science
peace
security '19

25.–27.9. 2019 | Darmstadt, Germany
www.sps.peasec.de

Science Peace Security ‘19

Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research

CHRISTIAN REUTER, JÜRGEN ALTMANN,
MALTE GÖTTSCHE, MIRKO HIMMEL (EDITORS)

Science Peace Security ’19
Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research
Christian Reuter, Jürgen Altmann, Malte Göttsche, and Mirko Himmel (Editors)
TUprints, Darmstadt, 2019

URN: urn:nbn:de:tuda-tuprints-91642
URI: https://tuprints.ulb.tu-darmstadt.de/id/eprint/9164

Content

TRACK IV: NEW TECHNOLOGIES AND ARMS CONTROL 137

TRACK IV: OPEN TRACK 225

APPENDIX 237

Science Peace Security '19 – An Editorial

Christian Reuter

Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt

Jürgen Altmann

Experimental Physics III, TU Dortmund University

Malte Göttsche

Nuclear Verification and Disarmament Group, AICES Graduate School and III. Institute of Physics B, RWTH Aachen University

Mirko Himmel

Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg

Abstract

Scientific discoveries and technological innovations have always exerted a great influence on peace and security. New civil and military technologies are revolutionizing warfare. Particularly striking areas are cyber warfare and the rapid development of unmanned weapons systems. Issues of nuclear disarmament, missile defence or space armament as well as chemical and biological weapons are again becoming more urgent. The conference SCIENCE · PEACE · SECURITY '19 aimed for an accurate understanding and fruitful discussions of today's and tomorrow's peace and security challenges. This includes scientific-technical as well as interdisciplinary contributions, focusing on problems of international security and peace-building as well as contributions dedicated to transparency, trust-building, arms control, disarmament, and conflict management.

1. INTRODUCTION

In July 2019, the Science Council, as the most important scientific-political advisory panel in Germany, published its recommendations on the further development of peace and conflict research. They point to an urgent need for action to strengthen scientific-technical peace and conflict research, which in Germany is now structurally too precarious to meet the massive need for political advice: In order to keep the necessary scientific and technical research and expertise permanently available in Germany, however, the Council considers the institutional development and expansion of this area in peace and conflict research to be essential and recommends that the Federal Government and States become active. In addition, the panel calls on the recently established research institutions for cyber security to increasingly address questions of peace and conflict research.

As a positive example of the permanent establishment of this discipline at an university, the Technische Universität Darmstadt was named, the venue for the kick-off event for the new conference series SCIENCE · PEACE · SECURITY: From 25 to 27 September 2019 scientists presented and discussed the current research on interdisciplinary challenges and solutions to questions of international security, the creation of peace as well as transparency- and confidence-building measures, arms control, disarmament and conflict management.

2. TOPICS

To address the interdisciplinary character of the research field, five tracks have been designed:

#	Title	Chair
1	Cyber-Security, Cyber-War and Cyber-Peace	Prof. Christian Reuter, TU Darmstadt
2	Nuclear Nonproliferation / Disarmament	Prof. Malte Göttsche, RWTH Aachen
3	Biological/ Chemical Weapons	Dr. Mirko Himmel, University of Hamburg
4	New Technologies and Arms Control	Dr. Jürgen Altmann, TU Dortmund
5	Open Track	All Track Chairs

The organisers invited researchers and practitioners to contribute to this conference. The conference had the following characteristics:

- 3 days | 30 talks | 16 posters
- 1 pre-workshop | 1 future workshop
- 2 conference dinners | 1 award ceremony
- >100 registered participants | 50 organisations | 10 countries

The program included lectures and discussions by researchers from over 50 organizations, ranging from the natural and engineering sciences (physics, biology, chemistry, computer science) to the humanities and social sciences (political science, peace and conflict research, psychology, philosophy). It bridges the gaps between "classical" challenges of nuclear, biological and chemical hazards and the emergence and need for regulation of "new" technologies such as drones, autonomous weapons or cyber weapons in "classical" and "new" spaces such as cyberspace or the universe.

3. CONTENTS

On the 25th of September Prof. Alfred Nordmann (TU Darmstadt) and Dr. René von Schomberg (European Commission) conducted a pre-workshop on 30+ years of IANUS, which was founded in 1988 at the TU Darmstadt as a central institution for scientific and technical peace research in exchange with social sciences and humanities. In 2000, IANUS received the *Göttinger Friedenspreis* for its outstanding interdisciplinary work. In 2018, coinciding with the establishment of PEASEC, IANUS transformed itself into a network within the TU Darmstadt, which is linked to the university's own funding line for interdisciplinary projects. A lecture on the ambivalence of science and technology (Prof. Jürgen Scheffran, University of Hamburg), which can be used for both good and abusive purposes, introduced the evening.

Prof. Christian Reuter opened the conference together with the section leaders Dr. Jürgen Altmann, Prof. Malte Göttsche and Dr. Mirko Himmel in the Georg-Christoph-Lichtenberg Haus and emphasized the pilot character of the conference format in his speech. Greetings followed by Prof. Ralph Bruder (Vice President of TU Darmstadt), Prof. Ulrich Schneckener (Chairman of the German Foundation for Peace Research) and Dr. Jürgen Altmann (Chairman of FONAS). Afterwards, the program on 26 and 27 September consisted of further lectures and discussions.

The lectures initially analyzed the worldwide state of arms control (Dr. Oliver Meier, SWP, German Institute for International and Security Affairs), especially in the field of chemical weapons (Dr. Paul Walker, International Green Cross) and biological weapons (Dr. Jonathan Forman, OPCW, Organization for the Prohibition of Chemical Weapons) as well as their current technological developments (Dr. Mirko Himmel, University of Hamburg). Challenges to the Biological Weapons Convention posed by biotechnological hazards were explicitly highlighted from the perspective of political science (Dr. Una Jakob, PRIF, Peace Research Institute Frankfurt). The potential for misuse of systems biology (Prof. Kathryn Nixdorff, TU Darmstadt) and innovative genetic technologies (Dr. Johannes Frieß, BOKU (University) Vienna) were examined, as well as nuclear archaeology (Prof. Malte Göttsche, RWTH (University) Aachen), the politics of non-proliferation of weapons of mass destruction (Dr. Jonas Siegel, University of Maryland), the modernization of airborne arms verification (Prof. Hartwig Spitzer, University of Hamburg) or challenges of nuclear proliferation (Dr. Matthias Englert, Oeko Institut).

In addition to nuclear, biological and chemical hazards, the speakers dealt with new technological developments and their impact on peace and security. These include in particular scientific challenges for computer science-related peace research (Prof. Christian Reuter, PEASEC) as well as questions on high-tech (Dr. Niklas Schörnig, PRIF) and cyber weapons

(Thomas Reinhold, PEASEC), cyber arms control (Dr. Matthias Schulze, SWP) and cyber attribution (Thea Riebe, PEASEC). Further lectures were dedicated to critical infrastructures (Dr. Moritz Weiss and Felix Biermann, LMU, Ludwig Maximilian University Munich), drone swarms (Maaike Verbruggen, Vrije Universiteit Brussel), additive manufacturing in the military (Dr. Grant Christopher, VERTIC, not-for-profit non-governmental Organisation) and trustworthy electronics (Dr. Moritz Kütt, IFSH, Institute for Peace and Research and Security Policy; University Hamburg).

Against the background of previous findings in scientific and technical peace research, further researchers tried to draw conclusions on future developments, such as Dr. Jürgen Altmann (TU Dortmund) with a view to military technologies, Prof. Götz Neuneck (IFSH Hamburg) on technological and political arms races and Prof. Martin Kalinowski (CTBTO) on the work of the Comprehensive Nuclear-Test-Ban Treaty Organization.

