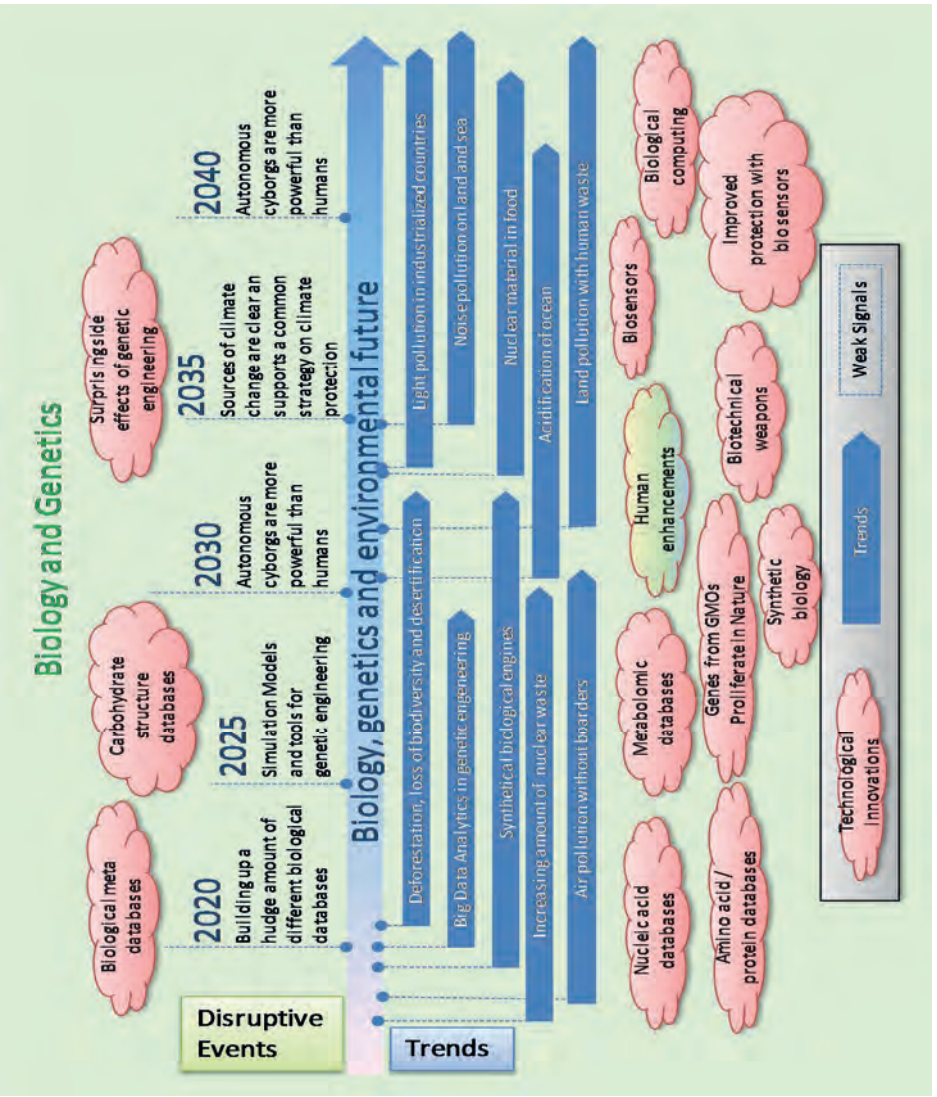


Figure 3: Biology - Emerging research fronts and technological innovation[234]

[234] Klerx, Joachim. ETTIS Global Threat Database. Unpublished, funded 2012 under:

The technological fields highlighted in specific colours are related to different focal points in this publication. Innovations relating to human enhancement might come from biotechnology, as well as material intelligence, ICT and artificial intelligence. In fact, it is very likely that the combination is much stronger than the solutions from a specific technology field.

In the centre of biological innovation, which might be useful for military applications, is human enhancement, better sensors, biocomputers and bioweapons. Advances in customised bioweapons are typically not communicated without classification. Thus, there might be a knowledge deficit.

However, it becomes clear, that human enhancement as well as almost all other technological innovations do benefit from synergies in 'new materials', computing and biological research.

Future materials and nanotechnology

A general goal in the research of materials is to find or develop 'better' materials (in relation to specific contexts this might mean, for example, strongest, hardest, most invisible for better camouflage etc.).

Methods in materials and nanotechnology are very similar to classical research. However, advances in research methods might have a huge impact on other research areas. The following figure summarises the horizon-scanning results for materials and nanotechnology.

FP7-SECURITY, Project ID: 28559, ETTIS - European security trends and threats in society, Vienna, DB Version 2016.

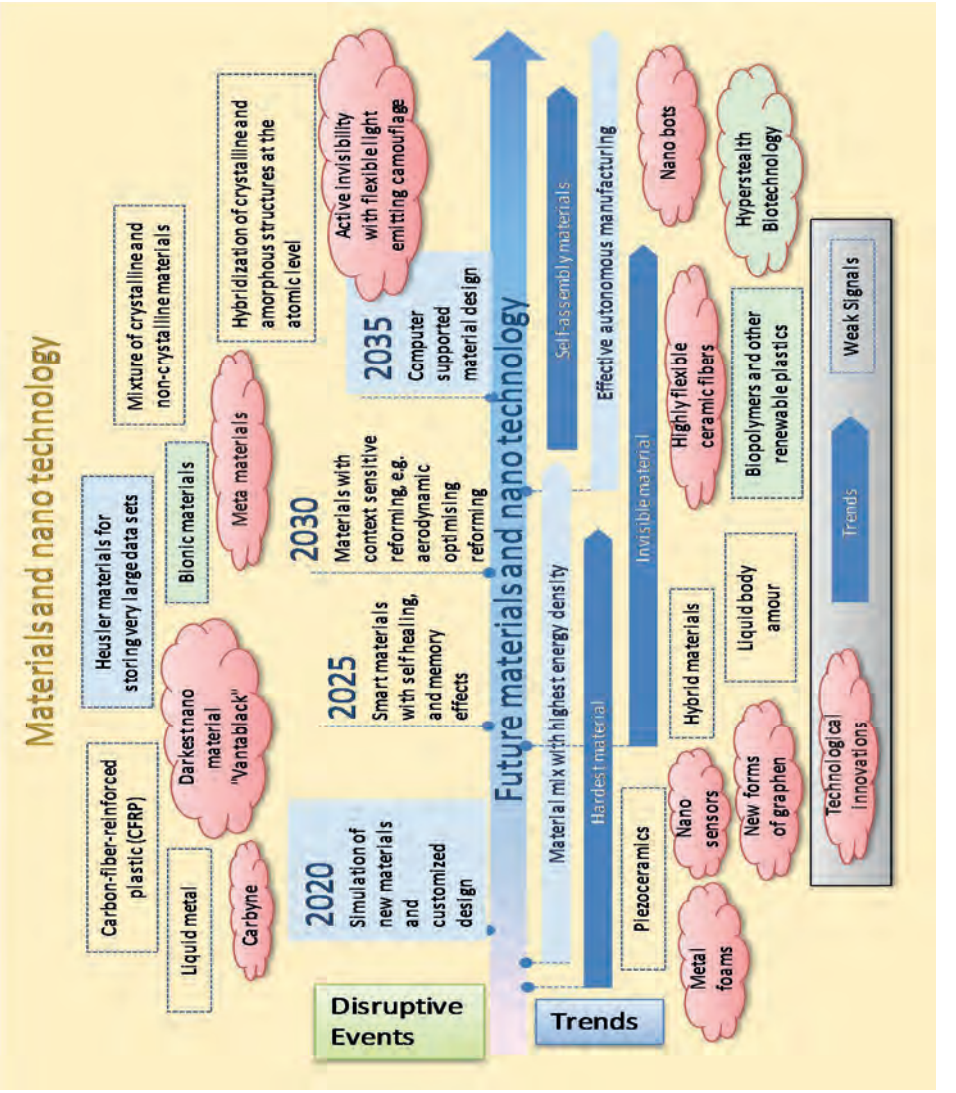


Figure 4: Materials - Emerging research fronts and technological innovation[235]

[235] Klerx, Joachim. ETTIS Global Threat Database. Unpublished, funded 2012 under:

According to the new materials needed in other technology fields, nanotechnology and other technologies in materials science produce new materials that are the hardest, most flexible, most invisible and blackest materials and and have many other desirable characteristics.

Very similar to biotechnology, computers are used to simulate new materials, collect data about specific materials and increasingly understand how to customise a specific material for a specific purpose. It seems that there is a need for specialised software and other computer capabilities that support the research in materials. However, given the methods used for technology forecast, it would be redundant to propose specific needs in any addressed research area.

Future challenges for the security sector

For the security sector, the increasing interdependence of complex new and emerging risks is a challenge in itself. New capabilities and new technologies can be a solution, but only in combination with training-, planning- and process innovation. New technologies are worthless unless they are available in a crisis situation or unless they are integrated in operational as well as training processes.

Military activities have always been and continue to be a dangerous business, involving a wide range of threats to the health and the performance of the personnel involved. Converging technologies offer a wide variety of possible innovations to protect soldiers, but, at the same time, they involve new risks. Innovations in autonomous systems with ballistics weapons, in chemical and biological weapons, and the new highly

---

FP7-SECURITY, Project ID: 28559, ETTIS - European security trends and threats in society, Vienna, DB Version 2016.

sophisticated situations in high-tech conflicts harbour a potentially new bundle of threats.

It is often overlooked "that the majority of casualties have historically resulted not from enemy weapons, but from diseases (especially infectious diseases), non-battle-related injuries, and stress."[236] Once all the innovations from converging technologies are in place and used, the time to react might be too short for humans and situations might become too complex for human judgement over the time. Even today, it becomes visible that cars driven by autonomous systems might be less dangerous than if driven by humans. Autonomous systems have better sensors and thus better situational awareness. Today this exists in the limited context of car-driving (and other even more standardised contexts), but it is obvious that this will change in the future.

Looking at the future threats in Chapter 2 and the emerging technological innovations presented in Chapter 3, the main challenges seem to be:

- Increasing interdependence and complexity of threats and technological opportunities;
- Increasing amount of knowledge required to benefit from technological innovations in threat situations;
- Increasing probability of being surprised by technological capabilities of other conflict partners involved.

It is important to recognize that the unique features of the military environment are directly affected by human performance and vice versa. This interdependence results in a technology race regarding autonomous systems. They are developed to substitute humans on the battlefield.

[236]Martinez-Lopez, Lester. 2004. Biotechnology Enablers for the *Soldier System of Systems*. In: The Bridge 34(3):17-25. National Academy of Engineering, Washington. p. 18.

However, the goal of innovation is to create the best autonomous system available.

Thinking of future military missions in which all potentially available innovations are successfully applied, a mission can be compromised not by better knowledge, but by smarter decision based on better knowledge. The soldiers' occupational environment will continue to be extremely stressful, maybe more mentally than physically. Some of the work might continue to be conducted outdoors in all types of weather and at all altitudes. However, more and more autonomous systems will replace soldiers. The workload will be 24/7 and possibly underlie sudden, rapid changes in intensity. Therefore, new capabilities and new process organisation will be required, with a very strong focus on develop the best available knowledge to be prepared for conflicts that might never happen.

The following figure shows a process to address the main challenge for future conflicts of having always the best possible knowledge available, without paying a huge amount of money to get this knowledge.

Figure 5: Knowledge as the most important strategic resource for future conflicts[237]

It is often stated that even greater demands will be made upon soldiers in the future. This is a faulty concept. Even if future operational concepts call for highly mobile forces enabled by increasingly sophisticated weapon and information systems[238], it will be necessary to build up a support infrastructure to take away some burden of knowledge from each single soldier.

---

[237] Klerx, Joachim: 2017, based on Klerx, Joachim: "ETTIS Global Threat Database". Unpublished, funded 2012 under: FP7-SECURITY, Project ID: 28559, ETTIS - European security trends and threats in society, Vienna, DB Version 2016

[238] Lester Martinez-Lopez, Biotechnology Enablers fort he Soldier System of System, In The Bridge, Biotechnology Revolution, September 1, 2004, Volume 34, Issue 3, https://www.nae.edu/Publications/Bridge/BiotechnologyRevolution/BiotechnologyEnablersfortheSoldierSystemofSystems.aspx accessed on 4 December 2017.

Since the famous 2002 report about converging technologies to 2017, it has become clearer that not all technological fields are equal with respect to their strategic relevance, and knowledge as well as knowledge management, research management, innovation management and training is definitely rank highest in importance.

However, knowing how to do this and how to develop proper support from all different disciplines is far beyond this publication. The first ideas might point to a direction that information systems need to be transformed into knowledge systems. Generic AI can support this, but automatic reasoning and, in particular, the development of new and creative innovations remain a mystery to computers with AI.

6 International Perspectives on Converging Technologies and Emerging Risks

The International Perspective

Doris Wolfslehner

Converging Technologies and Emerging Risks are discussed in different international frameworks, such as NATO, the Council of Europe, and the United Nations. The aim of the panel on International Perspectives was to start a discussion between these organisations in order to profit from each other's work and to stimulate deliberations on emerging risks related to the phenomenon of the convergence of technologies.

Ulf Ehlert illustrated the difficulty of creating a policy regarding new technological phenomena in relation to technologies by presenting the Collingridge Dilemma, which points to the lack of knowledge regarding a technology and its emerging risks when the technology is still new and the difficulty to regulate this technology once it has been established. He reflected on the question of the responsibility of science in the 21st century and pointed to open questions in relation to the conducting of scientific research, the so-called 'could-we' and 'should-we' questions.

Laurence Lwoff presented the work of the Council of Europe on Emerging Technologies, focussing on technology, intervention, and the control of individuals using these technologies as well as on related data protection issues. The Council of Europe identified new elements with regard to the discussion on Emerging Technologies, such as the speed of the development, the blurring of boundaries, complexity, uncertainty, and the emergence of new stakeholders, which are not necessarily bound by appropriate professional standards. As regards possible risks the Council of Europe expects consequences for the existing concepts of privacy, autonomy, and equity. It points to the critical issue that existing governance

mechanisms will not be sufficient to address the challenges of Emerging Technologies.

Peter Steiner presented an overview of the debate on Lethal Autonomous Weapons Systems within the United Nations and highlighted points of consensus in the related discussion, such as meaningful human control, the necessity of developing a guide on 'legal weapons review', and non-proliferation of Lethal Autonomous Weapons Systems through an international ban of such systems.

The exchange of views illustrated that the international community is aware of possible emerging risks related to converging technologies. The answer, however, to how these risks may be controlled is however still a good way ahead of us.

The Multilateral Debate about Lethal Autonomous Weapons Systems

Peter Steiner

The *Converging Technologies and Emerging Risks* conference 2016[239] looked at the trends and latest developments in the technology sector. The following chapters on international perspectives seek to shed light on the activities of three different international organisations (NATO, Council of Europe and the United Nations) in dealing with this technical revolution for the benefit of humanity.

In this short article I aim to outline the international perspective from the point of view of the United Nations. Based on a threat scenario that highlights the urgency of disarmament and arms control, I give a brief outline of the international landscape in Geneva, followed by an overview of the debate surrounding lethal autonomous weapons systems (LAWS).

The aim is to provide the reader with an impulse, which consequently should lead to a better understanding of multilateral processes.

Threat level, concept of security and debate – an outline

The High Level Panel on Threats, Challenges and Change, established by former Secretary General of the United Nations, Kofi Annan, in 2003, defined six threat clusters, which are subject to constant change[240]:

---

[239] Institute for Peace Support and Conflict Management: Conference on Converging Technologies and Emerging Risks – Challenges for the Security Sector. 19 May – 20 May 2016.
[240] United Nations. 2004. A more secure world: our shared responsibility. Report of the High-Level Panel on Threats, Challenges and Change. 12.

- Economic and social threats, including poverty, infectious diseases and environmental degradation;
- Inter-State conflict;
- Internal conflict, including civil war, genocide and other large-scale atrocities;
- Nuclear, radiological, chemical and biological weapons;
- Terrorism;
- Transnational organised crime.

The World Economic Forum annual Global Risks Report 2016 suggests additional risks concerning the economic, social and environmental sphere, which further highlight the complex challenges for security policy.[241] In sum, no state is able to face and manage these challenges on its own.