An important part of the conference program were also 16 poster presentations, most of them presented for discussion by young scientists. They covered a broad spectrum from information warfare, dual use, armed drones to disarmament and arms control of weapons of mass destruction.

4. ACKNOWLEDGEMENTS

The three-day conference was mainly organized by PEASEC (Science and Technology for Peace and Security) in cooperation with IANUS (Interdisciplinary Working Group on Science, Technology and Security) and CROSSING (DFG Collaborative Research Centre) at TU Darmstadt as well as FONAS (Research Association for Science, Disarmament and International Security) and the German Foundation for Peace Research.

The main organizer of the conference was Prof. Christian Reuter (TU Darmstadt) and his team, with support of Dr. Jürgen Altmann (TU Dortmund), Prof. Malte Göttsche (RWTH Aachen) and Dr. Mirko Himmel (University of Hamburg).

We like to thank all organizations and people that made this possible:

- FONAS (Research Association for Science, Disarmament and International Security), DSF (German Foundation for Peace Research), IANUS (Science Technology Peace, TU Darmstadt) and CROSSING (CRC 1119 Cryptography-Based Security Solutions, TU Darmstadt, funded by German Research Foundation) for financial support.
- All authors for their contributions; all reviewers and the programme committee for their feedback.
- All persons involved in organisation and implementation of the conference as well as the proceedings.
- Technische Universität Darmstadt for hosting the conference.

Darmstadt, September/ October 2019

Involved Organizations

Technische Universität Darmstadt (profile area CYSEC)

PEASEC (Science and Technology for Peace and Security), TU Darmstadt

IANUS Science Technology Peace, TU Darmstadt

CROSSING (CRC 1119 Cryptography-Based Security Solutions), TU Darmstadt

FONAS (Research Association for Science, Disarmament and International Security)

German Foundation for Peace Research (DSF)

Physics and Disarmament (P&D), TU Dortmund

Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg

Nuclear Verification and Disarmament Group, RWTH Aachen

Friends:

Institute for Peace Research and Security Policy, University of Hamburg

Öko-Institut e.V. – Institute for Applied Ecology

German Informatics Society – Special Interest Group Human-Machine-Interaction in Safety-Critical Systems

Conference Organization

TRACK AND PROGRAMME CHAIRS

Prof. Christian Reuter, Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt (+IANUS, FONAS, CROSSING)
(General Chair, Track Chair: Cyber-Security, Cyber-War and Cyber-Peace)

Prof. Malte Göttsche, Nuclear Verification and Disarmament Group, AICES Graduate School and III. Institute of Physics B, RWTH Aachen University (+FONAS)
(Track Chair: Nuclear Nonproliferation and Disarmament)

Dr. Mirko Himmel, Carl Friedrich von Weizsäcker-Center for Science and Peace Research (ZNF), University of Hamburg (+FONAS)
(Track Chair: Biological/Chemical Weapons)

Dr. Jürgen Altmann, Physics and Disarmament, TU Dortmund (+FONAS)
(Track Chair: New Technologies and Arms Control)

FURTHER MEMBERS OF THE ORGANIZING COMMITTEE

Thea Riebe, Science and Technology for Peace and Security (PEASEC), TU Darmstadt & University of Siegen (+IANUS, FONAS)

Birgit Schmidt, Science and Technology for Peace and Security (PEASEC), TU Darmstadt

Thomas Reinhold, Science and Technology for Peace and Security (PEASEC), TU Darmstadt (+FONAS)

Dr. Matthias Englert, Öko-Institut e.V., Darmstadt (+FONAS, IANUS Alumni)

Marc-André Kaufhold, Science and Technology for Peace and Security (PEASEC), TU Darmstadt & KontiKat, University of Siegen (+IANUS)

Members: Programme Committee

Dr. Sibylle Bauer, Armament and Disarmament Programme, Stockholm International Peace Research Institute (SIPRI)

Dr. Una Jakob, Peace Research Institute Frankfurt (PRIF)

Ute Bernhardt, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Dr. Myriam Dunn Cavelty, Center for Security Studies (CSS), ETH Zurich

Dr. Kai Denker, Security in Information Technology, TU Darmstadt

Prof. Franz Fujara, Solid State Physics, TU Darmstadt (+IANUS Emeritus)

Dr. Friederike Frieß, Institute for Safety/Security and Risk Sciences, University of Natural Resources and Life Sciences (BOKU), Vienna (+IANUS Alumna)

Prof. Matthias Hollick, Secure Mobile Networking Lab (SEEMOO), TU Darmstadt

Prof. Christoph Hubig, Philosophy, TU Darmstadt (+IANUS Emeritus)

Prof. Britta Hufeisen, Linguistics, TU Darmstadt (+IANUS)

Prof. Martin Kalinowski, Comprehensive Nuclear-Test-Ban Treaty Organization, Vienna

Prof. Stefan Katzenbeisser, Computer Engineering, University of Passau (+CROSSING)

Prof. Gerald Kirchner, Carl Friedrich von Weizsäcker-Center for Science and Peace Research (ZNF), University of Hamburg (+FONAS)

Dr. Moritz Kütt, Institute for Peace Research and Security Policy (ISFH), University of Hamburg and Program on Science and Global Security (SGS), Princeton University

Prof. Markus Lederer, International Relations/Political Sciences, TU Darmstadt (+IANUS)

Prof. Tilo Mentler, Institute for Multimedia and Interactive Systems (IMIS), University of Lübeck

Prof. Florian Müller-Plathe, Theoretical Physical Chemistry Group, TU Darmstadt (+IANUS)

Prof. Simon Nestler, Human-Computer Interaction, Technische Hochschule Ingolstadt

Prof. Götz Neuneck, Institute for Peace Research and Security Policy (ISFH), University of Hamburg (+FONAS)

Prof. Alfred Nordmann, Technoscience/Philosophy, TU Darmstadt (+IANUS, FONAS)

Ingo Ruhmann, Technische Hochschule Brandenburg

Prof. Jürgen Scheffran, Integrated Geography, University of Hamburg (+FONAS)

Dr. Niklas Schörnig, Peace Research Institute Frankfurt (PRIF)

Prof. Stefan Stieglitz, Professional Communication in Electronic Media, University of Duisburg-Essen

List: Authors and Presenters

Dr. Jürgen Altmann, Mathias Pilch and Hubertus Sonntag, Experimental Physics III, TU Dortmund University

Kolja Brockmann, Stockholm International Peace Research Institute (SIPRI)

Dr. Grant Christopher, VERTIC (the Verification Research, Training and Information Centre), London

Dr. Matthias Englert, Öko-Institut e.V., Darmstadt

Dr. Jonathan Forman, Organisation for the Prohibition of Chemical Weapons (OPCW), The Hague

Dr. Johannes L. Frieß, Institute for Safety/Security and Risk Sciences, University of Natural Resources and Life Sciences (BOKU), Vienna

Prof. Alexander Glaser, Program on Science and Global Security (SGS), Princeton University

Prof. Malte Göttsche, Dr. Madalina Wittel, Antonio Figueroa and Lukas Rademacher, Nuclear Verification and Disarmament Group, AICES Graduate School and III. Institute of Physics B, RWTH Aachen University

Maria Hemme, Department of Chemistry & Centre for Science and Peace Research, University of Hamburg

Prof. Martin Kalinowski, Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO), Vienna

Prof. Gerald Kirchner, Dr. Mirko Himmel, Dr. Gunnar Jeremias, Jan Opper and Hares Sarwary, Carl Friedrich von Weizsäcker-Center for Science and Peace Research (ZNF), University of Hamburg

Dr. Daniel Lambach, Goethe University Frankfurt & University of Duisburg-Essen

Dr. Oliver Meier, German Institute for International and Security Affairs (SWP), Berlin

Prof. Kathryn Nixdorff, Biology, Technische Universität Darmstadt

Prof. Götz Neuneck and Dr. Moritz Kütt, Institute for Peace Research and Security Policy (ISFH), Universität Hamburg

Prof. Alfred Nordmann, Institute for Philosophy, Technische Universität Darmstadt

Prof. Christian Reuter, Katrin Hartwig, Franziska Herbert, Marc-André Kaufhold, Tarun Kumar, Thomas Reinhold, Thea Riebe, Stefka Schmid and Gina Maria Schmidbauer-Wolf, Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt

Prof. Jürgen Scheffran, Integrative Geography, University of Hamburg

Dr. Niklas Schörnig and Dr. Una Jakob, Peace Research Institute Frankfurt (PRIF)

Dr. Matthias Schulze, German Institute for International and Security Affairs (SWP)

Dr. Jonas Siegel, School of Public Policy, University of Maryland

Arne Sönnichsen, Political Sciences, University of Duisburg-Essen

Prof. Hartwig Spitzer, Institute of Experimental Physics, University of Hamburg

Maaike Verbruggen, Institute for European Studies, Vrije Universiteit Brussel

Prof. Volkmar Vill and Gesine Rempp, Institute of Organic Chemistry, University of Hamburg

Dr. Paul F. Walker, Institute for Peace Research and Security Policy (IFSH), University of Hamburg, and Arms Control Association, Washington DC.

Dr. Moritz Weiss and Felix Biermann, Global Governance and Public Policy, Ludwig Maximilian University of Munich.

Track I: Cyber-Security, Cyber-War and Cyber-Peace

Track Chair:

Christian Reuter

Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt

Introduction

Technological and scientific progress, especially the rapid development of information technologies (IT), plays a crucial role in questions of peace and security. This track addresses the significance and potentials of IT with respect to peace and security. For this purpose, the track sheds light on: IT in Peace, Conflict and Security Research, Cyber Conflicts and War (Information Warfare, Cyber Espionage and Cyber Defence, Darknets), Cyber Peace, Dual Use and Technology Assessment, Confidence and Security Building Measures, Arms Control, Restraint Measures, Unmanned Systems, Verification in Cyberspace, Critical Infrastructures, Attribution, Resilient Critical Infrastructures, Critical Information Infrastructures, Open Source Intelligence, Situation Assessment, Human-Computer-Interaction, Culture and Social Interaction, Cyber Deception, Cultural Violence and Peace in Social Media, Social Media and ICT Usage in Conflict Areas.

To discuss information technology for peace and security, SCIENCE · PEACE · SECURITY invited contributions from the fields of computer science, IT security and Human-Computer-Interaction, as well as policy relating to technical issues.

Information Technology for Peace and Security – An Emerging Research Field

CHRISTIAN REUTER

SCIENCE AND TECHNOLOGY FOR PEACE AND SECURITY (PEASEC), TECHNISCHE UNIVERSITÄT DARMSTADT

[#1-PAPER]

ABSTRACT

Technological and scientific progress, especially the rapid development in information technology (IT), plays a crucial role regarding questions of peace and security. This short overview addresses the significance, potentials and challenges of IT for peace and security. For this purpose, the talk offers an introduction to peace, conflict, and security research, thereby focusing on natural science, technical and computer science perspectives. In the following, it sheds light on fundamentals (e.g. IT in peace, conflict and security, natural science/ technical peace research), cyber conflicts and war (e.g. information warfare, cyber espionage, cyber defence, Darknet), cyber peace (e.g. dual-use, technology assessment, confidence and security building measures), cyber arms control (e.g. arms control in the cyberspace, unmanned systems, verification), cyber attribution and infrastructures (e.g. attribution of cyber-attacks, resilient infrastructures, secure critical information infrastructures), culture and interaction (e.g. safety and security, cultural violence, social media), before an outlook is given.

1. INTRODUCTION

In December 2017, an invasion of the German government network was discovered; This network links federal ministries and authorities (see Reinhold 2018a). The attackers used the Intranet of the Federal College of Public Administration and the Federal Academy of Public Administration as a gateway. This is the least secure part of the system because external participants also need to access it outside the institution, for example, for further education of the Foreign Office. Probably the first intervention should further penetrate the network. In order to gain freedom of movement on the intranet, administrative rights were claimed systematically. So far it could not be clarified whether parts of the used malware remained in the system (see Mascolo et al. 2018).

This incident is a good example of the increasing relevance of information technology for peace and security (see Reuter 2019). The innovations of scientific and technical research have always been used for military purposes and have thus strongly influenced warfare.

2. CYBERSPACE AS A WAR SCENE?

Violent conflicts can be conducted in different domains. In addition to land, sea, air and space, the so-called cyberspace is one of them. Therefore, the resilience of IT infrastructures is of increasing importance. Nevertheless, security strategies only insufficiently consider the specific characteristics of IT:

- Many of the actors involved (representing the group of potential aggressors) are either individuals or part of the private sector.
- The attribution of security-threatening or offensive activities is difficult because the identity of the security threat is unknown.
- Security concerns and international proliferation - that is, the proliferation of military or military technologies within and between states (see Altmann 2019) - increase the risk of military intervention as a preventive measure (see Chivvis & Dion-Schwarz 2017).
- Many technologies can also be misused as a weapon or part of a weapon system. Therefore, they are inherent in the risk of being misappropriated to harm a significant number of people. The dual-use problem (see Riebe & Reuter 2019) is of increasing relevance to IT, in particular, because the military use of IT systems and infrastructures phenomena such as cyberwar, the information war (see Ruhmann & Bernhardt 2019), (terrorist) propaganda, fake news (see Kaufhold & Reuter 2019), data espionage and hacking (see Herrmann 2019).

3. CONCLUSION

Existing research shows that information technology has a significant impact on warfare and military strategies. On the one hand, military forces increasingly rely on cyberspace, create capacities for offensive action in this domain, and even place it, as in the case of the United States, at the centre of future warfare. On the other hand, there is a lack of appropriate responses to questions regarding the international regulation of cyber conflicts and the current dynamics of rearmament. This circumstance is also due to the permanent ambiguity that veils cyberspace, its actors, and the operations it carries out: there are no dividing lines between internal and external security nor is it clear which cyber resources are defensive or can be assigned as open-minded.

The digital revolution also continues with network-centred warfare, which has the potential to transform warfare permanently. Attribution and verification continue to pose problems, although they are indispensable for the enforcement of international law. After all, cyber-defence faces legal dilemmas, not least due to the lack of standards regarding pre-emption, prevention and counter-operations. The peculiarities of cyberspace in the context of peace and security require a separate consideration to address the complexity and ambiguity of the field.

4. ACKNOWLEDGEMENTS

This contribution is based on Reuter et al. (2019).

REFERENCES

Altmann, Jürgen. (2019). Natural-Science/Technical Peace Research. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 39–60). Wiesbaden: Springer.

Chivvis, Christopher S., & Dion-Schwarz, Cynthia. (2017). Why It's So Hard to Stop a Cyberattack - and Even Harder to Fight Back. Retrieved from https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html

Herrmann, Dominik. (2019). Cyber Espionage and Cyber Defence. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 83–106). Wiesbaden: Springer.