Security policy today is far more unpredictable than it was before the fall of the Berlin Wall. Therefore, disarmament and arms control are an integral part of international security. These concepts have to remain strong in times of crisis while taking into account the contemporary way of warfare. Arms control can provide a higher degree of predictability in the case of conflict and reduce the associated risk.

In order to understand the debate better, it is useful to trace back the development of the concept of security. In doing so, I largely rely on the observations of Christopher Daase. The definition of security concept evolved from a purely military security understanding, later taking into account economic considerations and thus the natural/ecological approach. More recently the humanitarian dimension of security has followed.[242] The

---

241 World Economic Forum. 2016. The Global Risks Report 2016. In: http://wef.ch/risks 2016, accessed on 01 September 2016.

242 Daase, Christopher. 2010. Der erweiterte Sicherheitsbegriff. Working Paper 1/2010. Goethe Universität Frankfurt: Projekt Sicherheitskultur im Wandel. 4.

particular context should be asssessed accordingly, dependent on whether we are talking about national or regional, economic or social security.

In the various disarmament fora different ideas of concepts of security have repeatedly collided. States that possess nuclear weapons emphasize the concept of national security as well as the importance of geostrategic balance. Both these states and the so-called 'umbrella states' view the maintenance of the strategic balance as a prerequisite for potential disarmament. They aim to advance arms control using different approaches (step by step, building blocks and the progressive approach).

The majority of states that do not possess nuclear weapons, however, try to prioritise humanitarian security and create legally binding regulations with the objective to enforce a weapons ban (in analogy to the Chemical Weapons Convention). In between these two concepts are the umbrella states, which stress the need for collective security, but are not completely closed off to the humanitarian agenda. This tense relationship between disarmament and the preservation of the strategic balance promotes the polarisation of relations.

The concept of strategic balance is not clearly defined because, according to Nash[243], this would mean that no actor can improve or that there can be no balance when clear strategies are applied.

Arms control and disarmament must have their regulative role in terms of stabilising measures. Due to the sensitivity of the subject matter, in principle no rapid progress can be expected. Perseverance and patience are

[243] Ross, Sean. 2015. What is the difference between a dominant strategy solution and a Nash equilibrium solution? In: http://www.investopedia.com/ask/answers/071515/what-difference-between-dominant-strategy-solution-and-nash-equilibrium-solution.asp, accessed on 25 August 2015. See also: Nash, John Forbes. 1950. The Bargaining Problem. In: Econometrica 18 (2):155-162.

the most important attributes in this struggle. Arms control has the potential to be undermined very quickly, as is illustrated by current security developments. National interests, regional constellations, pronounced mistrust adversely affect appropriate steps. Political will is a precondition for successful disarmament.

The subject of disarmament/arms control is not sufficiently addressed in the assessment of the respective security development. Potential opportunities and options are rarely used or not at all.

United Nations Office Geneva, UNOG

Besides New York and Vienna Geneva is the third centre with the classic focus on multilateral politics and traditionally of importance for Austria: disarmament, arms control, humanitarian issues, human rights and international law. Arms control and disarmament can be regarded as part of modern regulatory policies.

Geneva is a hub of global affairs and the centre of humanitarian issues (with the UNHCR, OCHA and IOM, ICRC as principal actors), human rights (the Human Rights Council still has links to arms control/disarmament, for example in the area of lethal autonomous weapons systems), as well as of economic issues, trade and public health (WHO, UNAIDS, Global Fund). The interdependences between these areas are not sufficiently taken into consideration in international security policy.

Geneva can be regarded as a barometer for future challenges, which acknowledges trends in international development at an early stage. An important example of the interaction of the mentioned dimensions (humanitarian issues and disarmament) are lethal autonomous weapons systems.

Debate in the United Nations – Lethal Autonomous Weapons Systems, LAWS

The technical innovation in the field of weapons and weapons systems is regulated by Article 36 of Additional Protocol I to the Geneva Conventions:

"In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."[244]

The efforts at innovation in the field of autonomous systems clearly illustrate military technological advances and will therefore influence strategies of, and guidelines for deployment.

In 2007, the debate surrounding LAWS was initiated by civil society with the Campaign to Stop Killer Robots. Civil society is an essential pillar in the field of arms control and disarmament. Besides its vital task of ensuring a sustained conventional dialogue between states, the dynamic activities of civil society also contributes significantly to the general advancement of the subject matter and should not be underestimated.

In the spring of 2013, the United Nations Special Rapporteur on extrajudicial killings, Christof Heyns, put the issue on the agenda of the United Nations clusters in Geneva.[245] Back then, Heyns supported an

---

[244] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I). Geneva 1977. Part III/Section I/Art.36.

[245] Human Rights Council: Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns. United Nations A/HRC/23/47, General Assembly 2013. *Summary:* "*Lethal autonomous robotics (LARs) are weapon systems that, once activated, can select*

immediate moratorium against 'killer robots' because he was concerned that autonomous robots, once activated, could ignore orders from humans. In addition, Heyns voiced the concern that states that have such technologies at their disposal would be more inclined to go to war. He laid the foundations for the treatment of this subject within the disarmament machinery.

Since 2014, the debate surrounding LAWS is taking place in the context of the Convention on Certain Conventional Weapons (CCW). The following topics have been addressed repeatedly:

Definitions: Some states have proposed a focus on the search for a precise definition; others have opposed this, arguing that this would delay the process. There is a consensus that any future development must comply with international law. Some delegations differentiate between 'autonomous', 'automatic' and 'teleoperated'. For the term 'autonomous', there are additional subcategories (semi- and fully autonomous). From the experts' point of view, at present there are no autonomous weapons systems operating independently of human supervision. However, this may be only a matter of technology and time. Above all, the majority of delegations are concerned with the study of artificial intelligence, which is why Self-Learning/Machine Learning[246], Self-Determination, Self-

---

and engage targets without further human intervention. They raise far-reaching concerns about the protection of life during war and peace. This includes the question of the extent to which they can be programmed to comply with the requirements of international humanitarian law and the standards protecting life under international human rights law. Beyond this, their deployment may be unacceptable because no adequate system of legal accountability can be devised, and because robots should not have the power of life and death over human beings. The Special Rapporteur recommends that States establish national moratoria on aspects of LARs, and calls for the establishment of a high level panel on LARs to articulate a policy for the international community on the issue."

[246] According to a study by the Pentagon in June 2016 machine learning is of great interest. Cf. Defence Science Board. 2016. Summer Study on Autonomy. Pentagon. p.7.

Assessment must be considered in the context of LAWS.[247] The issue of autonomy is technically and politically complex and can be defined and interpreted in a number of ways. It should be noted that it is necessary to re-evaluate our conception of the term system.

Control: There is a general consensus in this area. The majority of states advocate 'meaningful' human control. However, concepts like human judgement or intelligent partnership allow for different assessments and conclusions regarding the degree of autonomy and control and the way in which they are performed. It is unclear if and how autonomous weapons systems should fall under international legal framework. Therefore it is very important to ensure meaningful human control. The topic will remain on the agenda for some time to come.

Responsibility, proportionality: This topic was touched upon in the context of the commanding officers' and states' responsibility. In particular, Western states advocate a clear regulatory framework and stress the importance of a chain of responsibility (similar to a chain of command). In general, the question arises if a machine should be able to decide about life or death. The use of force is strictly regulated in international law (AP I to the Geneva Conventions, Article 51 (5) (b): Proportionality, Immediacy, etc.).

Review of weapons (systems): Legally binding reviews are regarded as a central instrument by some states in order to ensure compliance with international law. Therefore, they push for an international reviewing process or rather a 'guide on legal weapons review'.

---

[247] Nigitsch, Philipp. 2016. Memo of the final report of the chairmen of the last expert group meeting in April 2016. Presented on the occasion of the Review Conference of the Convention on Certain Conventional Weapons (CCW) 09/16.

Security context: Concerns were raised that LAWS could endanger global and regional security. An arms race undermining the already unstable balance could ensue. As a result, some delegations have suggested a preventive ban on such weapons systems.

At the meeting of experts in April 2016, the international community decided by consensus to submit a proposal to the Review Conference in December 2016 to establish an expert meeting at government level.[248] Meetings are planned in 2017 and possibly also 2018. The NGOs (subsumed under the Campaign to Stop Killer Robots) criticised the weakness of this approach for not taking into account the speed of technological advance or calling for sufficient human control.

The technologically advanced countries keep their options open. Especially already existing systems and the development in the civil sector clearly indicate that autonomy is the objective. The majority of states agreed that the development of civil autonomous systems should not be stopped (dual-use issue). These systems are particularly valuable for rescue and recovery services. This is illustrated by a further dilemma in arms control; the boundary between civil and military use is often hard to detect. Based on a cautious appraisal, the development of modern (autonomous) weapons

---

[248] Informal Meeting of Experts April 2016 for the Convention on Certain Conventional Weapons (CCW). Cf. http://unog.ch/80256EDD006B8954/(httpAssets)/6BB8A498B0A12A03C1257FDB00382863/$file/Recommendations_LAWS_2016_AdvancedVersion+(4+paras)+.pdf, accessed on 12 September 2016. Paragraph 3:
"3. The Informal Meeting of Experts recommends that the 2016 Fifth Review Conference of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons may decide to establish an open-ended Group of Governmental Experts (GGE) in accordance with established practice. The GGE should meet for an appropriate period of time starting in 20171 (original!) to explore and agree on possible recommendations on options related to emerging technologies in the area of LAWS, in the context of the objectives and purposes of the Convention, taking into account all proposals – past, present and future. The GGE should concentrate on technical and expert work in its first part and report on its progress to the 2017 Meeting of High Contracting Parties."

systems threatens to overtake efforts at containment on the part of the international community.

A step-by-step approach to autonomy can be expected. If and to what extent humans will be replaced cannot be established conclusively at present. In any case, the task will be to improve the synergy between humans and machines. Radically utopian ideas should be avoided while the contours of meaningful human control should be worked out.

The Austrian position

Austria advocates permanent meaningful human control of all autonomous weapons systems, regards the debate concerning CCW as valuable and emphasises the role of transparency in this context. In 2015 already, Austria proposed to set up an expert group. A state like Austria is active in a multilateral context by forming alliances in the field of disarmament and in compliance with its role as a catalyst.

Disarmament and arms control are difficult subject areas, and rapid and surprising developments are the exception. Success depends on the interplay of many factors. This includes local, national and regional constellations, interests as well as geopolitical positions.

Converging Technologies and Emerging Risks: Council of Europe Perspectives

Laurence Lwoff

Since the early 1980s, the Council of Europe has been following scientific and technological developments with a view to identifying and addressing the possible human rights challenges they raise. In 2015, work was initiated on emerging and converging technologies, which has already led and may lead to further specific activities and achievements in the next few years.

Council of Europe: a pan-European organisation

The Council of Europe (CoE), set up in 1949, is the first European intergovernmental organisation. 47 European states are members of the Council of Europe, including the 28 member states of the European Union. The CoE is also working closely with non-European states i.e. Canada, Holy See, Japan, Mexico and the United States of America[249], as well as Israel[250]. The CoE Headquarters are in Strasbourg (France), and its main aims are to strengthen human rights, democracy and the rule of law.

This European intergovernmental organisation develops international legal standards, but has also put in place monitoring mechanisms to monitor their application. Cooperation and training activities facilitate the implementation of those standards and help addressing possible related difficulties.

[249] Canada, Holy See, Japan, Mexico and the United States of America are observers to the Council of Europe.
[250] Israel is an observer to the Parliamentary Assembly of the Council of Europe.

Council of Europe and bioethics

The CoE's pioneering work in bioethics started at the beginning of the 1980s, and continues to be unique at the international level, due to its human-rights approach. It has become a reference at the European level, but also at the global level.

The CoE was guided by the following concerns: Scientific and technical developments in the biomedical field are a source of potential important benefits for human beings, in particular for human health, which are to be promoted; but, at the same time, the possibility of intervening in, and controlling human life and the human body increases. This raises concerns of possible abuse.

With its work in this field the CoE aims at protecting human rights with regard to the applications of biology and medicine, the former being one of the main pillars of the CoE's activities.

The Committee on Bioethics (DH-BIO)

This objective can only be achieved via a multidisciplinary approach. The importance of interaction, in particular between the legal and the biomedical fields, has to be underlined in this context. This is well reflected in the composition of the Committee on Bioethics (DH-BIO), the CoE's intergovernmental committee responsible for bioethics. The DH-BIO is composed of representatives from the 47 member states, mainly from the ministries of justice, health, and research as well as from public institutions, which illustrates its multi-disciplinary approach.

In addition to the states with observer status with regard to the CoE and its Parliamentary Assembly, Australia is also invited to participate in the work of the DH-BIO. Furthermore, other intergovernmental committees of the CoE, such as the Consultative Committee of the Convention for the

Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), participate in its work as well as the following intergovernmental organisations: the European Union, the WHO, the UNESCO, and the OECD.

The tasks of the DH-BIO are to further develop the legal corpus, in particular the principles laid down in the Convention on Human Rights and Biomedicine, to facilitate their implementation, but also to conduct regular re-examinations of adopted legal instruments in the light of the developments in the field concerned.

Finally, the DH-BIO, under the supervision of the Steering Committee for Human Rights (CDDH), also monitoring scientific and technological developments in the biomedical field in order to assess the ethical and legal challenges posed by them and, where appropriate, take action to address them.

Some achievements and their impact

The reference legal instrument is the Convention on Human Rights and Biomedicine (ETS n°164), opened for signature in Oviedo (Spain), in April 1997 and known as 'the Oviedo Convention'.[251] The Oviedo Convention is one of the key human rights instruments of the CoE. Whilst it has no formal link with the European Convention on Human Rights, it has close kinship with this text, from which it borrows several key concepts and terms, with the aim of preserving the coherence of the European legal system. It should also be mentioned that it provides for the possibility of asking the European Court of Human Rights (ECtHR) for advisory opinion on the interpretation of its provisions concerning legal issues

[251] Council of Europe.1997. Convention on Human Rights and Biomedicine. European Treaty Series No.164.

(Article 29). This possibility has never been used, but it also shows the link with the ECHR, for which this Convention has also become a reference. This is demonstrated by the development of the relevant case law of the ECtHR[252] and reference made by the ECtHR to the Oviedo Convention, as well as to related legal instruments and work achieved at intergovernmental level.

The objective of human rights protection is well reflected in the Article 1 of the Oviedo Convention, which requires State Parties to protect the dignity and identity of all human beings and guarantee everyone, without discrimination, respect for the integrity and all the rights and fundamental freedoms with regard to the applications of biology and medicine.

The drafters of the Oviedo Convention were guided by a double concern. First, individuals have to be shielded from any threat resulting from the improper use of medical and scientific developments. Second, the need to provide a common framework for the protection of human rights and dignity in both longstanding and developing areas concerning the applications of biology and medicine - a far more challenging objective for a legal instrument addressing a field in constant evolution. It was therefore important to ensure the lasting value of the principles that would be established.

The Convention contains a first set of provisions applying to daily medical practice. Those principles can be considered patient rights principles – hence the reference to this Convention as the 'European patient rights treaty'.

---

[252] European Court of Human Rights.2016. Research Report. Bioethics and the Case-Law of the Court. In: http://www.echr.coe.int/Documents/Research_report_bioethics_ENG.Pdf, accessed on 17 January 2017.

Key principles include: the primacy of the human being over the sole interest of science and society (Art. 2) - a particularly important principle in biomedical research, where freedom of research is reaffirmed but subject to the protection of the human rights of the participants. The Convention also requires that State Parties take measures to ensure equitable access to healthcare for their citizens (Art. 3).

The principle of free and informed consent prior to any intervention undertaken on a person (Art. 5) is a pillar in biomedicine. In this context, the Convention addresses the situation of persons not able to consent (Art. 6) and defines specific conditions to ensure their protection. Those provisions are presented as general rules, which are then specified further in specific chapters focusing on specific fields (see below).

The Convention also requires that everyone has the right to respect for private life in relation to information about his or her health. It also affirms the right of every person to know all details collected about their health. This implies also respect of the wish not to know – an increasingly important principle with regard to the development of genetics as well as the applications of information and communication technologies in the biomedical field.