Kaufhold, Marc-André, & Reuter, Christian. (2019). Cultural Violence and Peace in Social Media. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden, Germany: Springer Vieweg.

Mascolo, Georg, Steinke, Ronen, & Tanriverdi, Hakan. (2018, March). Die Geschichte eines Cyber-Angriffs. Süddeutsche Zeitung.

Reuter, Christian. (2019). Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden, Germany: Springer Vieweg.

Reuter, Christian, Aldehoff, Larissa, Riebe, Thea, & Kaufhold, Marc-André. (2019). IT in Peace, Conflict, and Security Research. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden, Germany: Springer Vieweg.

Riebe, Thea, & Reuter, Christian. (2019). Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 165–183). Wiesbaden: Springer.

Ruhmann, Ingo, & Bernhardt, Ute. (2019). Information Warfare - From Doctrine to Permanent Conflict. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 63–82). Wiesbaden: Springer.

Chips, Bits & Atoms: Building Trusted Electronics for Disarmament Verification

MORITZ KÜTT

INSTITUTE FOR PEACE RESEARCH AND SECURITY POLICY (ISFH), UNIVERSITY OF HAMBURG

ALEXANDER GLASER

PROGRAM ON SCIENCE AND GLOBAL SECURITY (SGS), PRINCETON UNIVERSITY

[#2-PAPER]

ABSTRACT

Whenever electronics are used to monitor and inspect states' obligations as part of nuclear arms control treaties, special attention has to be given to the trustworthiness of these devices. Carrying out verification without electronics has been discussed by some, however, it is unlikely that this would be a solution for every verification task. Instead, we have to build systems that have a reduced likelihood of hardware backdoors and hidden switches as well as less vulnerabilities with regard to the used software. As one idea to overcome this problem, we propose the use of very old electronics hardware and using physical storage media. Such vintage hardware has a number of important advantages for applications where multiple parties need to simultaneously establish trust in the systems used. CPUs designed in the distant past, at a time when their use for sensitive measurements was never envisioned, drastically reduce concerns that the other party implemented back-doors or hidden switches. Limited computing capabilities also limit the space of possible software manipulations. We present a prototype vintage verification inspection system using the MOS 6502 processor. Using a custom designed digitization circuit, the device records gamma spectra from a sodium-iodine detector. It also offers the possibility to store reference data on physical storage media (punched cards), which can improve resilience against attacks.

1. INTRODUCTION

Nearly three decades after the end of the Cold War, there are still about 15,000 nuclear weapons in the arsenals of the nine nuclear weapon states. After an era of transparency, cooperation, and confidence-building in the 1990s, progress in nuclear arms control has slowed down in the 2000s and is currently in a crisis. New propositions are needed, and any progress toward nuclear disarmament will rely on robust verification measures. Whenever electronics are used to monitor and inspect states' obligations as part of nuclear arms control treaties, special attention has to be given to the trustworthiness of these devices.

Disarmament Verification can include a variety of activities: Inspections of weapon production facilities, storage locations and deployment sites, measurements of radiation signatures of nuclear warheads to confirm their authenticity prior to their dismantlement, measurements estimating amounts of fissile materials, or technical methods to prove the absence of weapons and fissile materials after disarmament took place (Göttsche et al., 2015).

Inspections are carried out by inspecting countries or international organizations to ensure that a host country is in compliance with its obligations. Both host and inspector have competing interests. Devices used in these potentially hostile environments must, beyond providing correct measurements, be protected against malicious misuse and manipulation. One solution, carrying out verification without electronics has been discussed by some, however, it is unlikely that this would be a solution for every verification task (Glaser, 2014). Electronic-based system have to be developed with a reduced likelihood of hardware backdoors and hidden switches as well as less vulnerabilities with regard to the used software.

Confirming the authenticities of nuclear warheads is a common application of trusted measurement systems. To protect sensitive information of a warhead's radiation signature, "information barriers" process the data acquired during an inspection, but only display results in a pass/fail manner. Information barriers for warhead confirmation measurements use either an attribute approach or a template approach. For the attribute approach, the device measures a number of properties and considers an object a treaty accountable item if the results meet specific criteria. Properties, thresholds, and ranges have to be negotiated prior to inspections. Information barriers based on the template approach compare measured data to a template dataset that has been recorded from a trusted reference item, which can be obtained, for example, by randomly selecting a warhead directly from its delivery system under inspector supervision (Spears, 2001; Jie and Glaser, 2015).

2. Contribution

We focus on the issue of building an information barrier as an example of trustworthy electronics. Several research efforts have produced prototype systems for such information barriers (Sastre, Vanier, 1988; MacArthur, 1999; Seager et al. 2001; Williams et al. 2007; Allen et al., 2013). As a key requirement, the hosting party wants to ensure that the information barrier does not leak sensitive information to the inspector, neither due to an accident nor due to inspector intervention. Besides security concerns, the host is also concerned with the safety of device usage, avoiding accidents in the process of nuclear disarmament. Often, using only host-supplied tools in the host's facilities is an additional requirement. The inspector requires that the information displayed by the device correctly reflects the physical reality. Software and hardware vulnerabilities are a constant concern for such devices, as they could be used for malicious intentions.

As one idea to overcome this problem, we propose building information barriers based on very old electronics hardware and using physical storage media. Such vintage hardware has a number of important advantages for applications where multiple parties need to simultaneously establish trust in the systems used. CPUs designed in the distant past, at a time when their use for sensitive measurements was never envisioned, drastically reduce concerns that the other party implemented back-doors or hidden switches. Limited computing capabilities also limit the space of possible software manipulations.

We built a prototype vintage verification inspection system based on the MOS 6502 processor. The prototype uses an Apple IIe computer, for which we designed two custom extension cards. One card provides high voltage for a sodium-iodine detector, the second card records gamma spectra from a sodium-iodine detector. All processing, including energy calibration, is carried out on the 1 MHz 6502 processor. The prototype also offers the possibility to store reference data on physical storage media (punched cards), which can improve resilience against attacks. We demonstrate that the computational capabilities of the 6502 are sufficient to record and analyse gamma-spectra with count rates of several thousand counts per second.

REFERENCES

Allen K., Backe S., Chambers D.M., Day E., Hustveit S., Johansson K. et al. (2013). UK-Norway Initiative (UKNI) approach for the development of a Gamma Ray Attribute Measurement System with an integrated Information Barrier. Proceedings of 35th ESARDA Symposium. Edited by F. Sevini. Bruges, Belgium; May 2013.

Glaser, A., Barak, B. and Goldston, R. J., (2014). A zero-knowledge protocol for nuclear warhead verification, Nature 510: 497–502.

Göttsche, M., Kütt, M., Neuneck, G. and Niemayer, I. (2015). Advancing Disarmament Verification Tools: A Task for Europe?. EU Non-Proliferation Consortium, Non-Proliferation Papers No. 47, October 2015.

Jie Y., Glaser A. (2015). Nuclear Warhead Verification: A Review of Attribute and Template Systems. Science & Global Security; 23(3): 157-170. doi:10.1080/08929882.2015.1087221.

MacArthur D. (1999). Proposed Attribute Measurement System (AMS) with Information Barrier For the Mayak/PPIA Demonstration: System Overview. Report LA-UR-99-5611. Los Alamos National Laboratory.

Sastre C., Vanier P.E. (1988) CIVET a Controlled Intrusiveness Verification Technology. Report BNL-90156-1988, Brookhaven National Laboratory.

Seager K.D., Mitchel D.J., Laub T.W., Tolk K.M., Lucero R., Insch K.W. (2001). Trusted Radiation Identification System. Proceedings of 43rd Annual INMM Meeting, Indian Wells, CA, July 2001.

Spears, D. (Ed.) (2001). Technology R&D for Arms Control. U.S. Department of Energy, Office of Nonproliferation Research and Engineering, Washington, DC; 2001. Available from www.ipfmlibrary.org/doe01b.pdf.

Williams R., Johansen T., Karpius P., MacArthur D., and Smith M. (2007). Implementation of an Information Barrier for the Next Generation Attribute Measurement System. 48th Annual INMM Meeting, Tucson, AZ; July 2007.

Quo Vadis Cyber Arms Control? – A Sketch of an International Vulnerability Equities Process and a 0-Day Emissions Trading Regime

Matthias Schulze

German Institute for International and Security Affairs (SWP)

[#3-long-paper]

Abstract

Although the threat of cyber-conflict rises with the ongoing digital arms race, not much ground has been gained with cyber arms control regimes. This is due to technical characteristics of the digital domain, issues of regime verification and the lack of political will. The paper analyses proposals for cyber arms control designed after traditional arms control regimes and concludes, that this is the wrong paradigm. Instead, it sketches out a regime that is modelled after the climate change regime, including emissions trading for 0-day vulnerabilities. Additionally, the paper discusses the suggestion of an International Vulnerability Equities Process as a second component to such a regime.

1. Introduction

The economic damage caused by cyber-activities rises every year and now resides around 600 billion US-Dollar annually. Cyber-espionage, both political and economic, is causing headaches in many governments around the world and the spectre of a full-fledged inter-state cyber-conflict, resulting in loss of life and physical damage, features prominently in many threat assessments of governments (Lawson 2013). The digital arms race is in full swing as now more than 100 states possess cyber-capabilities and many of them offensive military cyber-programs (Smeets 2018a). Since modern industrial societies are highly dependent on information technologies, which are vulnerable to hacking, the urgency rises to react to growing cyber-threats. Since the late 1990s, there are multiple efforts to restrict collateral damage from cyber-attacks and to enforce responsible state behaviour in cyber-space. Approaches taken in reigning-in cyber-warfare, are mainly driven via international law and the laws of armed conflict (Tallinn Process) & informal norms of appropriate state behaviour (UN GEE Process, Paris Call) (Henriksen 2019), Confidence Building Measures (Pawlak 2016), industry associations (Digital Geneva Convention, Charter of Trust), bilateral cyber-treaties restricting economic espionage (US, China agreement 2015), or unilateral measures, such as national due diligence and resilience (deterrence by denial), active cyber-defense and engagement (deterrence by punishment) or non-escalatory policies of state-restraint. But arguably, no substantial ground has been made in terms of cyber arms control regimes, although calls for these are repeatedly uttered in international discussions (Nye 2015). The most prominent proposal in this direction is that of an international attribution agency to provide a collection solution to the problem of attributing cyber-attacks (Davis 2017). Joseph Nye describes the fragmented regulatory landscape in the cyber-domain as regime complex of multiple, separate governance issues that often lack depth (Nye 2014). These mostly normative efforts lack "punch", since they rely on voluntary adoption and have no "strong" verification or enforcement mechanisms as traditional arms control regimes.

The scope of the paper is to give an overview of current academic debates about cyber-arms control regimes. Scholars unison argue, that traditional arms control models do not easily, if at all, apply to the particularities of the digital domain. Therefore, a second related question is what best practices from other regime-types can be deduced that might apply to the characteristics of the digital domain. Besides technical issues, there are political reasons and factors of regime-design, especially issues of verification of non-compliant behaviour and treaty enforcement that complicate any type of digital arms control regime. Although similar issues have plagued other arms control regimes as well (Eilstrup-Sangiovanni 2018), the thesis of this paper is that the paradigm of arms control might not be feasible in the cyber-domain and instead we need to look for other regime types that regulate different things and include non-state actors. The climate regimes, especially emissions trading seem to be an interesting avenue to pursue. It is checked whether this regime type is feasible for the digital domain. The following section describes the state of research and presents the arguments that have been produced against digital arms control.

2. LITERATURE REVIEW: CHALLENGES IN REGULATING DIGITAL ARMS

Arms control regimes typically aim to limit or reduce certain types of weapons or military behaviour (like testing, use or deployment) in order to prevent conflict, to limit the acceleration and the cost of arms races (Reinhold & Reuter 2019, 207-210). There are three major problem complexes that restrict the feasibility of the arms control approach in the digital domain: 1) the particularities of the object of regulation, 2) challenges of verification regime-enforcement and 3) political problems.

2.1. CYBER-WEAPONS AS AN OBJECT OF ARMS CONTROL?

The first problem is, that it remains unclear what exactly the object of regulation in any type of digital arms control regime would be. It could be prohibiting behaviour like cyber-attacks, or objects like "cyber-weapons". The term cyber-attack is highly politicized and encompasses various elements such as penetrating a network with digital or social (phishing) means, implanting malicious code, stealing information, disrupting services or producing a destructive, or even kinetic effect (Arimatsue 2010). Depending on the interpretation, cyber-attacks can be an object, a technology or an activity/operational capacity. Likewise, there is no consensus that digital software qualifies as an object, like a weapon (Tikk 2017). The terms cyber-weapon or digital arms describe not one entity but a vast array of tools and techniques, from low potential (Distributed) Denial of Service attacks, social engineering, credential theft and the use of malware, which can be subdivided into exploits utilizing known or unknown vulnerabilities (0-day). High potential malware with destructive effects is most likely to be considered a cyber-weapon since it utilizes a launch vehicle (a means to deliver) and a payload that executes actions on the objective (Rid 2018, 2018, 73–75).

If one would assume the position, that malicious code could act as a cyber-weapon, which then could be perceived as the object of regulation, more problems arise. Geers (2010) argues, that malicious code is notoriously difficult to define (Geers 2010). Unlike physical weapons, which are traditionally defined as devices intentionally designed to kill, injure or disable people or property, malware is seldom designed to kill. Digital objects like malware code have no intrinsic properties, unlike a war-head with a determined destructive capacity measured in kilo-tons. Even though malware could potentially kill someone, for example by disabling a pace-maker, this is always a secondary or indirect effect that is dependent on the interaction of a digital and a physical system (Arimatsue 2010). A computer cannot kill directly, until it is attached to a physical device that can, like an Unmanned Aerial Vehicle for example. The potential destructive effect of malware is highly dependent on the characteristics of the system it penetrates. This makes damage highly unpredictable and difficult to establish. However, this might change in the future since software is developing fast, which presents another challenge for finding a suitable definition for an arms control regime. The transitory nature of 0-day exploits, basically describing their limited shelf-life, might present a further issue for arms control (Eilstrup-Sangiovanni 2018; Smeets 2018b). Thus, it remains elusive, whether the weapon analogy makes sense at all.

2.2. INSTITUTIONAL PROBLEMS: VERIFICATION AND ENFORCEMENT

The second major challenge for a digital arms-control regime is verification. In order to be effective, arms control regimes need a mechanism to verify that regime members adhere to the principles outlined in a treaty. Historically, verification measures "range from methods that allow supervision without on-site assessment like aerial imaging or seismic sensors to the structured collection, submission and exchange of data between states on stockpiles and trade volumes and on-site inspections with counting and measuring stockpiles and facilities" (Reinhold & Reuter 2019, 216). This means there must be some sort of accounting measuring the relative strength of cyber-arsenals and cyber-power. Cyber-power is notoriously difficult to measure. Since the main actors of cyber-conflict are intelligence agencies, whose activity is shrouded in high levels of secrecy, and considering the problem of attribution, there is no easy way to measure cyber-arsenals (Borghard & Lonergan 2017) or relative cyber-power.