But the Convention also lays down principles relevant to specific fields raising particular concerns for human rights: genetics (Chapter IV), organ- and tissue removal for transplantation (Chapter V) and biomedical research (Chapter VI).

Some of the provisions focusing on the human genome are particularly relevant when it comes to emerging technologies. The main concerns are non-discrimination on the basis of genetic characteristics (Art. 11) and the protection of privacy. This is duly taken into account when considering in particular predictive genetic testing (Art. 12). The safeguards established by the Convention appear particularly relevant with regard to the evolution of

genetics and sequencing technologies. The Convention limits interventions on the human genome to preventive, diagnostic or therapeutic purposes, and only when their aim is not to introduce any modification in the genome of any descendants (Article 13). New genome-editing technologies make the modification of genomes easier, more precise and cheaper. The potential application of this technology to the embryo and to germ lines prompted major ethical debates at the national and international level. The limits and prohibitions laid down in Article 13 provide an important reference in this context.

The Oviedo Convention is a framework legal instrument, whose principles have been complemented and developed in additional protocols focusing on specific fields. Four additional protocols have been adopted so far.

The First Protocol on human cloning[253] had not been provided for at the time the Convention was elaborated. It was a decision taken after the announcement of the birth of Dolly, the sheep, produced by nuclear transfer. The adoption of this Protocol within a very short period of time after this announcement bore testimony to an extremely wide political consensus and agreement on human rights challenges connected to this technology. This Protocol is the only internationally legally binding instrument prohibiting the cloning of human beings.

The three other additional protocols had already been provided for at a time when the Convention was elaborated, covering fields where developments raised particular concerns regarding the protection of human rights.

---

[253] Council of Europe.1998. Additional Protocol to the Convention on Human Rights and Biomedicine, on the Prohibition of Cloning Human Beings. European Treaty Series No.168.

The Additional Protocol on Transplantation of Organs and Tissues of Human Origin[254] further develops the principles laid down in Chapter VI of the Oviedo Convention, aiming at the protection of donors and recipients. Its provisions address in particular living and deceased donation, the protection of donors not able to consent, the establishment of appropriate transplantation systems and the prohibition of organ trafficking.

The Additional Protocol concerning Biomedical Research[255] mainly focuses on the protection of participants in biomedical research. It specifies the conditions for consent, access to information resulting from research and care of participants. It lays down specific requirements concerning the ethical review of research projects to assess the respect of human rights.

The Additional Protocol concerning Genetic Testing for Health Purposes[256] is the most recent protocol, which mainly addresses issues of privacy and non-discrimination in relation to genetic testing. It includes specific provisions for the protection of persons not able to consent, in particular minors.

What is the impact of the Oviedo Convention?

The Convention had and continues to have a profound impact, both on legislation and in practice. This is not restricted to countries that have

---

254 Council of Europe: Additional Protocol to the Convention on Human Rights and Biomedicine, on Transplantation of Organs and Tissues of Human Origin.1998. European Treaty Series No.186.

255 Council of Europe.1998. Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research. European Treaty Series No.195.

256 Council of Europe.1998. Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes. European Treaty Series No. 203.

ratified or acceded[257] to the Convention, but is also a reality in countries that have not even signed[258] it. This was the result of a survey in 2009 conducted in the Member States of the Council of Europe.[259] The impact of the Convention is acknowledged in many different fields: patient rights, mental health, reproductive medicine, geriatric care, research etc. There is a whole list of national legal instruments the drafting of which was influenced by the Convention.

The latter has also become a reference at European level, such as for the European Court of Human Rights, as already pointed out; but also within the EU the Charter of Fundamental Rights borrows principles from the Oviedo Convention, in particular concerning the protection of personal integrity (Article 3). It is also referred to in several EU directives and regulations and part of the ethical rules for research funding.

The Convention has furthermore become a reference at global level. It is indeed one of the rare regional instruments referred to in texts of the United Nations, in particular the Universal Declaration on Bioethics and Human Rights[260]. Finally, the Oviedo Convention was also referred to by

---

257 Ratification of/accession to a treaty is an act by which the State expresses its definitive consent to be bound by the treaty. Then, the State Party must respect the provisions of the treaty and implement it.

258 Signature of a treaty is an act by which the State expresses its interest to the treaty and its intention to become a Party. The State is not bound by the signature. However, it has the obligation not to defeat the object and purpose of the treaty until it has made its intention clear not to become a Party to the treaty (See Article 18 of the Vienna Convention).

259 Questionnaire on the impact of the Oviedo Convention and its Protocols on legislation and practices. The survey was carried out for the purpose of the conference on "the Convention on Human rights and Biomedicine: 10 years later"(Strasbourg, 3 November 2009).

260 United Nations. 2005. Universal Declaration on Bioethics and Human Rights. Adopted on 19 October 2005.

the Inter-American Court of Human Rights in a decision against Costa Rica (case of Artavia Murillo et al. ('In vitro fertilization') v. Costa Rica).[261]

Other legal instruments, which are not legally binding, have also been developed by the DH-BIO, such as Recommendation (2016)6 of the CoE Committee of Ministers on Research on Biological Materials of Human Origin, adopted in May 2016.

Emerging technologies

In recent years more and more innovations in the biomedical field are emerging from the convergence of developments in different domains, including nanotechnology, cognitive science and information technology.[262] As a result of this convergence, we can observe an increasing interaction between life sciences and the engineering sciences. This interaction and convergence of different scientific and technological fields that are important sources of possible progress, in particular for human health, also raise new questions about the implications of these developments for human rights and human dignity. This prompted the DH-BIO to include emerging technologies in its working programme.

International conference

To launch its work in this field, the DH-BIO organised an international conference on '*Emerging Technologies and Human Rights'* in May 2015[263], the

[261] Inter-American Court of Human Rights. 2012. Case of Artavia Murillo et al. (In vitro fertilization) v. Costa Rica. Judgement of 28 November 2012.
[262] Council of Europe, Bioethics, Emerging technologies, https://www.coe.int/en/web/bioethics/emerging-technologies accessed 6 December 2017.
[263] Committee on Bioethics (DH-BIO) of the Council of Europe: International Conference on Emerging Technologies and Human Rights. Strasbourg 4-5 May 2015. See also https://www.coe.int/en/web/bioethics/-/emerging-technologies-conferen-1 accessed on 13 November 2017.

aim of which was to identify priority human rights challenges, which arose in connection with emerging and converging technologies (such as Nano-, Bio-, Info- and Cognitive technologies - NBICs). Rather than looking into each technology, a transversal approach was adopted for the conference programme, based on the type of 'interventions' on human beings made possible by technological developments and the key ethical concerns they raise. This objective is in line with the mandate of the DH-BIO and, more generally, of the organisation itself.

Background studies

The conference was informed by two background studies commissioned by the DH-BIO. The first one '*From Bio to NBIC convergence – from medical practice to daily life*'[264], focused more on scientific aspects and was developed by the Rathenau Instituut, a technology assessment institution in the Netherlands. The second study: '*Report on ethical issues raised by emerging sciences and technologies*'[265] was prepared by the Centre for the Study of Sciences and Humanities of the Bergen University in Norway.

The Rathenau Study highlighted two major trends in bioengineering: Biology is becoming technology and vice-versa. "Humans and technology are becoming increasingly entangled 'and' biological and biomedical

[264] Van Est, Rinie et al. 2014. From Bio to NBIC convergence – From Medical Practice to Daily Life. Rathenau Instituut, The Hague: Report written for the Council of Europe, Committee on Bioethics. See also https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680307575, accessed 18 January 2017.
[265] Strand, Roger & Kaiser, Matthias. 2015. Report on Ethical Issues raised by Emerging Sciences and Technologies. Centre for the Study of the Sciences and the Humanities: University of Bergen. See also https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168030751d, accessed 18 January 2017.

technologies are increasingly applied in multiple ways outside the practices of professional health research or health care"[266].

Using the first study as a basis, the report from Bergen University examined ethical challenges raised by such developments. It highlighted in particular the uncertainty and complexity of these technological developments and their applications as well as the influence of imaginary scenarios on research practice and policy. It looked at challenges to human identity and integrity as well as autonomy and privacy. It also briefly discussed some cross-cutting aspects, including the blurring of lines between medical and non-medical domains, and the particular ethical challenges of the military use of technologies. With regard to the latter, it noted that if there was comprehensive international governance of nuclear as well as biological and chemical weapons, there did not seem to be equivalent institutions for warfare making use of robotics, nanotechnology, neurotechnology and converging technologies.

Main topics addressed

The conference programme included four main sessions, which focused on technology, intervention and the control of individuals by using neurotechnologies and genetics as case studies. The second session was dedicated to the new dimension of data collection and processing, in which the massive generation of health data as well as big data, in particular, were referred to. Equality of access to technological applications was addressed in the third session. Finally, governance, highlighted in the studies prepared as a key issue, was at the centre of the last thematic session.

---

[266] Van Est, Rinie et al. 2014. From Bio to NBIC convergence – From Medical Practice to Daily Life. Report written for the Council of Europe, Committee on Bioethics. The Hague: Rathenau Instituut. 8.

Each of these topics was elaborated on by the respective speaker, who discussed the issues at stake, namely the ethical and social perspectives and the human right challenges raised.

Some points underlined…

The significant potential benefits for individuals and society were again acknowledged. As concluded by the rapporteurs to the conference, these benefits *"might be medical, personal, social or economic or, most likely, a combination of all of these."* [267]

Other aspects of emerging and converging technologies were also underlined, including their potential for increasing control on individuals.

Persuasiveness was highlighted in this context. As indicated in the Rathenau report: "*Persuasive technology builds on insights derived from psychology and behavioural sciences as well as from (computer) design practices. Large-scale data collection on online behaviour can be used to analyse how users make their choices, which enables the design to adapt to this. By designing choices and the interaction with technology, users can be stimulated to make certain choices."* [268]

The close connection between the persuasive and personality-altering or enhancement aspects of the technologies was also stressed.

The fast and continuing development of these technologies and their convergence through the application of digital technologies, whose capacity

[267] Witthall, Hugh & Pallazani, Laura & Fuchs, Michael & Gaszo, Andre. 2015. Emerging Technologies and Human Rights. Conference Report May 2015. 29. See also https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Emerging%20techno%20Report%20e_DH-BIO.pdf, accessed 18 January 2017.

[268] Van Est, Rinie et al. 2014. From Bio to NBIC convergence – From Medical Practice to Daily Life. Report written for the Council of Europe, Committee on Bioethics. The Hague: Rathenau Instituut. 34.

and power are expanding rapidly, were also noted. This speed of development raises challenges for regulatory and existing governance mechanisms.

The 'blurring' and 'breaking' of boundaries are also characteristics of the application of these technologies. The boundaries between the medical and non-medical fields can be blurred, as illustrated by the use of direct-to-consumer (DTC) genetic tests as well as health- and fitness-tracking apps and devices. The blurring of boundaries also includes the emergence of technical tools at the crossroads of therapy and enhancement.

Boundaries may be broken where the technology developed for one purpose is used in a totally different setting. In this respect reference could be made to the "dual use" of neuromodulation technologies, developed for health purpose but also used in gaming, which could also be considered for other purposes, such as military ones. This has also consequences for the applicability of regulations: For instance, the legal instruments regulating the use of medical technology or medical devices may not apply to the use of the same technology outside the health field.

Complexity and uncertainty are inherent elements of certain emerging technologies, and especially the latter may challenge the way we assess and manage risk.

Finally, the driving forces and new stakeholders (not necessarily bound by appropriate professional standards) in these technological developments also raise additional challenges to address the human rights issues at stake.

…and concerns

Emerging technologies are developing extremely rapidly, and their complexity and the uncertainties attached to them, raise concerns for safety, both from a quantitative and qualitative point of view. Indeed, the risks related to these technologies cannot be calculated through traditional

assessment methods. Furthermore, emerging technologies manipulating the human body and brain give rise to concerns about the physical and mental integrity of individuals. Mental integrity may be at stake when it comes to persuasive and personality-altering technologies. Non-invasive brain stimulation, for example, may be used for therapeutic purposes but also with enhancing aims, with the potential of altering the personality.

The protection of privacy and confidentiality may also be challenged in unprecedented ways. The emergence of 'big data' entails the generation and collection of massive amounts of personal data, and challenges the possibility for the individuals concerned to exercise their right to privacy.

The autonomy of individuals may be affected. Emerging technologies can be considered to enable individuals to become proactive managers of their own condition. However, they could also lead to heteronomy, for example, if freely collected data is available to third parties and used for purposes that do not serve the self-determination and well-being of the concerned individuals.

Equality of access to the beneficial applications of these technologies and the sharing of risks was also a concern with regard to the developments of emerging technologies and their applications.

Finally, the issue of governance was highlighted as a key element to be considered in relation to these technologies. The very novelty of these technologies and the way they are combined in novel applications can make it particularly difficult to find ways of addressing the challenges they raise. Indeed, as stressed earlier, they can reach across the boundaries that often shape our understanding of, or our responses to them. The governance mechanisms in place, which are rather field-specific, may need to be reconsidered in this context. Governance mechanisms set up in the biomedical field do not cover other areas where the technologies would be

applied, however, with similar human rights concerns raised by their applications.

Some key findings

One of the conclusions highlighted by the rapporteurs of the conference was that there was no specific or universal response to the challenges raised by these technological developments. Furthermore, it was necessary "*to focus not simply on the technologies themselves, but rather on the practices, the goals, and the context in which they emerge*." [269]

A certain number of areas have been identified as particularly challenging. Two need to be particularly underlined: the relevance of existing legal frameworks and governance mechanisms.

How can existing legal instrument contribute to addressing human rights challenges raised by these technological developments? Which governance mechanisms are capable of responding to a large variety of applications and contexts? How to develop the participatory mechanisms for involving a wider public in the discussion around research policies, practices and governance that emerging and converging technologies necessarily require?

Current work

Work has already been undertaken with regard to specific developments with important implications for human beings and human rights. This is the case with gene-editing technologies. Such technologies make it possible to modify human genetic characteristics in a much more efficient and detailed way. There is considerable research potential, in particular for the

[269] Witthall, Hugh & Pallazani, Laura & Fuchs, Michael & Gaszo, Andre. 2015. Emerging Technologies and Human Rights. Conference Report May 2015. 29.

benefit of human health. But it is also a source of concerns with regard to possible abuses, in particular the intentional modification of the human genome so as to produce individuals or subgroups with particular characteristics and required qualities. These concerns have led the Committee on Bioethics (DH-BIO) to adopt a statement on genome-editing technologies[270]. In its statement the DH-BIO, composed of the representatives of the 47 Member States of the Council of Europe, reaffirmed the principles laid down in the Convention on Human Rights and Biomedicine as legal basis, in particular its Article 13 (Intervention on the human genome), for the debate called for on an international level on the fundamental questions raised by these recent technological developments. Furthermore it agreed, as part of its mandate, to examine the ethical and legal challenges raised by the emerging genome-editing technologies, in the light of the principles laid down in the Oviedo Convention.

Emerging technologies are also on the agenda of other Council of Europe bodies. The T-PD (Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) is preparing guidelines on Big Data and a recommendation on health-related data taking into account emerging and converging technologies.

The Parliamentary Assembly of the Council of Europe - the consultative body of the organisation, composed of delegations of the national parliaments of the CoE Member States – is currently preparing a report on 'genetically engineered human beings' and another one on 'technological convergence, artificial intelligence and human rights'.

---

[270] Statement on gene editing technologies, adopted by the DH-BIO on 2 December 2015 https://rm.coe.int/168049034a accessed on 13 November 2017.

In conclusion, emerging technologies are now an integral part of the Council of Europe activities programme. The DH-BIO, together with other CoE committees and bodies, will continue its strategic reflection with a view to initiate actions regarding the protection of human rights focussing on possible misuses and abuses of these emerging and converging technologies. However, cooperation and complementary actions with other intergovernmental organisations on the European as well as the global level will be needed in this context, taking into account respective fields of competence and expertise.

As underlined by Ms. Gabriella Battaini-Dragoni, Deputy Secretary General of the Council of Europe, at the opening of the Conference on emerging technologies and human rights in May 2015 "…carrying out multidisciplinary discussion, identifying challenges to human rights and addressing them, will contribute to build trust and promote progress for the benefit of human beings."[271]

[271] Council of Europe. Conference on emerging technologies and human rights. Strasbourg. May 4-5 2015.