Digital arms in that regard share many of the problems that other dual-good items, like chemical agents or biological toxins, have. In fact, it could be argued, that software is more than dual use. Dual-use unfolds on two axes: First, most software is primarily developed in the private sector, rather than in the military domain. Everyone with sufficient knowledge can write malware on any computer around the world, even at home (Geers 2010). Malware is cheap and being sold on a thriving black market for crime-ware and exploits (Ablon et al. 2014). Additionally, there is a thriving grey market of the traditional arms industry engaging in research and development and reverse engineering of vulnerabilities and exploits (Burgers & Robinson 2018). The private sector is rather dominant in the digital domain and has shown little interest in regulation. The regulation would most likely be ineffective as well. Software is easy to conceal, highly intangible and malleable. Software code is essentially knowledge, which can be easily copied and thus cannot be destroyed. The Crypto-Wars of the 1990s showed, that software in form of encryption algorithms could even be printed out and smuggled over a border on paper (Schulze 2017). Thus, proliferation is easy, and the very concept of digital "disarmament" does not make sense.

The second axis is, that code can be used both defensively and offensively. Attackers and defenders often rely on the same toolkits. Banning or regulating software designed for cyber-offense, might impede cyber-defense, like vulnerability research and ethical hacking (Dumbacher 2018). The current malware-trend called "living off the land" basically utilizes on-board software of hijacked systems, like the Windows Powershell. In many cases, attackers subvert the legitimate tools of defending IT-administrators for offensive purposes. This essentially makes software code "quadruple use". All of this implies, that "artifact-centric" arms control mechanisms fall short in the digital age" (Dumbacher 2018, 221).

More so, a verification for software might come with unacceptable costs and risks, since it would technically imply a global surveillance infrastructure that monitors what is happening on every single digital device on the planet. Ruhrmann (2015) suggests that global surveillance infrastructure set-up by NSA, with programs such as Turmoil and Turbulence, could act as a means of verification since it scans Internet traffic at large scale IXP (Ingo Ruhrmann 2015, 572). Infrastructures for active cyber-defense, i.e. observing adversary behaviour and capability at his/her network could serve a similar function, especially since more states are adopting these types of policy (Schulze & Herpig 2018). Given the current reactions to cyber-espionage, it is highly unlikely that states would voluntarily agree to monitor each other networks. Alternatively, a mass-surveillance system like Chinas Great Firewall could be utilized for screening every data-packet at the Internet Service Provider or Internet Exchange Point Level for the proliferation of malicious cyber-weapons (Geers 2010). This type of intrusive monitoring would be more dangerous for highly digitized economies. The cost of compliance with such a regime thus might be higher than the actual reduction of risk that follows from such a mechanism (Ford 2010). Additionally, a Chinese-style Great Firewall would be a direct violation of Western norms such as free speech and a promotion of a free and open Internet.

Closely connected to the problem of verifying treaty-violating behaviour is the problem of enforcing treaty policies. How do we punish non-compliant behaviour? The attribution problem, i.e. the issue of identifying actors responsible for malicious cyber-activity lies at the core of the enforcement problem. This is a multifaceted problem. State-driven cyber-attacks often use proxy-actors, like hired cyber-criminals or contractors to maintain plausible deniability (Maurer 2017). It is not just states operating in the cyber-domain, but a multitude of non-state actors like hackers, organized crime, and exploit-brokers, which makes determining treaty compliance hard. More so, state actors hijack the offensive infrastructure of their opponents to launch attacks (4th party collection) and repurpose malware of other state entities to operate under false-flag (Guerrero-Saade & Raiu 2017). Thus, it is still relatively hard and especially time-consuming to obtain tamper proof evidence that shows non-compliance. States also operate on vastly different skill levels or tiers. This unequal skill level makes it harder for smaller states to detect non-compliance of the more tech-savvy states. Additionally, the asymmetric vulnerability that different large and medium-sized economies face, make it harder for small-states to file violations against more powerful ones. Additionally, what would a proportionate response to non-compliance entail? There is currently no international consensus on what a proportional response could be (Eilstrup-Sangiovanni 2018, 393).

2.3. POLITICAL PROBLEMS PREVENTING CYBER-ARMS CONTROL

Another non-trivial issue is the question, what carrots would a regime offer that would overcome the lack of political will to restrict offensive cyber-capabilities. Many states regard cyber-space as an offense-dominant environment and thus assume that they would gain a relative advantage by building-up offensive cyber-capabilities, compared to the costs that such a build-up implies (Eilstrup-Sangiovanni 2018, 384-388). In many states, spending and personal for offensive-operations outweigh that of cyber-defense. As of now, states don't perceive it to be in their self-interest to restrict cyber-capabilities (Dumbacher 2018, 208). This was also the case with other types of arms control regimes that historically developed in the step-by-step process from no-regulation to a full-fledged regime. Oftentimes, the political will aims to regulate increases after shock-situations, for example (near)-catastrophic events like the Cuban missile crisis, that convinced policy-makers of the risks that have grown too high (Jervis 1978). Compared to the nuclear-age, the cyber-age did not witness its Hiroshima and Nagasaki wake-up call yet (Kaplan 2016).

Even if a "digital pearl harbor" ought to occur, scepticism might be in order whether it increases political momentum for regulation. First, some argue, that "cyber-weapons" are simply not dangerous enough, at least compared to nuclear weapons (Burgers & Robinson 2018). Pearl Harbor style strategic cyber-attacks are regarded as highly overrated in the academic literature (Lawson 2013). Second, even if political momentum for regulation arises, it does not guarantee that one aspect of cyber-activity will be regulated: cyber-espionage. States historically lack the will to restrict peacetime espionage which is why it is highly ambiguous with regard to international laws since it is not explicitly condoned nor condemned and thus almost without any international regulation (Radsan 2007). Most cyber-activity entails an espionage component, mainly the reconnaissance of a target (such as lateral movement) before the action on the objective (the payload) is executed. Computer-Network Attack and Computer-Network-Exploitation share many characteristics and cannot be meaningfully separated (Lindsay 2013, 370). They are often indistinguishable from another, especially from the defender's point of view, which is why espionage is often treated as if it was a destructive attack (Buchanan 2017). Likewise, military cyber-operations rely extensively on signals intelligence, so that these two spheres converge, neatly illustrated by the organizational dual-hat set-up of US Cybercommand: the head of NSA is the head of cyber command. It is conventional wisdom in espionage that nobody likes it, but everyone does it. As such, regulation of cyber-capabilities that often entail espionage is highly unlikely since it is in states-interest to maintain this capability. The problem is, that arms control regimes and the overall strategic posture must go hand-in-hand in order to be a feasible policy option (Eilstrup-Sangiovanni 2018, 381). If arms control regimes do not complement national security behaviour and entail concrete carrots, they are less likely to be adopted (Lewis 2010). Since no-spy regimes typically have the same issues of verification and enforcement, due to the attribution problem, their strategic value remains limited.

Final points are ideological differences and different threat perceptions regarding the digital domain. Cyber-security is a fuzzy, undefined concept that includes competing narratives and thus threat assessments (Tikk 2017). Especially Western states securitized the digital domain differently than authoritarian regimes (Hansen & Nissenbaum 2009). The West adheres to the notion of cyber-security, which is first and foremost a technical issue and has critical-infrastructure failure as its referent object. “We tend to conceive cyber conflict in terms of warfare, as a matter of attack and defence” (Ford 2010). This cyber-war paradigm regards cyber-attacks as an analogue to conventional military attacks, enacted by combatants, based on a dualism of war and peace. Viewing cyber-threats through that lends leads logically to the conclusion, that “cyber-weapons” should “be governed by the traditions embodied in the law of armed conflict”, including the right to self-defence and the concept of equivalence (cyber equals physical) (Ford 2010). Likewise, if cyber-weapons targeting critical infrastructures are perceived as an existential threat, arms control follows logically as a seemingly appropriate solution.

Russia and China perceive digital insecurities through the lens of information warfare, a much broader concept of which cyber-attacks are a mere sub-component. The referent objects in this paradigm are political and social systems that can be undermined by threats emerging from information weapons, such as social media platforms, mass-media, and propaganda (Tikk 2017). The psychological effect of cyber-attacks in this view is way more important than their kinetic potential. The fear of a propaganda campaign that mobilizes the masses to revolt against the ruling elites is central in this paradigm. Information war is continuous and the dualism of war and peace is abandoned (Ford 2010). The logical conclusion following from this problem definition is not arms control, but information control, basically meaning censorship and the dissolution of public discourse through disinformation and active measures (Bendiek & Schulze 2019).

These two competing paradigms are irreconcilable since information control violates the core norms of democratic societies such as freedom of speech. Thus, the West should not fall into the trap of adapting to the authoritarian playbook and starting to “weaponize information” as well (Klimburg 2017). The ideological divide historically was one reason why so far, international efforts, such as the United Nations Governmental Group of Experts failed and why consensus is hard to achieve in other spheres of Internet Governance. China and Russia prefer state control over Internet data-streams and oppose the multi-stakeholder governance model that Western states prefer (Nye 2014).

2.4. Summary of the most important obstacles of cyber-weapons in arms control

The previous section outlined the most important aspects of the cyber-domain that any arms control regime has to account for in order to meaningfully restrict dangers of the digital domain:

- The problem of the unclear definition of the object being regulated, namely software, cyber-attacks, malware.
- The dual use issue (civil/military and offensive/defensive) and intangible features of the object being regulated.
- The question, whether the regime should sanction behaviour, like attacking or proliferation weapons, or prohibit certain types of objects.
- The question, how an unobtrusive and beneficiary verification regime could look like.
- The attribution of non-compliant behaviour and enforcement of sanctions.
- The problem of easy proliferation of digital goods on black markets, over the Internet as well as the decentralized means of production, storage and distribution of digital goods.
- The dominant role of the private sector in the cyber-domain, accounting for 95% of all digital infrastructure and goods.
- The power balance asymmetries between high-tech and low-tech actors.
- The overcoming of the lack of political will to restrict behaviour in an offense-dominated cyber-space.
- Overcoming the ambiguous nature of espionage activity.
- Overcoming the ideological differences, i.e. paradigms of cyber- vs. information war.

2.5. Traditional obstacles of arms control regimes

Besides these newer, digital-domain specific obstacles to arms control, any type of arms control regime must overcome some traditional obstacles as well. According to Eilstrup-Sangiovanni (2018), an effective arms control regime must ”1) secure broad participation from major cyber-faring states, (2) set out rules that effectively constrain state behaviour, (3) provide sufficient credible information on actions in cyberspace to reduce uncertainty about state interests and allow effective signalling, and (4) ensure significant costs to non-compliance. Fulfilling these goals in tandem will be challenging.” She further outlines elemental features for effective arms control:

- “Any regime must supply information to reduce uncertainty and to clarify states’ interests, information about their activity in order to reassure others.
- It must constrain behaviour by defining clear rules for (im)permissible behaviour, i.e. restricting the use of cyber-weapons, or prohibiting certain types of attacks, or against certain targets.
- It must lower the risk of accidental conflict by introducing transparency and mechanisms for crisis management.

- It must entail collective attribution, since otherwise it cannot impose costs for non-compliance. This would lower the costs of attribution, reduce asymmetries in attribution-capabilities and thus would present an incentive to participate.
- It must clarify the responsibility of state and non-state actors, especially of states utilizing cyber-proxies.
- It must offer support (carrots) for compliance, for example by increasing access to funding, professional expertise or capacity-building measures" (Eilstrup-Sangiovanni 2018, 391–398).

3. REGIME TYPES ACCOUNTING FOR THE PARTICULARITIES OF THE DIGITAL DOMAIN

Having outlined the principles of effective arms control regimes, generally, as well as for the specifics of the digital domain, most research analyzes what arms control regimes could serve as a model for restricting cyber-war activities. The following arms control regimes have been proposed in research:

- Nuclear arms control regime such as the Non-Proliferation Treaty (Borghard & Lonergan 2018), which is generally regarded as impractical (Nye 2015), with the exemption of the Comprehensive Test Ban Treaty (Eilstrup-Sangiovanni 2018).
- The Geneva Protocol (1925) proposed by Dumbacher (2018) and the later Chemical Weapons Convention of 1997, as proposed by Geers (2010).
- The Biological and Toxin Weapons Convention proposed by Fidler (2015) and Reinhold & Reuter (2019).
- The Wassenaar Arrangement, proposed by Fidler (2015) and Reinhold & Reuter (2019).

Other regulatory approaches that have been considered as possible regulatory frameworks, but have not been analysed in greater detail:

- The Convention on Civil Aviation of 1994, proposed by Durmbacher (2018).
- EU Cybercrime Convention 2001, Fidler (2015).
- Shanghai Cooperation Organization's International Information Security Agreement 2009 (Eilstrup-Sangiovanni 2018).
- The 2018 Proposal of the EU parliament for harmonized dual use export regulation Reinhold & Reuter (2019).
- International Telecommunication Union Fidler (2015).

The following table presents an overview of these studies, analysing which particularities of cyber-weapons introduced in section 2 of this paper are covered by these regimes, and which are incompatible. Note that this list does only account for the question, whether the particularities of the digital domain could be accounted for or are addressed in these regimes, not whether how well or effective these issues are addressed. It does not answer the questions on how effective these regimes would be in regulating digital arms (on the issue of regime efficiency see Müller (2000)). The table uses a simple classification scheme assessing, whether the regime could account for the particularities of cyber-weapons: mostly, somewhat, or not at all. This assessment only uses a nominal scale and is based on a rough-heuristic and no quantitative models. Of course, since none of these regimes is a "digital-only" regime, they cannot account fully for the particularities of the digital domain. Whether these regimes indeed could serve as a model for digital arms control has to be judged with in-depth case studies in future research and lies beyond the scope of the paper.