Converging Technologies – A Topic for NATO?[272]

Ulf Ehlert

The NATO Picture. What is NATO's Role? What is NATO's Stake?

Alliance Strategic Concept

At the Lisbon Summit in November 2010, the Heads of State and Government adopted the Alliance Strategic Concept[273] as high-level guidance for the North-Atlantic Alliance. This concept defines three core tasks for the Alliance: Collective Defence, Crisis Management, and Cooperative Security. All three are targeted to achieving the political objectives while maintaining the military means of NATO and its member nations.

It can hardly surprise that this high-level political document remains entirely unspecific regarding specific technologies and their potential implications. Still, the Strategic Concept clearly articulates the need to "… *ensure that the Alliance is at the front edge in assessing the security impact of emerging technologies, and that military planning takes the potential threats into account* …"[274] This commitment to technology risk assessment gives evidence to the Alliance's strong interest in emerging technologies and their potential impact, implicitly including converging technologies as well.

[272] The views expressed in this article should be understood as solely those of the author.
[273] NATO. 2010. Active Engagement, Modern Defense. Strategic Concept. Lisbon.
[274] Ibid. 17.

Science & Technology in NATO

NATO was established as an international politico-military alliance, its structures and processes designed to support and facilitate strategic-level decision making on defence and security matters in the Euro-Atlantic area. Against this backdrop, Science & Technology (S&T) is an essential underpinning, supporting the core tasks stated in the Strategic Concept and striving to maintain the advantage in technology and knowledge that provides a critical force multiplier to Nations and NATO. In the Alliance context, S&T broadly covers basic and applied research across the entire spectrum of physical-, engineering-, information-, human-, medical- and social sciences.

In fact, a large number of NATO entities (e.g. commands, committees or agencies) hold stakes in S&T. Each of these entities pursues its own specific mission; and often their relation to S&T, i.e. the stake that they hold, is tangential. As an orientation, they broadly fall into three categories:

Many stakeholders benefit from S&T as customers, exploiting S&T results as appropriate to achieve their specific mission, but without being actively involved in 'doing S&T';

A few stakeholders are designated to execute dedicated S&T programmes as essential part of their mission; these programmes have different scales, topical portfolios, or funding mechanisms;

Yet, other stakeholders influence requirement definition or investment decisions that inform and orient future S&T activities.

Due to the broad range of stakeholders' missions and portfolios, the close coordination, cooperation and collaboration between all stakeholders is of vital importance to avoid unnecessary duplication while encouraging synergies, and to seek complementarities for burden sharing. Coherence of

effort across all stakeholders is promoted through an overarching NATO S&T Strategy; its implementation is overseen by the NATO S&T Organization. Topical guidance for medium- to longer-term planning is expressed through the NATO S&T Priorities.

Strategy

To foster the collaboration and synergies across all NATO S&T stakeholders, the North Atlantic Council adopted the NATO Science & Technology Strategy in January 2013. This Strategy formulates the mission of NATO S&T to enable and focus the generation and exploitation of scientific knowledge and technological innovation in order to support the Alliance's core tasks[275], thereby promoting the political and military effectiveness of the Alliance.

Under that broad heading, the Strategy articulates the following three strategic objectives:

Support capability development – NATO S&T supports capability development by bringing scientific knowledge and technological innovation to bear on the definition, development, demonstration, improvement, cost reduction and evaluation of sustainable, connected and interoperable defence and security capabilities for the benefit of the Nations and NATO, in line with NATO defence-planning priorities, in the short, medium, and the long term.[276]

---

[275] NATO, NATO Science & Technology Strategy, p.3, https://www.sto.nato.int/NATODocs/NATO%20Documents/Public/NATO-Science-and-Technology-Strategy-Public-Release.pdf accessed 7 December 2017.
[276] NATO, NATO Science & Technology Strategy, p.3, https://www.sto.nato.int/NATODocs/NATO%20Documents/Public/NATO-Science-and-Technology-Strategy-Public-Release.pdf accessed 7 December 2017.

Foster consultation and partnerships – NATO S&T contributes to political consultation and partnership objectives by conducting cooperative S&T activities between the Alliance and non-NATO Nations, in line with NATO's partnership policy, and thus, over time, fostering strategic and technological interoperability. NATO S&T enhances security dialogue and mitigates threats by building trusted relationships, even in situations where direct political dialogue is difficult.

Deliver knowledge, analysis, and advice – NATO S&T provides targeted and timely evidence-based knowledge, analysis, and advice, in response to requests or proactively, using and developing appropriate tools, such as Operational Research and Analysis, to contribute effectively to political and military planning and decision making across the full spectrum of NATO and Nations' activities.

The strategic objectives build on the Alliance core tasks defined in the Strategic Concept, and reframe them as concrete guidance for NATO S&T. In developing these objectives, NATO took into account the essential driving forces that shape the global S&T environment, including increasing speed and complexity, the blurring divide between defence and security, the economic challenges Allies and partners are faced with, the globalisation of S&T, the evolving role of industry as well as converging technologies:

Converging technologies – Scientific trends suggest that nano-, bio-, and information technologies along with cognitive sciences will converge to enable breakthrough capabilities, for both civilian and military applications.[277] At the heart of this development is the increase in interdisciplinary collaboration among S&T experts. Such collaboration not

[277] NATO, NATO Science & Technology Strategy, p.6, https://www.sto.nato.int/NATODocs/NATO%20Documents/Public/NATO-Science-and-Technology-Strategy-Public-Release.pdf accessed 7 December 2017.

only enables significant breakthroughs, it provides multiple paths for the exploitation of the results, thus accelerating the implementation of S&T innovation. And as psychological, societal, and ethical impacts of technology receive increased attention, social sciences play an ever more important role in this collaboration.

This notion of converging technologies was not intended to be an issue addressed by NATO S&T; it rather served as a prominent example of the type of interdisciplinary challenge that S&T would need to overcome. Still, this notion clearly acknowledges the importance of converging technologies for the Alliance.

Organisation

NATO offers a variety of frameworks to facilitate the generation and exchange of knowledge and to promote the exploitation of S&T results in international collaboration. Within the trusted environment of NATO, participants can capitalise on the diversity of approaches and the different schools of thought to augment their own resources and investments. Acknowledging that the majority of S&T efforts are funded directly by the Nations in pursuit of their individual objectives, S&T for the Alliance leverages past and current S&T investments and informs investment decisions on future S&T activities and programmes.

The collaboration in NATO S&T is of voluntary nature; its intensity is tailored by the participants to meet their capabilities, interests and needs. The spectrum of engagement ranges from the exchange of S&T results through the coordination of individual S&T projects to the joint planning, execution, and exploitation of entire S&T programmes.

NATO Science & Technology Organization

Within the diverse set of S&T stakeholders, the NATO Science & Technology Organization (STO) plays the critical role of developing and maintaining the strategic guidance for S&T in NATO, without prejudice to the responsibilities and authority of the individual stakeholders in NATO and the Nations. In this overarching role, the STO serves as the focal point for the coordination of all S&T programmes and activities within NATO. The STO is governed by the NATO Science & Technology Board (STB), which is composed on the senior S&T managers of the Nations.

The main focus of the STO is the planning, execution and delivery of the largest NATO S&T work programme. Covering the full spectrum of defence and security-related S&T, this programme is designed to promote multinational collaboration that augments each contributor's resources by leveraging the knowledge, skills, and investments made available by all contributors. The participating Nations (allies as well as partners) fund their individual contributions in line with their own specific objectives; NATO funds only a small portion of the programme directly in support of overarching Alliance objectives.

The STO is home to the world's largest network of defence and security scientists and engineers: every year, over 4,500 subject matter experts from governmental, industrial, or academic affiliations actively contribute to the S&T work programme. This network is structured in seven topical domains, each embracing a broad spectrum of scientific fields; each designed to address all militarily relevant aspects:

- Applied Vehicle Technology Panel (AVT);
- Human Factors and Medicine Panel (HFM);
- Information Systems Technology Panel (IST);
- Modelling and Simulation Group (MSG);
- Systems Analysis and Studies Panel (SAS);

- Systems Concepts and Integration Panel (SCI); and
- Sensors and Electronics Technology Panel (SET).

For each domain, a committee of national defence S&T managers and experts is responsible to the STB for planning and by executing the S&T activities it contributes to the STO collaborative work programme. In each domain, several hundred national subject matter experts are actively involved in planning and executing commonly agreed S&T activities, such as joint research projects, conferences, workshops, lectures, or technology demonstrations. Every year, the STO runs well over 200 such activities; for around 70% of those activities Partner Nations are invited to participate. The concrete topics for all these STO activities are defined on a case-by-case basis, according to the interests, capacities, and needs of the participating Nations.

Given that the STO's expert network is structured along topical domains as indicated above, a cross-disciplinary theme like converging technologies has many potential entry points and contributors. As is often the case for interdisciplinary research, there are many partial owners, each interested in a specific aspect of the overall topic.

Priorities

In order to guide the medium- to long-term planning across NATO S&T, the STO has developed NATO S&T Priorities. These Priorities are firmly rooted in NATO's military capability requirements and informed by scientific knowledge gaps and emerging technology opportunities. They offer national S&T planners additional orientation from an overarching NATO perspective, seeking to inform national S&T investments, while respecting sovereign national budget decisions.

The 2016 NATO S&T Priorities are organised into the following ten S&T Areas that provide a broad reference frame covering the full spectrum of S&T in defence and security:

- Precision Engagement
- Advanced Human Performance & Health
- Cultural, Social & Organisational Behaviours
- Information Analysis & Decision Support
- Data Collection & Processing
- Communications & Networks
- Autonomy
- Power & Energy
- Platforms & Materials
- Advanced Systems Concepts

Each of these broad S&T areas includes up to six Targets of Emphasis (ToE), which provide selective focus and orientation for future S&T activities. These ToEs present challenges from two different perspectives; more research is needed to either make progress towards delivering a military capability or to overcome a significant knowledge gap, for example the implications of emerging technologies. Many of the ToEs directly relate to converging technologies; a short summary includes the following (with the respective S&T Area indicated in brackets):

- Rules of Engagement, Legal, and Ethical Implications (Precision Engagement)
- Human Resiliency (Advanced Human Performance & Health)
- Medical Solutions for Health Optimisation (Advanced Human Performance & Health)
- Enhanced Cognitive Performance (Advanced Human Performance & Health)

- Human/Machine Interfaces (Advanced Human Performance & Health)
- Big Data & Long Data Processing and Analysis (Information Analysis & Decision Support)
- Advanced and Adaptive Materials (Platforms & Materials)
- Integrating Live & Simulation Systems (Advanced Systems Concepts)
- High Assurance Engineering & Validation (Advanced Systems Concepts)

Even though the NATO S&T Priorities do not explicitly call for research on converging technologies, they implicitly cover many of the essential aspects that need to be addressed. Therefore, aspects of converging technologies are addressed in NATO S&T activities; these are always shaped by the participating Nations' interests.

Policymaking in NATO

Any NATO policy is the expression of the common will of the Allies, adopted by the consensus of all. Such policies are clearly focused on international defence policy, embracing the responsibilities of national Ministries of Defence and Ministries of Foreign Affairs. Underpinning or tangential topics, such as economics, industry, education, or technology, will be taken into consideration; but they are not considered topics for dedicated NATO policies.

Individual Allies follow the subject of converging technologies, and pursue national policies (either implicit or explicit, potentially up to regulations and law making) to secure their individual political, economic, and societal interests. In these domestic deliberations, defence might be taken into account, but will not be the driving consideration. As a result, the views of Allies on the importance of converging technologies are rather fragmented.

Role of NATO

Nations interested in pursuing the further development and maturation of converging technologies can choose a NATO framework, like the STO, to collaborate with like-minded Allies and Partners. In this voluntary collaboration, they retain full flexibility regarding how much of their individual national S&T investments they want to share, and what they want to focus their joint projects on.

This collaboration will push the envelope of emerging technologies, such as converging technologies; and it will advance the understanding of their potential impact on military operations. If likely risks appear to outweigh potential benefits, NATO could also serve as a forum for discussing policies to mitigate such risks. Adopting such policies would then necessarily require the consensus of all Allies. Given the current lack of a commonly agreed risk that converging technologies might bring for NATO and its Allies, a NATO policy on converging technologies is not on the horizon.

It is obvious that the institutional framework of NATO is a challenging environment to develop any policy in. But even outside this framework, for example in a single sovereign nation, policymaking can be difficult. Policies on emerging technologies are a particular topic that turns out to be fraught with numerous problems.

The bigger picture - the dilemma of policymaking regarding emerging technologies. Past. Present. Future?

The known dilemma

Policymaking is never easy, regardless of the topic. It always requires striking a delicate balance between the divergent interests and needs of a broad range of stakeholders. But when it comes to emerging technologies,

the fundamental challenge of policymaking becomes particularly pronounced: How to devise meaningful policy on something that does not yet exist? How to engage stakeholders that are not yet identified?

At the heart of this challenge is a divergence between the knowledge of a possible problem, on the one hand, and the control over that problem, on the other hand. David Collingridge captured it well in his book on 'The Social Control of Technology'. Back in 1980 he observed the dilemma of control:

When change is easy,
the need for it cannot be foreseen;
when the need for change is apparent,
change has become expensive, difficult and time consuming.[278]

Known as the **Collingridge Dilemma**, this formulation elegantly paraphrases the challenges of policymaking regarding emerging technologies between two extremes. In the first instance, at the beginning of the evolution of a novel technology, we do not know all its future applications, nor can we judge its future impact. But at this time, it would still be easy to exert control over the further course of that development, for example to re-direct it or to limit its distribution. In the second case, when a technology has matured, we can clearly see its impact, its intended effects as well as its unintended consequences. We can thus define what we would like to change, how we would want to control that technology. Yet at that time, because the technology is already in the market, because it is widely distributed and used, our means of control are very limited. In the first instance, we have control

[278] Collingridge, David. 1980. The Social Control of Technology. London. Frances Pinter. Preface, Page 11

but lack knowledge. In the second case, we have knowledge but lack control. i.e. the more we know the less we control.[279]

While the Collingridge Dilemma provides a good description of the challenge, it does not offer an explanation. The root cause for this dilemma is not simply found in human nature, nor is it the essence of policymaking. Rather, its deeper reason is directly related to the way in which technology develops and matures over time.

The nature of technology

Technology is widely understood as a key driver for human progress and prosperity, yet its inner workings have remained a puzzle to many. A thorough analysis of *what technology is and how it evolves* was published by the engineer, economist, and complexity researcher W. Brian Arthur in 2009. His 'The Nature of Technology'[280] offers us further insight into the root causes of the Collingridge Dilemma.

In essence, Arthur describes technology as a complex adaptive system that evolves along a path that is not predetermined. While this path might be explained in hindsight, it cannot be predicted a priori. To illustrate his point, Arthur suggests three key characteristics of technologies:

- A technology is composed of elements that are technologies themselves.
- A technology is the orchestration of phenomena to a purpose.

[279] Ulf Ehlert, Society´s ambiguity, Understanding Innovation, https://understandinginnovation.blog/2013/11/06/societys-ambiguity/, 06 Nov 2013, accessed 6. December 2017.
[280] Arthur, W. Brian. 2009. The Nature of Technology. What it is and how it evolves. Free Press New York.

- Technology areas co-evolve with society in a process of mutual adaptation.

The first characteristic explains the self-similarity of technologies. Arthur uses the example of jet engines, their numerous components (e.g. compressor) and countless parts (e.g. shaft, blades, cowling): they all are technologies in themselves. If you think about the production of these individual parts, you will see yet more technologies: from mining the raw material to transportation, processing, finishing, and assembly. You could add the design process with all the information technology and knowledge management tools. Include the testing and validation as well. And even then you only have a jet engine, which is just one of the many elements of an aircraft, which again is only one of the many components of the global air traffic system that each of us rely on almost every day, be it for business or for leisure purposes. Taking this full background into consideration, all the tangible and intangible, the visible and invisible technologies, this characteristic also explains the path-dependence of technology development: any novel technology is always built upon predecessor technologies. Technology cannot jump, say, from flint stone to nuclear power plant.

The second characteristic describes how we actually create a technology: we employ our understanding of natural phenomena (like electric conduction or thermal insulation) and combine them to achieve an objective. This objective, or purpose, is defined by humans; and without such a purpose, we might have a brilliant idea, but not a functional, useful technology. That is an essential observation. Technology always serves a human purpose; it neither has a life of its own nor an inherent reason for being; technology is always subject to human intent. Furthermore, this characteristic implies that technology development is actually a shared effort and responsibility, shared between specialists and laymen. On the specialist side, the orchestration is the discipline and art of engineers, while scientists focus on the discovery and validation of phenomena. On the layman side, the

expression of purpose is everybody's business, as a single user, as one of many customers, and as a citizen. Each of them might drive the development of a novel technology (through a novel orchestration, by discovering a novel phenomenon, or by defining a novel purpose). And each of them bears responsibility for the outcome.

Finally, the third characteristic articulates the interplay between technology areas and society at large. You could think of technology areas as families of orchestrations of a set of phenomena, which are applicable to many purposes but specific to none. Examples, such as steam power, railway, petro-chemistry, or microelectronics, show that they have shaped and often transformed economies and societies. However, the reverse influence is less obvious, and sometimes forgotten: how society has shaped technology areas. The steam engine was first developed to pump water from coalmines, and the success of that application triggered the imagination of developers and users alike to consider additional problems that a steam engine could solve. These considerations led to the mechanisation of manufacture (driven by static, immobile steam engines) and agriculture (employing mobile steam engines). In this example, the story started with water in coal mines and ended with the demise of horse and oxen as mankind's primary power sources. This long-term result had neither been foreseeable nor intended, let alone planned. Rather, it is the result of technology influencing society *and* of society influencing technology. Both these influences occur at the same time, they overlap and interact; hence Arthur's notions of *co*-evolution and *mutual* adaptation. The outcome is the spiral forward movement we call progress.

If technology areas co-evolve with society, and if technology does not have a purpose of its own, we arrive at yet another fundamental question: What is our motivation in pursuing technology development, and what do we expect from technology? What do we really want?

Human motivations / Human expectations

In 2010, historian and archaeologist Ian Morris published a long-data analysis of human development in different corners of the globe, covering the 16,000 years since the last Ice Age. [281] True to the book's subtitle, Morris is keenly interested in 'The Patterns of History, and What They Reveal About the Future'. Based on his research, he acknowledges the differences between individuals, but he concludes that large groups of people (like societies) will always display similar behaviour regardless of location or time. And he expresses that concept in candid words:

Change is caused by lazy, greedy, frightened people
looking for easier, more profitable, and safer ways of doing things.
And they rarely know what they are doing.[282]

People do not have an explicit desire for technology as such; they rather use technology as their tool to change and adjust their environment according to their needs. Fully in line with Arthur's second characteristic, technology is subject to human purpose; in very general terms, technology generates *easier, more profitable, and safer ways of doing things*. But apart from the intended impact, i.e. the desired changes, technology leads to unintended consequences as well. And Morris clearly pronounces how severely limited our ability is to foresee the full consequences of the technologies we employ. Which leads to a search for the underlying reasons: *Why is it that we do not anticipate the full impact of what we are doing*?

One conceivable reason is quite simple and, in fact, simplistic. Starting out from Morris' statement that "people do not know what they are doing" we

281 Morris, Ian. 2010. Why the West Rules – For Now. The Patterns of History, and What They Reveal About the Future. New York: Farrar, Straus and Giroux.
282 Ibid. 28.

might wrongly imply that they cannot know. And from here it is only a short step to concluding –and that would be wrong again – that we cannot influence technology anyway, hence we can stop thinking about it. Such a fatalistic view is as convenient as it is seriously flawed – it rejects any responsibility for the effects of technology and, at the same time, strips society of its active role in co-evolution and mutual adaptation.

But there is a serious deeper reason why we do not anticipate the results of what we are doing. Our thinking about emerging technologies is situated between two extreme poles: unrealistic expectations and a lack of imagination. The future thinker Roy Amara coined this concept in what is known as Amara's Law:

We tend to overestimate the effect of technology in the short run and underestimate the effect in the long run.[283]

In the short term, we focus on the intended purpose of a specific emerging technology, say, 3D- printing. As individual customers, we have a fairly clear idea of the benefits we expect from a specific application, for example, a personalised case for your mobile device. We tend to see the short-term advantages through this rather personal lens. Focussing on our individual immediate benefit, we tend to ignore the effort required to turn such a technology into a marketable product. Hence our short-term hopes are frequently disappointed, as exemplified in the technology hype-cycles identified by Gartner Consulting, especially in the IT-sector.

In the long term, we do not have specific expectations; we are happy as long as the immediate benefit is guaranteed and maintained. That means we

283 Amara, Roy; Boucher Wayne. 1977. The study of the future: an agenda for research. Washington D.C. National Science Foundation, ed.; Washington D.C.: General Post Office OCLC 3200105.

do not have an idea of, or even a feeling for the unintended purposes and the unforeseen applications that will evolve over time, as society gets more familiar with a technology area, and more creative in employing it. For example, the potential benefit of 3D-printing in building a whole new class of three-dimensional micro-electronic-devices does not initially cross our minds; hence they come to us as a surprise, exceeding our fairly low expectations.

Neither as individuals nor as society do we see the active role that society plays in 'influencing technology'; rather, our perspective remains limited to ourselves and our passive role of 'being influenced by technology'. This limited understanding leaves our thinking seriously incomplete, neglecting our own influence on the potential risks and benefits that the future evolution of technologies might bring about. Because we do not see society as an active player, we do not systematically seize the opportunities we have of shaping the future of technological developments, neither as customers nor as policy makers.

Dealing with unintended consequences

We do, however, try our best to deal with technologies and their undesired effects. Essentially, societies have developed two different risk management approaches: an *a priori* approach (mainly employed in Europe) and an *a posteriori* approach (for example, in the U.S.). These approaches have been designed and established to control the potentially undesirable effects of concrete products or services, i.e. specific applications of technology.

The *a priori* approach seeks to avoid potential risks. This *precautionary principle* is widely applied in the European Union. It demands evidence that a new product or service complies with existing regulations before that product or service enters the market. These regulations are intended to ensure that no harm arises for individual customers, society or the environment. This approach is preferred in a legal system that is based on

codified law; the main effort is invested in defining and applying the appropriate regulations.

The *a posteriori* approach accepts potential risks and deals with consequences as they arise. It assumes that any new product will be designed and delivered in such a way that harm to individuals, society, or the environment is effectively avoided.[284] In case damage arises and can be attributed to a specific product, the originator of that product is held liable and has to compensate for the damage. This approach is more easily pursued within a legal system based on case law; the main effort is invested in litigation.

Both approaches share a common precondition that is essential for our discussion: they assume that there is a clearly identifiable legal entity (a natural or a legal person) that owns the product in question. With ownership, there usually is a clear economic interest to gain or keep market access. On that basis, the legal entity is either obliged to prove the product's compliance with existing regulations or held liable for any damage arising. As long as the expected economic gain generated by the product outweighs the cost for compliance testing (or the compensation for potential damage), both approaches have demonstrated reasonable effectiveness in dealing with the undesirable effects of specific technological applications.

But we have to ask ourselves honestly, whether they will still be appropriate, or even applicable, in the future. And we have to be aware that the approaches themselves are difficult to change. They both exist within legal and institutional frameworks that have developed over centuries; these frameworks exist, because societies have invested considerable time and

[284] Ulf Ehlert, Rethinking trust – in technology, 23 Oct 2017, https://understandinginnovation.blog/2017/10/23/rethinking-trust-in-technology/, accessed 6 December 2017.

resources in their creation and maintenance. Therefore, and regardless of the significant philosophical differences, no society can easily afford to adapt its approach or to adopt an alternative approach.

Instruments of the past

In recent years, the nature of public discussion on the impact of technology has evolved. Today, we are observing considerable controversy over the potential risks emanating from genetically engineered food, stem cell therapy, or artificial intelligence. It is only natural that a part of this debate calls for some control of these technology areas in order to avoid or at least minimise potential damage. And it is equally natural that societies should turn to the risk management approaches that they have already in place.

But this time we are facing a fundamental challenge: both the *a-priori* approach and the *a-posteriori* approach are designed to control specific applications of technology, whereas current discussions address entire field of technology, **calling into question the very applicability of either approach**. Both approaches are built upon the fundamental assumption of a legal entity that owns the technology in question. While this is true for concrete products, the situation for a technology area is less clear.

A technology area is not defined in a specific manner; it has no fixed scope, which is just a logical consequence of its emerging character. Furthermore, a technology area does not have a concrete owner either; rather, ownership is implicitly shared by many stakeholders of diverse backgrounds and interests, including academia, research establishments, industry, and the general public. Finally, and again due to the emerging nature, the concrete outcome of a novel technology area, for good or for bad, is yet unknown. For all these reasons, the legal preconditions for the application of either approach to any technology area are difficult to fulfil. This implies that our available risk management tools are too blunt an instrument to exercise

control over technology areas. They cannot be effective in dealing with them and are instruments of the past, not the future.

You might want to consider **a little thought experiment: What if** we insisted on employing those tools anyway? Under the *a-priori* approach, the lack of clearly defined products and outcomes of a technology area means that it is practically impossible to deliver positive evidence of any technology area's compliance with existing regulations. Rigid application of this approach would therefore necessarily lead to a complete ban on any further research and development in a specific technology area. Under the *a-posteriori* approach, the lack of a clear owner of the technology area poses a challenge regarding potential litigation: who is actually to be held liable? Furthermore, the emerging nature of technology areas implies that the dimension of potential future damage is yet unknown: even if we know the originator, that legal entity might be too small to compensate for the entire harm done, leaving much of the incurred cost to society.

This means **we cannot exercise effective control over technology areas** through the established risk management approaches. In fact, we are between a rock and a hard place: we could either strangle the evolution of an entire technology area or implicitly accept considerable risk and nationalise the cost of damage repair.

Of course we might consider that such discussions on the potential impact of emerging technology areas are only a temporary trend. But is that plausible? Will such discussions simply go away? Or is the contrary more likely? Are we going to see more discussions on technology areas and their impact on society?

The emerging dilemma of "Could we?" and "Should we?"

Humankind has progressed beyond the point where we can now cause serious damage to our own future; either physically, directly jeopardising

our existence; or metaphysically, potentially changing what it means to be human. Just consider nuclear fission, artificial intelligence or converging technologies. It is therefore highly likely that discussions on those (and other) technology areas will continue and even gain in intensity.

These debates will be difficult and controversial, and they will force us to thoroughly consider what we think responsible science in the 21st century should be like. Of course, the freedom of science from political interference remains the guiding principle that we hold dear. Within this principle we will continue to apply ethical constraints on the methods employed for acquiring new knowledge. Beyond the question of '*how we do science'* there is, however, a higher challenge looming, regarding the question '*what we do with science'*: the question of responsibility for the long-term outcomes of scientific research and for emerging technologies. So far, mankind was able to evade this question for several reasons.

Increasing means, maturing awareness

In the past, we did not have the means to directly harm our existence; neither intentionally nor unintentionally. And we were unaware of the detrimental long-term effects of our technological prowess. This explains the unbridled optimism up to the beginning of the 20th century; the blind faith in the progress that science and technology would inevitably bring about. Regardless of our achievements since the Industrial Revolution, we neither had the means for nor an awareness of serious destruction.

In the first half of the 20th century, we learned about the power of the atom and developed means to employ nuclear fission. For the first time, we had created a tool that could potentially destroy our existence. And we soon became aware of that potential. We suddenly had a means that could bring about serious destruction. Yet, we considered that means to be exceptional and did not change our thinking.

Towards the end of the 20th century, we gained a broader understanding of our impact on the planet, and the extent to which we had been jeopardising our own livelihood. That was only a slow realisation in hindsight, as unintended consequences of past actions became more and more visible (think about pollution, depletion of resources, shrinking biodiversity or climate change).[285] With that realisation our awareness of unintended means of destruction kept growing.

Nowadays, we are trying to think about the potential impact of scientific research, in well-meaning efforts to pre-empt negative consequences. In this endeavour, we seem to focus on the transition zone between basic and applied science, on emerging technologies that seem very promising in view of future benefits, while their concrete shape is still in the making. Take artificial intelligence or genetic engineering as prominent examples, which are currently subject to controversial public debate: both have the potential to change the psychological, physiological, or even moral meaning of the word 'human', for good or for bad. The result of these emerging technologies is in no way predetermined or certain. Yet, fully aware of this uncertainty, it is still plausible that these technologies could become new means of destruction.

Whether we like it or not: mankind has lost the innocence of ignorance, and instead gained access to potentially destructive means. With maturing awareness and increasing means, today we can neither deny nor reject responsibility; the responsibility for the intended and unintended outcomes of scientific research.

[285] Ulf Ehlert, On the freedom and responsibility of science, 26 May 2016, https://understandinginnovation.blog/2016/05/26/on-the-freedom-and-responsibility-of-science/, accessed 6 December 2017.

This leads to the fundamental question I believe our generation needs to address: **What is responsible science in the 21st century?**

In the past, we only used one simple question to guide all our scientific research: "**Could we?"** That is a question of mere feasibility: Could we understand, learn, know? And further on towards technology development: Could we do something with that knowledge? Since the Scientific and the Industrial Revolutions, science and technology have been the art of the possible: we did what we could.

However, given the means available to humankind in the 21st century, feasibility alone is not a sufficient guideline. Rather, we must complement feasibility with desirability to guide our research. We must add the questions **"Should we?"**, "Should we know this?" and, further down the road, "Should we do this?." And if the answer is "no" for some specific research, we have to be very careful how and where to impose constraints: on the basic science in general? Or, more specifically, on concrete applications resulting from technological research? These are the difficult choices we have to (learn how to) make.

The questions "Could-we?" and "Should-we?" pose a real dilemma: how to avoid undesired consequences of scientific research without strangling the much sought-after benefits? This is a serious and still unanswered question, and I will not claim to have a definitive answer. The only certainty I can offer is this: radical approaches will not solve the problem. While a full ban of scientific research would mean the end of human progress, a *laissez-faire* attitude might lead to self-destruction. **Neither panic nor hype offer sound advice**. We will have to make smart choices to find the golden mean between the 'do-nothing' and the 'do-anything'.

The current development seems to go from an *'unknown known'* to an at least *'known unknown'* dilemma. That means some progress, but knowing is not yet solving. We must realise that this is neither a superfluous question, nor one that we can postpone until later. Our available tools are ineffective, while the demand for appropriate policy is growing on two fronts: regarding specific technology as well as policy on science and entrepreneurship in general. So we have to speed up our efforts, and we have to break new ground at the same time.

Much in line with Alvin Toffler's famous words:

The future always comes too fast,
and in the wrong order.[286]

Outlook

Who owns the problem? Who owns the solution? There are no simple answers.

Converging technologies hold significant promises for future applications that could change and even disrupt that way we think about delivering military capabilities. It is therefore only natural that great efforts are being made to extend the art of the possible and at the same time to investigate the potential impacts of such technologies. In the defence and security context, NATO serves as a consultation- and collaboration forum for like-minded Nations to leverage their individual investments and to jointly push the envelope of emerging technologies.

But converging technologies are not simply a technological challenge that can be mastered. They also pose fundamental questions about the ethical

[286] Toffler, Alvin. 1970. Future Shock. New York. Random House.

desirability of some of the conceivable applications of these technologies. These questions are not limited to military applications, nor do they stop at national borders: these questions cut across many government departments, and they are likely to affect humanity in its entirety.

The underlying dilemma then is one of policymaking regarding emerging technologies in general, with converging technologies serving as a current and very prominent example. Previous approaches to policymaking and risk management have turned out to be either too limited (ineffective control of negative impacts) or too limiting (unduly constraining positive impacts). More importantly, these approaches were essentially static and it has not been possible to alter or adjust them over time. For the future, it will be critical to develop dynamic policies that can be modified as we learn more about the real impact of an emerging technology.

In order to achieve such dynamic policymaking we must overcome two interrelated challenges: first, we must develop dynamic risk-management approaches. Such approaches would evolve over time, and today's decisions might be corrected or even revoked in the future at marginal cost. In this way, we do not attempt a perfect, yet unrealistic guess; we rather take a pragmatic and cautious step-by-step approach. Second, in order to understand when changes are necessary and what those changes should be, we need to engage in a whole-of-society-discourse. **This discourse must engage scientists, politicians, and citizens**. And it needs to take place for every emerging technology, including the specific case of converging technologies.

Such discourse cannot be confined to defence applications only, nor can it be focused on NATO alone. Rather, such discourse must reach out across societies, across nations, and across international organisations. Therefore, a truly international effort is indispensable, engaging governments and non-governmental organisations alike. What we really need is a novel way of thinking international policymaking, beyond and across all traditional

compartments. Given our ever-increasing means, it is high time for such a genuine breakthrough in our way of dealing with technology.

7 Outlook

Complexity, Systemic Risks and Converging Technologies[287]

Herbert Saurugg

This chapter will address *Complexity, Systemic Risks and Converging Technologies* from a different point of view to raise awareness regarding possible challenges in connection with Converging Technologies that might not currently be in the focus of security considerations.

Network Centric Warfare

I would like to start my considerations by looking back 15 years, when Network Centric Warfare (NCW) was also a big topic in the Austrian Armed Forces. The discussion centred around the question how to improve military capabilities with new technologies and the possibility to connect sensors, command and control systems and actors in a much better way than we could ever have done before.

What really happened

Not particularly to the Austrian Armed Forces, because we were luckily not engaged in major military conflicts. But let us take the US Armed Forces as an example, which were the major driving force behind Network Centric Warfare. In fact they were really successful by using this concept in military

[287] This article originally was written in 2016 as a contribution to this book, but was published in a slightly altered version on a later date in a blog http://www.herbert.saurugg.net/2016/blog/vernetzung-und-komplexitaet/complexity-systemic-risks-and-converging-technologies, accessed on 11 December 2017.

operations, such as in Iraq or in Afghanistan, at least at the beginning of these wars. But was this sustainable as well? Not really. The high-tech forces, especially the supply chains, were successfully targeted by enemy forces which caused major casualties and cost an enormous amount of money. This was done by simple but highly sophisticated low-cost techniques, like, for example, using mobile phones to build efficient roadside bombs. The so-called Islamic State succeeded in establishing itself and spreading, within a very short time, over a very large area; they did so by, amongst others, using modern technologies, like Social Media to recruit followers and broadcast propaganda. Moreover, mass migration from the former war theatres started, which also preoccupied the Austrian Armed Forces, but in a completely different way than we had thought before. So the primary military operations were very successful because of the use of new technologies and the concept of Network Centric Warfare, but it was not possible to bring peace and democracy to these countries, which had been the official reason for deploying military forces there.

The missing holistic approach and view

So my conclusion is that our preparations for Network Centric Warfare were important but were insufficient with regard to the overall topic. The focus had mainly been on hard military targets – which is the main task of military forces – but disregarded other major developments. And it had been assumed that enemy forces were not connected or not using systems similar to those of friendly forces. Looking back this was short-sighted and a wrong conclusion.

The focus had been on hard military targets but in reality, the enemy was weak and poorly organised, as we assume enemy forces to be. This current enemy is using new civil technologies with capabilities that the armed forces were dreaming of fifteen years ago, and still are. Everybody can communicate wirelessly worldwide by using GPS – originally a military system – to beat high-tech military forces that are always equipped with the

latest maps from all over the world; all this does not cost much money and it fits in everybody's pocket. We have missed the fast technological improvement in the civilian area, which has also led to the possibility of hitting military forces hard with less effort.

Mindfulness

If we had considered Moore's Law or exponential growth as described by John Casti in this book, we would have been more mindful and aware of possible developments. This should also be a major lesson learned for the future. Therefore, both of these chapters dealing with off-topic considerations at the first glance, are so important for addressing possible future developments in the sector of Converging Technologies, even if we will still not be able to predict the future. But if one knows how complexity works and which challenges are connected to it, one will be able to handle these developments in a better way.[288]

Have we learnt the right lessons?

Back to Network Centric Warfare. We still have to ask if we have learnt the right lessons from the past within the Security Sector, especially in the armed forces. Are we not still focusing on air strikes for hitting enemy forces that are mainly diffuse, asymmetric force, not organised as during the Cold War? Are our achievements really clear and are we aware of the collateral damage? Has this led to policy changes regarding the armed forces or in general? Has this changed anything in our military planning?

[288] Saurugg, Herbert. 2016. Compexity, Systemic Risks and Converging Technologies. In: http://www.herbert.saurugg.net/2016/blog/vernetzung-und-komplexitaet/complexity-systemic-risks-and-converging-technologies, accessed on 6 December 2017.

As we have already learnt, the main driving force for the developments mentioned was – and is – interconnectivity by easily available ICT (information and communication technology) and, therefore, the amount of available information. So the question is "Do we now have the capabilities to control information of hostile forces?", "Can we disrupt their information flow?", "Do we know what is going on?", and "Can we stop virtual support?" Not really. Even if the drone war of the US Forces is based on information gathering and the tracking of digital traces. But most other security forces do not have these capabilities.

Even if we handle this topic very carefully, these capabilities could also be misused (unintended side effects). However, we will not be successful by merely focussing on hard military targets and on solutions that were successful in the past. We also do not want mass surveillance, as for example, performed by NSA. The question is whether we really need this on a very large scale or whether it could also work on a small, focused scale, as described by the concept of Electronic Warfare. We should not throw the baby out with the bath water. So broader discussion and transparent decisions will be needed to answer these questions.[289]

Times of VUCA

This is also a good example for the fact that we live in so-called VUCA times', the acronym for volatility, uncertainty, complexity and ambiguity, which is directly connected to the increasing complexity caused by the ongoing man-made interconnectivity between everything. In particular, we are not used to dealing with ambiguity.[290]

[289] Ibid.
[290] Ibid

Transformation to Network Society

During the Industrial Age we had simple structures and clear hierarchies that worked very well most of the time. The ongoing transformation to the Network Age or Society will fundamentally change our life and societies. Considering ongoing developments, it is dangerous to be guided by the knowledge and experience of former times, even if past solutions were successful then.

One major challenge will be that the structures and thinking of the Industrial Age will not completely disappear; however, they will be increasingly losing in influence and importance. This will enhance the complexity as well as the challenges for those who have to keep up with the developments.

But where is the link to Converging Technologies now?

It is the transformation to a Network Society and the digitisation process that also leads to Converging Technologies and Emerging Risks. On the one hand, these developments lead to fast and far-reaching improvements and, on the other hand, this entails completely new challenges and risks including for the security sector. In our culture we are used to an *either-or way of thinking*, which will no longer enable us to tackle future developments in the right way. It may have worked more or less with the simple structures at the time of the Industrial Age, but it will not in complex Network Age structures. Therefore, we will need an 'as-well-as' way of thinking, in order to address reality and ambiguity as we can see it already on an almost daily basis. Other statements and points of view may sound easier and provide short and clear answers; however, in a complex environment they are often false and harmful in the long term perspective, considering, for example, the populist tendencies of our times. Populists have short and very simple answers to many unanswered questions, and

people believe them, even though we already know that they will not function and are dangerous for our societies.

Systemic risks

This will be similar developments in, and reactions to Converging Technologies. We often try to address new possible risks with methods that were successful in the past, which, however, can hardly tackle the increasing interconnectivity and complexity. So the rise of systemic risks is hardly noticed. Systemic risks are characterised by a high degree of interconnectivity and interdependence and missing range limitation. Cascading effects are possible. Because of the complexity and feedback loops, there are no simple cause-and-effect chains and the triggers as well as the impact are systematically underestimated by the responsible persons and organisations.

From my point of view, the most dangerous short-term systemic risk is contained within the Europe-wide electrical power system. If this system failed, the effects could have major cascading and disruptive effects on the entire European society. Also the Network Centric Warfare example showed developments that were underestimated. Therefore, systemic risks are the root of X-Events, which John Casti described in this book.

What does complexity mean?[291]

Complexity is already a part of everyday language use, even if different meanings are often associated with it, such as opacity, uncertainty, dynamic, and so on. To address complexity in a very short way, it can be also described by some typical characteristics:

[291] Cg. Ibd.

- Changing system properties because of feedback-loops, and therefore the possibility of emerging new system properties. For example, oxygen and hydrogen are flammable gases; those two elements combined with aqua lead to a liquid that disguises a fire. Even if we knew the nature of the gases, we would not be able to foresee the nature of the new element.
- This also causes non-linearity, where our approved risk-management systems inevitably fail and predictions are difficult or impossible. They may work, as usually, work for a time, but within one moment the system's behaviour could change completely.
- Interconnectivity leads to an increasing dynamic (faster and faster …) because the possibilities with regard to the system's behaviour are increasing.
- This also leads to irreversibility (no way back) and the impossibility of reconstructing the causes or restarting at a well-known point. Take a creature as an example of a complex system: you cannot cut creatures into well-structured pieces, analyse them and put them together again. It will not work as will not for all complex (living) systems. This only works with complicated (inanimate) systems (machines).
- Another very well-known characteristic is that small causes could lead to large effects ('butterfly effect'). A minor problem in the link of a supply chain could bring down the whole system/production, as we have seen recently.
- Yet another characteristic that is often underestimated are delayed and long-term effects. Especially in our very short-term oriented economy. The figures are related to quartiles. We know that apparent short-term solutions often have a negative impact on a long-term view and that long-term success often requires the acceptance of short-term disadvantages. Take asbestos as an example of long-term effects. For years it had been considered a miracle material with great qualities, until people learned that it has

negative long-term side-effects and causes cancer. Now it has to be removed in compliance with high safety requirements and at high cost. Imagine what this could mean in terms of GN-technologies. It will not be possible to remove this parts because of the size of the material. As described by John Casti, an X-Event could be the consequence.

What challenges are we facing?

First, we have to know that in nature there are only complex, open systems. But they are new on a technical level, especially the increasing interdependences (vulnerabilities). We are still used to dealing with linear simple machines instead of complexity, mainly due to a lack of education and training. Especially in the education system we often still train and teach in a way that was appropriate for the Industrial Age, which is hardly what is needed in the upcoming Network Age; thinking in black and white is too simple.

Lack of knowledge and systemic thinking

There are of course improvements but, in general, they cannot keep up with the fast technological developments. Even though there are people who have the necessary knowledge to develop these emerging and converting technologies, most of them do not, including those who should, for example people working for public authorities or regulatory bodies who protect public interests. In particular, administrative bodies are often still organised according to old hierarchical structures that are hardly able to cope with quickly changing 'VUCA developments'. Not to mention that often interconnected special knowledge and fast reaction is needed. Today nobody is able to know everything anymore and therefore we have to arrange more flexible ad-hoc networks and interaction among different experts in order to address complex dynamic challenges. We are increasingly establishing and improving interconnections between technical

systems, but the necessary interconnection between people and organisations to cope with unintended side effects is lagging behind. This leads to gaps due to complexity, which implicate systemic risks and danger of X-events!

Cyberspace

I would like to give you another example. Are we prepared for the challenges connected to Cyberspace? At the moment we are mainly focusing on cybercrime and data theft. But this is just the beginning. We should be much more aware and worried about our Critical Infrastructures (CI). Yes, we have established Critical Infrastructure Protection, Cyber Security and Cyber Defence. But protection is not enough because perfect security does not exist anywhere.

Therefore, we have to rethink our system design, because the way we have organised not only our infrastructure but also our reaction capabilities is not appropriate for handling X-events. We are not prepared for dealing with major disruptions in our infrastructure either. And with the increasing interconnectivity and interdependence, especially within our infrastructures, the danger of far-reaching X-Events is growing.

We still have different 'silos' from those we had in the past. So we have a Critical Infrastructure Protection and Cyber Security where the police is responsible. Military forces should be responsible for Cyber Defence. But if Cyber Security fails and cascading effects bring down infrastructures, there will be no second line of defence where Cyber Defence could be successful. The only task will be to clean up the mess on a very basic level.

So what does this mean in the context of Converging Technologies?

The main question is "What are we talking about? Are we talking about possible military developments, which are of course there, but mainly concentrated on a small scale, like Network Centric Warfare?"

Or should we focus more on possible other realities that should concern us more, as they are relevant for the security sector and the society? For example, on drones over Critical Infrastructures that could lead to major cascading effects, or drones that hit aeroplanes and bring them down; or already existing biological invaders that could lead to an environmental collapse? And how much more easily could this happen if GNR-technologies are used? Therefore, we have to recall complexity and some of its characteristics: small causes, large effects, delay/long-term effects, irreversibility, increasing dynamic and so on.

Possible consequences for the security sector

The main question is "Who is responsible?" However, it remains unanswered because there has been no major event until now. But this is not a good way of dealing with uncertainty. Military forces are principally qualified to think ahead and to address security-related developments before they escalate.

This requires us to be vigilant, to have early warning systems and to be attentive with regard to weak signals because developments always follow an s-curve: very slowly and on a low level at the beginning. But at one point, the development increases in an exponential way, and soon a critical point will be reached with no way back. If the weak signals are neglected, you can hardly follow the developments. And we really have a poor understanding of exponential developments.

The only chance to keep up with 'VUCA developments' and GNR is to stay flexible and agile and not to resort to former military core skills. The challenges will not come only from the known side or the enemy. Therefore, we need an 'as-well-as' way of thinking: we require both and we need to look at both sides of the coin. So the security sector will be confronted with an increasing number of requirements.

Of course, the question remains "Who is responsible now?" Nobody and everybody. These topics are new to our society and therefore a new way of thinking and acting will be called for. Less than we did until now because an increasing technical connectivity also needs a way of thinking that takes into account the interconnectedness of systems, not only in the military forces but also within the whole security sector.

Learning from nature: 'Small is beautiful'

Therefore, we should also learn more from nature, which can look back to a very long history and development. Only successful structures have survived. We often neglect the so-called 'silent witnesses', those who did not survive and cannot be found in history books. One major structure that succeeded is 'small is beautiful'.

- Small structures are more flexible and robust against strokes (asymmetry).
- People are more resilient in small structures.
- You cannot prevent the development, but early warning is an important part of navigation and we have to prepare to cope with uncertainty and with major incidents/disruptions (X-events).
- It is all about communication and knowledge. If people and decision-makers know the challenges, they can react to, and prepare for crisis/disruption or change the path.

- Communication in the security area will be a main driving force in increasing people's resilience and their capability to act in case of uncertainty and after X-Events.
- Understanding the problem is half of the solution.

So we are moving on a very narrow path. The border line between benefits and risks is very thin. One main question therefore is "Are we mature enough?"

The good news at the end:

- Near future X-Events will most likely not be triggered by GNR – even if we cannot give a guarantee.
- But we should consider major temporary infrastructure collapses and social unrest, because there have been/are many weak signals which have been hardly noticed until now.
- We also have to be attentive to weak signals in other areas – like GNR.
- And we should learn more from history and transfer this knowledge into the future; although history never repeats itself, there are similarities we should search for.

This book will just be the start when it comes to increasing our increase awareness of new challenges for the security sector with respect to Converging Technologies and Emerging Risks.

Conclusion and Final Considerations

Anton Dengg

Technological knowledge is a determining factor in security policy. Once again, new technology is a double-edged sword. It has an impact on the culture of societies and states – in a good and a bad way.

As already mentioned in the introduction, *converging technology* is going to have a huge impact on future security policy. Robotic, nano- and biomaterial technology will change not just the entire field of technology but also the structure of conflicts. Therefore it is of utmost priority that society and states are aware of future trends and new challenges. Those societies who realize the need of resilience and can handle it will be able to withstand upcoming complex threat scenarios in a better way. Countermeasures can only be successful in a comprehensive approach of national and international partners and organizations, such as the United Nations, NATO or the European Union. International law is especially challenged because of blurred threat scenarios with an increasing number of different actors. Therefore, a common understanding of possible threat scenarios is an absolute necessity.

In a quickly changing world, where technological developments emerge tremendously fast and are combined with hybrid threats, we should particularly focus on the future complexity of security policy. A changing technology environment will also create a more complex infrastructure, implying that the emerging complexity cannot only be handled by humans. One possible solution for this problem is to rely on automated systems and artificial intelligence. But this leads us to a spiral of complexity, a higher dependence on technology, and thus, to increased vulnerability.

There are possible unwanted spill-over effects of new converging technologies nobody can foresee with the potential of getting out of

control.[292] A *black swan* event could have a huge impact on security policy. Converging technologies, as Herbert Saurugg mentions in his chapter, can hardly manage by using methods from the past because of the "[…] increasing interconnectivity and complexity"[293]. Therefore, an ongoing analytical process is a must-have for a responsible security policy. One prerequisite for such an analytical forum or cell is to have relevant experts in this field of research. Another pre-condition is the need for out-of-the-box thinkers as well as decision-makers who accept this unconventional approach.

A possible unwanted spill-over effect could include terrorists capable of using knowhow based on nano-, bio-, or information technology, using them for attacks. But this know-how can be acquired in many ways. It could also potentially be derived from sympathizers with subversive ideas. Filippa Lentzos, citing the World at Risk 2008[294], is convinced that there is less risk of terrorists becoming biologists than of biologists becoming terrorists. We should not forget that statement.

In recent years, extraordinarily increased investments in promising future technological research, especially in the field of biodefense have been observed.[295] More investments basically mean more money for research and experts. More experts imply a possible higher risk of proliferation because there is a higher chance of corruption.

---

[292] See article in this book from Norbert Frischauf, Converging Technologies and Emerging risks: What is the `sinister´ Potential of Nano-, Bio-, and Information Technology Products in the year 2025?

[293] See article in this book from Saurugg, Herbert, Complexity, Systemic Risks and Converging Technologies

[294] Department of Justice: Amerithrax Investigate Summary. Department of Justice, Washington, DC 19 February 2010.

[295] see article of Wolfgang Schallenberger, "Pandemic and Bioterrorist Threats – Risk Assessment", in this book, S. 79.

The fact that the "[c]urrent military investments in synthetic biology and neurobiology are significant"[296] underlines the potential of possible future challenges in the field of converging technological developments in this field.

There is an urgent need to widen our view on threats and security. Some researchers are convinced that converging technologies, especially nano-, bio-, and information technology, will have the same ground breaking effect on society as inventions, like the printing press, the steam engine or the Internet. Just to be clear, technology is not a threat in itself. The problem starts where humans misuse technological achievements and apply them as a weapon.

Due to the wide range of challenges the development of new converging technologies pose, risk assessment is an indispensable prerequisite in any national security policy.

Future and Technology

Future developments cannot be stopped and the rise of robotic is a good example. In future, robotics will have a wide range of functions in our daily life. But robotics will also have an increasing significance for security forces. There are different reasons. On the one hand, machines could reduce the threat for human security forces, which do not have to work in danger zones any more. Fewer casualties would lower the political risks for decision-makers. On the other hand, some experts are convinced that unemotional autonomous robots could take less incorrect decisions than an armed human being. But there are also many counter arguments, for example, that the reactions of unemotional robots could escalate violence

[296] see article of Filippa Lentzos, „Emerging Security Challenges in Biology", in this book, S. 99.

in conflict areas. The emotionality of a security guard would bring a human factor to the battlefield that would mean fewer victims. However, these considerations mean a lot of challenges for international law and their representatives.

Beside robotics, enormous potential is expected from science branches related to bio- and nanotechnologies. These two technological sectors will also have tremendous influence on robotic technology.

The development of biogenetic weapon systems is not anymore fiction. Genotype manipulations make the re-establishment of old and the development of new kind of viruses possible. This will lead to totally new risks. But the main challenge is not the development of new products but the knowledge of insiders and the misuse of dual-use products. Beginning with 2025, the developments in the field of nanotechnology will rise in an exponential manner. State contracts are currently the main driving force of research.

The European Commission recommends the following definition of nanomaterial: "'Nanomaterial' means a natural, incidental or manufactured material containing particles, in an unbound state or as an aggregate or as an agglomerate and where, for 50% or more of the particles in the number size distribution, one or more external dimensions is in the size range 1 nm-100 nm."[297] Because of potential security risks there is demand for a responsible behavior and a responsible handling of inventions in the field of nanotechnology. This technology will offer an unlimited potential of future applications from weather forecast and health care to new military

[297] European Commission. 2011. Commission Recommendation of 18 October 2011 on the definition of nanomaterial. Official Journal of the European Union (2011/696/EU), L 275/40, Brussels, 18 October 2011. In: http://ec.europa.eu/research/in dustrial_technologies/pdf/policy/commission-recommendation-on-the-definition-of-nanomater-18102011_en.pdf, accessed on 29 August 2017.

applications, for example, in camouflage. But nanotechnologies can also have negative and dangerous side effects to environment and organisms that realistically are difficult to assess. Asbestos can be taken as a warning example.

Achievements e.g. in the field of biotechnology, are accompanied by research in miniaturisation and robotics. Implications on security forces and their weapon systems are probable.

It is highly probable that nanotechnology will particularly influence the armed forces, a view also confirmed by General Hostage.[298] On the one hand, new products in the security forces can be used in an active way (e.g. weapon technologies) as well as in a passive (e.g. new personal protective equipment). This can influence conflicts positively and a negatively. Also, security forces have to react with the same new technological countermeasures as opponents.

The armed forces have big interest in not-lethal, neurobiological weapons systems. Apart from the U.S. Russia is conducting extensive research on this subject. In 2002, for example, Chechen separatists took 800 people hostage whereupon Russian security forces channeled chemical substances into the theater where the terrorists acted. As a consequence, terrorists and hostages fell unconscious. About 100 people died in this operation. Nevertheless, the risk of a bio-terrorist attack happening is very much overestimated and rather unrealistic due to the complexity and cost intensity, resulting from the production of 'useful' ingredients. Such an attack requires the support of a state actor.

---

[298] Mehta, Aron. 2014. Interview with General Michael Hostage, Commander US Air Force´s Air Combat Command.. In: Defense News. (http://www.defensenews.com/apps/pbcs.dll/article?AID=2014302030017 accessed on 8 April 2014).

Changing risk challenges have also arisen because of the easy access to, and the misuse of knowledge on the Internet. There is also a higher danger of misuse by so-called insiders because of the open access to knowledge and training.

The rise of missions of Internet-of-things components creates totally new vulnerabilities and risks that have been irrelevant until today. At international level there are several initiatives, e.g. bioethics commission or the *Convention on Human Rights and Biomedicine,* which deal with possible scenarios. Inside the United Nations, questions regarding definitions, on how to control new technologies and responsibilities they call for such means are debated extensively. However, geopolitical conditions and different point of views very often hamper efficient progress in finding solutions.

Bigger problems have to be expected especially from states and groups without ethical hesitations during operations that employ *Converging Technologies*. So far, there have been no universally accepted solutions for these specific challenges. But it is clear that an inter- and trans- disciplinary approach for risk monitoring and assessment is indispensable.

In May 2014, the outcomes of an informal expert meeting on Conventional Weapons (CCW) showed that the correlation between national and international law and the arising new forms of technology need to be considered. Awareness should be raised even in national and international security policy committees.[299] A comprehensive approach between national

[299] UN: Meeting of the High Contracting Parties the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. Report of the 2014 informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS); CCW/MSP/2014/3, 11 June 2014; https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/048/96/PDF/G1404896.pdf?OpenElement, retrieved 11 April 2017, p. 3

and international organisations is a prerequisite for reflecting on future challenges. Especially the dual-use character of many technological products can only be handled by international institutions, such as the United Nations, NATO, the European Union, or the OSCE.

Consequences for security forces

Technological change will not just affect the private sector but will also, in the long run, have an impact on the upcoming 'battlefield' in all its different dimensions (not only military). In the future, conflicts will have strongly blurred borders, if there are borders left. Combat fighters will be affected in the same way as strategists, with the goal to gain superiority in a future conflict zone.

The mentioned future fighters will be surrounded by a lot of technological equipment and artificial supporters: drones, direct artificial support e.g. exoskeletons and camouflage devices to perform first-aid activities. These converging robotic systems will force the adversary to use anti-robotic systems for defense.

All the above mentioned information will especially challenge strategic thinkers in several ways:

- Long-term estimations regarding future developments can hardly be made. Experts recommend a future outlook of no longer than 5 to 8 years concerning converging technologies, due to their complexity and unpredictability.
- International organisations are required to closely cooperate in all spectra of converging technologies.
- One of the main questions is whether we can handle the complexity that already exists. If the answer is no, the question arises of how tomorrow's complexity can be handled and reduced.

- There is the need for an unorthodox and innovative planning group composed of interdisciplinary experts dealing with security policy issues.
- Procurement agencies of security forces have to have a clear picture of how threat scenarios of at least the next ten years will look like. If they open a procurement transaction for the equipment of today's usual arms and applications, security forces will be outdated because of the old fashioned equipment. So the effect of security forces could be less effective against future adversaries. Converging technologies mean a better and of course a more qualified training of armed forces. That means procurement agencies of security forces have to cooperate their planning activities even more effectively than ever before.
- Because of sophisticated converging technologies the employment of high-profile employees with different qualifications is necessary. Higher qualified people mean much higher income for security forces and higher costs for employers.
- Lawyers will be an important asset within the early warning and reaction teams of future technological developments. Especially on the international level, will (the results and) consequences of technological progress have to be discussed. Blurred definitions will have to be clarified at a very early stage. Issues whose legal dimensions have to be spelt out are:
    - What instruments of defense against much better equipped adversaries violating international standards are legally acceptable? What if outdated international standards are not compatible with new technological developments?
    - Who is responsible for malfunctioning devices, especially in case of humans only assuming secondary function and the actual action being carried out by a robot (e.g. the state that bought the device, the security organization owing the

technology, the people 'pressed the button', the company that sold the vehicle, the software engineers etc.)?

- How can human use of robots, microrobots and other such equipment be regulated if the boundaries between human capabilities and robotic capacities are blurred (e.g. if technical devices enhance soldiers' capabilities)? Where is a boundary between a human being and a robot? For example, if soldiers are surrounded by technological equipment, as for instance in the movie *Robocop,* is it necessary to distinguish between human beings and robots?
- Should robots be allowed to kill a human being? That would include software with detailed If-Then-Routines. What consequences would software bugs have for victims? Should self-defence have the same legal consequences for robots as for humans?
- Can Isaac Asimov's Law of Robotics[300] become international law?
- Should there be a ban on the proliferation of technological knowhow and devices? For whom? Who decides?

• Security forces must think in a more open, intellectual and creative way to be able to handle future challenges.

---

[300] Asimov's Three Laws are the following:

- A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.
- A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

Salage Christoph: Asimov's Laws Won't Stop Robots from Harming Humans, So we've Developed a Better Solution. The Conversations US on 11th July 2017. https://www.scientificamerican.com/article/asimovs-laws-wont-stop-robots-from-harming-humans-so-weve-developed-a-better-solution/ accessed 25 August 2017.

- The continuous development of scenarios concerning the future scope of new converging technologies is a prerequisite for security forces. Clear visions for new developments enable preparation and the adaptation of equipment as well as training methods of security forces. Procurement procedures also take about one decade to be effective. If the signs regarding future developments are ignored, the wrong instruments for counterstrategies will be available in ten years.

This offers at least three challenges for an efficient counterstrategy and prevention:

- If there threats exist from security forces using such progressive technological, they need to be countered by similar techniques. A new competition between actors in a conflict possibly leads to a spiral of violence.
- Threats do not always coming from adversaries. We should be aware of a much bigger threat coming from sympathizers. They could be employees of, for example, security forces or experts who potentially offer their knowledge and capabilities to criminal or terrorist organisations via the Internet. Examples from the recent past, where soldiers were involved in terrorist acts, confirm this thesis. 'Dual-use research' is, therefore, an indispensable for an effective countering of threats.
- There is always the danger of proliferation of high-tech devices and specialist knowledge.

Possible approaches to avoid and counter the potential misuse of converging technologies:

- Currently, states are hardly prepared against these new forms of threats. Therefore, awareness regarding these threats has to be raised. Measures have to be taken to enhance resilience in the society as a whole and its capacity of handling unexpected X-events. This is not only a task of security forces but the responsibility of States.
- By 2040, the convergence between nanotechnology and robotic will have massively increased the challenges linked to it. This requires the development of new measures of conflict prevention with regard to system risks.
- Experts consider cryptography as a useful answer to global cyber threats.
- Restricting the research on converging technologies to reduce the risk of misuse will have limited effect since nearly all technologies involve a misuse factor.
- Raising awareness among researchers as well as with security forces and civil servants seems to be more promising. Additionally, there is the need to foster cooperation between different actors through confidence-building measures.

Technologies will change not just security forces; they will influence and challenge societies and their way of life. This calls for a comprehensive approach in elaborating countermeasures with regard to developments in converging technologies. Raising awareness for future challenges is the first step.

Authors

Dr Anton Dengg

Senior Researcher at the Institute for Peace Support and Conflict Management, National Defence Academy Austria

Colonel Dr. Anton Dengg has been working as a research fellow at the Institute of Peace Support and Conflict Management (IFK) of the Austrian National Defence Academy since 2004. From 2011 – 2013 Mr. Dengg served as Adviser on Anti-Terrorism Issues at the OSCE Transnational Threat Department/Action against Terrorism Unit. Since March 2013 Col. Dengg has been serving again in the IFK. Mr. Dengg has been awarded a doctorate in Political Science at the University of Vienna in 2017. His main focus is on Terrorism Issues, Critical Infrastructure Protection, Hybrid Threats and New Technological Challenges.

Michael B. Janisch MA.

Director Armaments and Defence Technology Agency

1979-1983 basic officers' training. Followed by duties as training officer, platoon- and company commander with tank battalions 10 and 33. 1988-1991 command and general staff course at the National Defence Academy in Vienna. 1991/2 post-grade studies at the Graduate Institute of Geneva University, Switzerland. 1992-1999 various functions in the area of arms control, confidence building and military policy within the military policy division at the MoD including functions at the Austrian Missions to the UN in Geneva, the OPCW in The Hague and the OSCE in Vienna. 1995 staff familiarization with HQ IFOR in Bosnia-Hercegovina and secondment to the Military Strategy Division of the German MoD in Bonn. Chief of staff and deputy commander of the 3rd Infantry Brigade during their activation periods 1995-1998. 1999-2001 Senior Military

Adviser to the Austrian Ambassador to NATO in Brussels, Belgium. 2001-2002 Chief of staff and deputy commander of the 4th Mechanised Brigade incl. NATO/PfP Exercise Strong Resolve in Poland. 2003 Austrian National Contingent Commander in Kosovo and Deputy Chief of Staff of Multinational Brigade South-West in KFOR. 2004-2006 responsible planning officer for training requirements and Air Force training concepts at the MoD. In parallel also project team leader and finally commander of the enabling staff of the new Austrian Air Force School. From 2007 to 2011 Austrian Defence Attaché to the Nordic and Baltic countries. 2011 deputy head of the Organizational Division of the MoD. Since 2012 Director of the Armaments and Defence Technology Agency and promotion to BG.

Michael Janisch holds a masters' degree of the University of Vienna, a certificate in Security Policy from the University of Geneva and owns Commander's Crosses of the Norwegian Order of Merit and the Swedish Polarstar Order as well as the NATO Non-Article 5 and the Italian Per La Pace medals.

Prof. Dr. John L. Casti

Director of the X-Center, Vienna

Dr. Casti received his Ph.D. in mathematics at the University of Southern California. He worked at the RAND Corporation in Santa Monica, CA, and served as a profesor at Princeton and New York University in the USA before becoming one of the first members of the research staff at the International Institute for Applied Systems Analysis (IIASA) in Vienna, Austria. He has also been on the faculty of the Technical University of Vienna and the Santa Fe Institute in the USA.

He has published eight technical monographs in the area of system theory and mathematical modeling, as well as 12 volumes of popular science,

including *Paradigms Lost, Complexification, Would-Be Worlds, The Cambridge Quintet, and Mood Matters*. His 2012 book, *XEVENTS* addresses the role complexity overload plays in the creation of potentially life-changing events such as the crash of the Internet or the outbreak of a global pandemic.

Dr. Casti is currently Director of The X-Center, a private research institute in Vienna focusing on the development of tools for anticipation of extreme events in human society. He is also a Senior Research Fellow at the Center for Complex Systems and Enterprise at the Stevens Institute of Technology in New York.

In early 2016, Dr. Casti received the Medal of Honor for meritorious service to the city of Vienna.

Dr. Johannes Rath

International Biosafety and Security Advisor (EU,UN); Head DNA Laboratory - Department Integrative Zoology, University of Vienna

Dr Rath has been engaged in CBRN security for almost 20 years. He served as Chief Inspector to the United Nations Special Commission (UNSCOM) and Inspector to the United Nation Monitoring and Verification Commission (UNMOVIC) in Iraq.

Dr. Norbert Frischauf

R&D and hi-tech Partner at SpaceTec Partners

Norbert Frischauf studied Technical Physics at the Technical University in Vienna and Electrical Engineering at the Technical University in Graz (Austria). Following his specialization on high energy physics he moved to CERN in Geneva (Switzerland) to work on two particle detectors in the DELPHI Experiment of the Large Electron Positron Collider (LEP).

After having spent some years at CERN, his professional career led him to the European Science and Technology Centre (ESTEC) of the European Space Agency (ESA) in Noordwijk (Netherlands), where he worked as future studies systems engineer and expert for emerging technologies. From 1999 to 2006, Dr. Frischauf was engaged with consultancy work for Booz Allen Hamilton, mostly focusing on aerospace, telecoms and hi-tech. After a professional detour into management with the start-up QASAR in Vienna, Dr. Frischauf returned to the Netherlands in the beginning of 2009, where he worked for three years as a scientific officer at the EC Joint Research Centre – Institute for Energy and Transport in the action for 'Hydrogen Safety in Storage and Transport', being responsible for scientific aspects of high pressure hydrogen storage activities and further technical developments.

As of 2012 Dr. Frischauf is a partner at SpaceTec Partners a unique boutique consultancy providing strategy and technology consulting, communication activities and interdisciplinary project management mainly for the European Commission, ESA and leading industries. Being the 'R&D and hi-tech partner', Dr. Frischauf´s role within the company involve: Strategy development, Science and technology competence, Experimental research, Networking, as well as Authoring and presenting.

Beside these scientific activities, Dr. Frischauf is a leading member in various associations (like the Austrian Space Forum, the Space Generation Advisory Council of the United Nations and the International Academy of Astronautics) and is active as science communicator, making science documentaries for the Austrian Broadcasting Corporation, Bayern Alpha, 3Sat and writing popular science articles in various magazines.

Dipl. Ing. Dr. techn. Wolfgang Schallenberger

Independent Consulting Firm, Vienna

Wolfgang Schallenberger obtained a degree in Chemistry and Biochemistry/Biotechnology at the University of Graz (Austria). He received his Ph.D. in 1982 in the field of Biotechnology. For 20 years he worked in the emerging biotech industry and is founder of the first Austrian biotechnology start up followed by two more companies, he acted as founder/CEO and CEO of different R&D focused companies. 2003 to 2012 he was partner in an investment company with mandates in biotechnology, medical devices and green energies. Since 2013, Wolfgang Schallenberger leads an independent consulting firm in Vienna, Austria, focusing on investment services for the life science industry. He is Member of the Science Advisory Committee to the Ministry of Defense and Officer (Miliz, Colonel) in the Austrian Army.

Dr. Filippa Lentzos

Senior Researcher King's College, London

Filippa Lentzos is an academic researcher focused on security and governance aspects of emerging technologies in the life sciences, particularly interested in contemporary and historical understandings of the threat of biological weapons, bioterrorism and the strategic use of infection in conflict.

Originally trained in human sciences, she switched to sociology for her doctoral work, and spent the first ten years of her career at the London School of Economics and Political Science (LSE), the United Kingdom's leading Social Science Research University with an unrivalled concentration of social, political, legal and economic expertise. In 2012, she joined King's College London as part of the team establishing the Department of Social

Science, Health & Medicine, a cutting-edge department carrying out leading research on some of the biggest global health challenges facing the world today.

Her work is theoretically driven, empirically informed and policy-relevant. It draws on a range of methods from participant observation, interviews and documentary analysis, to archival research, database searches and statistical analysis. She is committed to rigorous and responsible research that contributes to addressing the significant social, political and security challenges of developments in the life sciences. Responding to these challenges rarely involve simple, reductive or straightforward answers; and so she embraces interdisciplinary perspectives and learning, as well as collaborative research.

Em.o.Univ.-Prof. Ing. Dr.phil. Robert Trappl MBA

Head of the Austrian Research Institute for Artificial Intelligence, Vienna

Robert Trappl is head of the Austrian Research Institute for Artificial Intelligence in Vienna, founded in 1984. He was professor of Medical Cybernetics and Artificial Intelligence and head of the Department of Medical Cybernetics and Artificial Intelligence, University of Vienna, for thirty years, and is now professor emeritus at the Center for Brain Research, Medical University of Vienna. He holds a Ph.D. in psychology (minor: astronomy), a diploma in sociology (Institute for Advanced Studies, Vienna), is Ingenieur (BEng) for electrical engineering, and, in 2012, graduated as MBA in General Management. His main research interests have always been the human mind, cybernetics, systems research and artificial intelligence, AI not restricted to the so-called rational processes but encompassing also emotional ones. Besides these main research interests which led also to his cooperation in the Neurorobotics Sub-Project of the EC-sponsored Human Brain Project, he has been attempting to answer questions related to the application of artificial intelligence

methods e.g. how to develop rational and emotional personality agents for interactive media, how to develop robots that may aid persons with special needs, how to aid persons who want to prevent the outbreak of a war or to end one with artificial intelligence methods applied to conflict databases, etc.

He has published more than 180 articles, he is co-author, editor or co-editor of 35 books, among others 'A Construction Manual for Robots' Ethical Systems', Spinger, Cham, Switzerl, 2015.

He is Editor-in-Chief of 'Applied Artificial Intelligence: An International Journal' and 'Cybernetics and Systems: An International Journal', both published by Taylor & Francis, USA. He has been on the editorial board of numerous scientific journals and has been a member of program committees of many national and international conferences.

Dr. Markus Reisner

Major (GS), Institute for Higher Military Command and Control, Austrian National Defence Academy Vienna

1998-2002 Markus Reisner enrolled for officer training at the Theresian Military Academy. He was employed in various missions in Bosnia and Herzegovina, Kosovo, Afghanistan, Chad and Central African Republic since 2005. Mr. Reisner received his Ph.D. in History at the University of Vienna in 2013; 2013 to 2016 participation in the 20th General Staff Course at the Austrian National Defence Academy. Since 2016, he is teaching at the Austrian National Defence Academy and employed as a researcher. He started his Ph.D. studies in 'Interdisciplinary legal Studies' 2013 at the Law Faculty Vienna and is Fellow of the Vienna Doctoral Academy – 'Communicating the Law'. Currently his research focus is employment and future of unmanned armed systems. He published two books ('Bomben auf Wiener Neustadt' and 'Unter Rommels Kommando') and is working on a

publication about the 'Wiener Operation' – Viennese Operation of the Soviet Armed Forces of March/April 1945.

Univ.-Prof. Dr. Reinhard Posch

Scientific Director of A-SIT, Secure Information Technology Center Austria; CIO for the federal government of Austria

The role of the CIO for the federal government is primarily the strategic coordination of activities in the field of information and communications technology that concern more than one ministry. As such the CIO is the Chair of the Austrian eGovernment platform 'DIGITAL:AUSTRIA' that includes all level of government. As Head of the Institute he specialised in Applied Information Processing and Communications Technology and as scientific director of the Austrian Secure Information Technology Centre the main efforts are computer security, cryptography, secure hard- and software and eGovernment. He is chairman of the board of trustees of the non-profit foundation Secure Information and Communication Technologies SIC which has been donated by Graz University of Technology. Reinhard Posch was also Chair of the Board of ENISA, the European Network and Security Agency. Reinhard Posch takes part in groups installed by the European Commission to elaborate ICT and security strategies (e.g. 'Future Internet Visionaries', RISEPTIS). Being a member of the 'Rat der IT Weisen' he is providing advice to the Commissioners Kroes and Sefkovic in the area of IT- security to assist the implementation of the Digital Agenda. Reinhard Posch got awarded the Grand Decoration of Honour in Silver for Services to the Republic of Austria.

Dr. René Fries

Consultant and Researcher at the Institute for Technology Assessment of the Austrian Academy of Sciences

René Fries studied experimental physics at the University of Hamburg; he received his doctorate in 1978. He was employed for several years as Research Associate at Northwestern University at Evanston near Chicago, and later at Indiana University and the Argonne National Laboratories in Illinois. He was member of an international collaboration in high-energy physics experiment - the 'free quark search' - at the SLAC research facility at Stanford in California. 1983 he started to work as researcher at the Laboratory for High Energy Physics of the École Poly-technique in Palaiseau near Paris and the CNRS - Centre National de la Récherche Scientifique. 1985 he started to work as administrator and scientific counsellor for the Ministry for Science and Research in Vienna. He developed research-promotion activities for micro-electronics, information technology, and nanotechnology. For more than ten years he was delegate at the OECD working group for information technology and communications policy in Paris. He left the public service in 2003 and works as a consultant and researcher at the Institute for Technology Assessment of the Austrian Academy of Sciences since. He has been advisor for members of the Austrian Parliament and for the Chairwoman of the Parliamentary Commission on Research and Innovation (2005-2010); he is author of a number of reports on the handling on nanomaterials and on nanorisks for Austria's Ministry of Health (BMGF) and the Austrian statutory accident insurance (AUVA).

Prof. Dr. Michael Fredholm

Professor Michael Fredholm is a historian and former military analyst. He currently is the Head of Research and Development at IRI, a fully independent research institute that emerged out of the work carried out at the Stockholm International Program for Central Asian Studies (SIPCAS). At Stockholm University, Michael Fredholm conducted a special study of Central Asian geopolitics, Afghanistan, Islamic extremism, and the causes of and defense strategies to counter terrorism. He worked as an independent academic advisor to governmental, inter-governmental, and

non-governmental bodies for more than two decades, including on Foreign Ministry official reports on Eastern Europe, Russia, Central Asia, and failing states. Michael Fredholm also led the team which developed the lone actor terrorism counter-strategy and training program for the Swedish National Bureau of Investigation and Swedish Police Authority, which was implemented in 2014-2015. Educated at Uppsala, Stockholm, and Lund Universities, Michael Fredholm taught at Stockholm University, Uppsala University, the Swedish Royal Military Academy and Defence University, at a special educational and advisory program on East Asia for the Commander-in-Chief and held lectures at numerous institutions and universities around the world.

Dr. Joachim Klerx

Researcher at Austrian Institute of Technology, Innovation Systems Department

Joachim Klerx is researcher at AIT Innovation Systems Department and visiting researcher at the National Defense Academy. As philosopher and economist by education, his main research focus is currently the development of new foresight and horizon scanning methods as well as developing national horizon scanning centers. Some of his achievements in recent years were the development of ISA (Intelligent screening agent) an agent who is looking for weak signals of emerging issues on the Internet, financed by SESTI an EU project about identification of weak signals developed for emerging issues. In the EU project ETTIS Joachim Klerx worked on a system for threat-identification and political agenda setting. In EFP, he did the engineering for a global knowledge exchange platform for the world foresight community. As visiting researcher at the National Defense Academy, he is involved in setting up national horizon scanning center. In addition to this, he works on using artificial intelligence for deep web and dark-net search engines with topic mining and emotion mining as a source for long term strategic planning and innovation management.

Dr. Doris Wolfslehner

Head of the Secretariat of the Austrian Bioethics Commission at the Austrian Federal Chancellery

Doris Wolfslehner holds a PhD in Political Science from the University of Vienna. Presently she is the Head of the Secretariat of the Austrian Bioethics Commission at the Austrian Federal Chancellery. She is member of the Intergovernmental Bioethics Committee of UNESCO, the Bioethics Committee at the Council of Europe (DH-BIO) and the Forum of National Bioethics Committees of the European Union. She regularly works as an ethics evaluator at national and international level and is lecturing at the University of Vienna.

Dr. Peter Steiner

Military Advisor Geneva

Colonel Dr. Peter Steiner started his training at the Theresian Military Academy in 1980 and joined the Austrian Ministry of Defence in 1991 where he worked in different positions, amongst others as a security policy advisor. Peter Steiner was part of an OSCE Electoral Observer Mission in Macedonia in 2002. He promoted 2004 in Ethnology and Political Sciences, 2008 he held a seminar for Security Policy in Berlin, BAKS. 2012 he left for Geneva and works there as a Military Advisor since.

Dr. Laurence Lwoff

Head of Bioethics Unit (DGI - Human Rights Directorate) and Secretary of the Committee on Bioethics (DH-BIO), Council of Europe

Mrs Laurence LWOFF holds a MSc. in reproductive physiology from the University of Paris VI – Jussieu (France). She then obtained her degree in

agronomy from the Institut National Agronomique Paris-Grignon (France) in 1986 and received her PhD in molecular biology in 1989.

She joined the Council of Europe in 1991, where she was entrusted with the responsibilities of the Secretariat of the Conventions concerning the use of animals in agriculture and science, in the Directorate of Legal Affairs. In 1999, her responsibilities were extended to biotechnology. She was the Secretary of the International Conference of the Council of Europe on Ethical Issues Arising from the Applications of Biotechnology (Oviedo, Spain, May 1999). In 2002, she joined the Bioethics Department where she has been responsible in particular for the activities on human genetics and on the protection of the human embryo and the foetus. She was the Secretary of the Group in charge of the elaboration of the Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Genetic Testing for Health Purposes.

She is currently the Head of Bioethics Unit (DGI - Human Rights Directorate) and Secretary of the Committee on Bioethics (DH-BIO), intergovernmental committee in charge of the activities on the protection of human rights in the biomedical field, at the Council of Europe.

Ing. Dr. Ulf Ehlert

Officer, Strategy and Policy Office of the Chief Scientist at NATO Headquarters

Ulf Ehlert holds a Ph.D. in Aeronautical Engineering and worked at the German Aerospace Center in Braunschweig. Since 2005 he held various functions at NATO: Executive Officer to the Applied Vehicle Technology Panel at the NATO Research & Technology Agency, Officer for Technology Outreach and Coordination at the Defence Investment Division at NATO headquarters and Officer for Strategy and Policy at the Office of the Chief Scientist, also at NATO headquarters in Brussels.

Herbert Saurugg MSc.

Expert for Preparation for the Loss of Vital (Critical) Infrastructure

Herbert Saurugg, expert for preparation for the loss of vital (critical) infrastructures, was 15 years career officer in the Austrian Armed Forces in the field of ICT / cyber security. Since 2012 he is dealing with the possible impacts of the increasing connectivity and complexity especially in the infrastructure sector. Special topics: The European Power Supply System and an Europe-wide electricity and infrastructure breakdown ('blackout'). He runs a comprehensive blog at www.saurugg.net.

For the last 10 years Dr. Rath focused on advising the European Commission on Dual Use and Misuse concerns related to research and development. Dr. Rath chaired and participated in numerous multinational review- and audit-panels on security sensitive research. He also chaired and participated in European working groups to develop guidance documents on Human Security (with a section on CBRN), data protection and privacy for the new European 80 billion Euro framework research programme Horizon 2020. Dr. Rath also worked as an advisor to different national authorities on biological weapons related issues and advised individual CBRN sensitive research projects in handling safety and security issues.

Currently, Dr. Rath holds a tenure position as staff scientist at the University of Vienna, Austria, where he heads the Central DNA laboratory and is also the responsible officer for biological, chemical and radiological safety and security of the Department. Dr. Rath lectures a 3 credits University course at the University of Vienna on laboratory safety and security and a 3 credit course in molecular biology. He published extensively on CBRN related issues and gave numerous presentations in international workshops organised by the UN, OSCE, NATO and other international players in the area of security. Dr. Rath has a wide academic background with a Ph.D. degree in microbiology and a Master degree in toxicology, biology and law.

Band 3 / 2018

New technologies have always influenced societies. They have not only entailed advantages. Revolutionary technologies have been misused and, in this way, impacted means and methods used in armed conflict, thus changing strategies as well as tactics. Especially in the fields of nano- and biotechnology as well as robotics experts are expecting new upcoming technological developments that might influence threat scenarios.

Societies spearheading these developments will also play a leading part in global security policy. Competition has already started on a global level and will heat up in the future.

This book outlines future challenges regarding the technological complexity of the individual research areas of nano- and biotechnology and robotics.

ISBN: 978-3-903121-31-7