The regime accounts for…	**Chemical Weapons Convention 1997**	**Biological and Toxin Weapons Convention 1975**	**Wassenaar Arrangement, 1996**	**Protocol for the Prohibition the Use in War of Asphyxiating Poisonous Gases, and of Bacteriological Methods of Warfare, 1925**	**Convention on Civil Aviation 1994**	**Comprehensive Test Ban Treaty 1996**
… Problem of unclear definitions of the object being regulated	Mostly	Somewhat	Somewhat	Somewhat	Mostly	Mostly
… dual use issues and intangible features of the object being regulated.	Somewhat	Somewhat	Mostly	Somewhat	Mostly	Mostly
… regulating behaviour or objects	production, stockpiling	development, production, stockpiling, distribution	Distribution	Prohibiting use in war. Storage, production, transfer and peaceful use not included.	Regulating behaviour. Restricts military aviation over territory.	bans all nuclear explosions, for both civilian and military purposes, in all environments.
… reliable, unobtrusive verification	Mostly	Not at all	Not at all	Not at all	Mostly	Mostly
… attribution of non-compliance and enforcement	Somewhat	Not at all	Not at all	Not at all	Mostly	Mostly
… the problem of easy proliferation (black markets) and decentralized production of the object to being regulated.	Somewhat	Somewhat	Mostly	Somewhat	Not addressed	Somewhat
… private sector/non-state actors participation in the problem.	Somewhat	Somewhat	Mostly	Somewhat	Mostly	Not addressed
…balances power asymmetries of members.	Somewhat	Not addressed	Not at all	Not at all	Mostly	Mostly
… overcoming lack of political will by offering sticks and carrots.	Mostly	Somewhat	Somewhat	Somewhat	Mostly	Mostly
… overcoming unregulated espionage aspects.	Not addressed	Not addressed	Somewhat	Not addressed	Not addressed	Not addressed
… overcoming ideological differences (cyber vs. information war)	Not addressed	Not addressed	Not addressed	Not addressed	Not addressed	Not addressed

Table 1. Overview over the studies

From this preliminary overview, three regime types are particularly noteworthy. First, the biological weapons and toxins share some of the problems of digital arms, namely the ease of proliferation, the difficulties of delineating offensive and defensive use and the hard-to verify nature. There is an indication, that future trends such as bio-printing might lead to similar problems as in the cyber-domain, namely drop of prizes and an increase in decentralized production and proliferation of biological agents, for example in form of CAD files shared the Internet (Brockmann et al. 2019).

Secondly, the Wassenaar Arrangement is by far the most advanced regime accounting for the particularities of the digital world. However, it is not without flaw. The offense/ defence dual-use nature of some of the objects being regulated is not clear-cut, as some vulnerability researchers criticize the export list of being too broad, that it covers legitimate tools as well (Gannon 2015). Also, the voluntary nature and the lack of a verification and enforcement mechanism, make it an imperfect candidate.

Lastly, the Convention on Civil Aviation covers accounts for the dual-use nature and the private sector dominance, while including verification and enforcement. This might be due to the relatively uncontentious nature of the object being regulated, namely aircraft. Furthermore, since it deals with aircraft, the attribution issue is not as complicated as in the digital world, since airplanes can be demarcated by transponders and national insignia. This solution does not hold well in the digital domain since there is no easy way to create tamper-proof digital insignia.

Noteworthy is, that none of the aforementioned regimes cover the issue of espionage, which reflects its ambiguous nature in international law.

4. VULNERABILITIES AS A CHANCE?

Since definitional issues are a problem for outlawing cyber-weapons directly, another avenue could be to prohibit the use of some of their subcomponents, namely zero-day or 0-day vulnerabilities (Fidler 2014). If the cyber-weapon analogy applies, then 0-days are the munition or the launch-vehicles for such weapons. While certainly not totally without issues, the definition of a 0-day is straight forward and relatively uncontested: it is a vulnerability in a soft or hardware that the software vendor is not aware of and that currently is not fixed by a patch. If the vendor is notified and a patch is released, a 0-day turns into a N-day vulnerability. Publicly disclosed vulnerabilities are typically being collected in a public CVE database (CVE Database 2019). Thus, it can be easily determined ex-post facto whether a cyber-attack utilized a 0-day, without necessarily answering the question who used it. A regime prohibiting the use of only 0-day attacks, while leaving the door open for less intrusive types of N-day attacks, could be in states self-interest. First, 0-day attacks are typically the ones with the most destructive potential often, targeting critical infrastructures. Stuxnet is the prime example here. Since cyber-norms and confidence building measures also focus on prohibiting critical infrastructure attacks, there is room for consensus here (Pawlak 2016). Second, restricting only 0-days while allowing the use of N-days and phishing leaves states with enough room to manoeuvre for limited offensive operations. 0-day exploits are not a requirement for effective cyber-operations, but rather a luxury item. Third, there already exists a worldwide ecosystem and infrastructure for disclosing and managing vulnerabilities, from CERT information sharing to coordinated vulnerability disclosure policies and bug-bounties within companies, that could be utilized for such a regime (Schulze 2019).

To be effective, the regulation of 0-days requires at least two components: a regime that focuses on state behaviour (use of 0-days), and a second component that addresses the private sector dominance in emanating zero-days.

4.1. International Vulnerabilities Equities Process (IVEP)

Currently, the USA, Great Britain, Australia, Canada, and China have a published vulnerabilities equity process (VEP), with other countries like Germany working on one (Herpig & Schwartz 2019). VEPs are inter-agency processes that gauge the offensive and defensive value of 0-day vulnerabilities. VEPs try to answer the question, whether a government obtained 0-day vulnerability is kept secret and being utilized for offensive purposes, or whether the knowledge of this vulnerability is being disclosed to the software-vendor, thus increasing defence. After being notified of a vulnerability, the vendor ideally patches the vulnerability and thus immunizes the software system against any further attacks based on this vulnerability. The idea behind a VEP is to restrict certain types of offensive cyber-capability that represent a high-risk for a state, while permitting the use of 0-days that entail little risk (Healey 2016). Vulnerabilities in the core Internet or encryption protocols, would entail global and collective risks, because they affect everyone using the same software, while others, for example software in country-specific military equipment, only entail localized risks.

Since many states started to restrict 0-days for their own use, it is reasonable to envision a global and collective process reducing the risk emanating from 0-day vulnerabilities, an International Vulnerabilities Equities Process (IVEP). The concept has been brainstormed at the UN Disarmament Center, but not much has been published about this (United Nations Institute for Disarmament Research 2018). An IVEP could be grafted upon national VEP processes but would require an international organization that acts as a hub to which states then will disclose their vulnerabilities, that went through their domestic VEP in the first place. The organization, consisting of member-states and IT-security experts would then assess the vulnerabilities. Like on the national level there could be two options a) retain a vulnerability for exclusive use among IVEP members or b) disclosing it to the vendor. Exclusive access to vulnerability information could be a useful carrot to ensure membership participation, since members gain something from adhering to such a regime. Knowing of a 0-day before others allows to immunize systems first or to employ this 0-day for own offensive cyber-operations. It could be modelled after already existing threat sharing programs in cyber-security, for example the Zero Day Initiative. CERTS for example regular share threat indicators in rather exclusive circles to which not everyone has access. Maylin Fidler (2014) suggests, that because of trust issues, such a regime should focus on like-minded states first, and then gradually expand: “NATO could institute a group disclosure program: when one member stockpiles a vulnerability, it could also disclose the vulnerability to a NATO clearinghouse. NATO members could then protect themselves against that vulnerability, or potentially also make use of it” (Fidler 2014, 162). The IVEP secretariat could also be tasked with measuring compliance. Violators of the agreement could be sanctioned with exclusion from relevant information streamed. An IVEP secretariat could also have the role of assisting less-developed member-states with mitigation strategies or supplement national VEP processes in the first place. Many smaller cyber-powers often lack the expertise and know-how to evaluate 0-day by themselves and thus are unable to set up VEP. An IVEP secretariat, doing the 0-day equities on a national level could inform national VEP processes.

There are, however, major obstacles to overcome. First, states are reluctant to share their "crown jewel" vulnerabilities, even among close partners such as the Five-Eyes intelligence alliance of NATO. Sharing knowledge of a 0-day reduces its operational value, since others can start to immunize themselves against attacks based on the vulnerable. 0-days are only valuable when nobody else knows about them (Nobody but us, or NOBUS principle). Sharing vulnerabilities also might uncover espionage assets and shed light on the relative operational capacity or cyber-power of states, which they are unwilling to uncover (Aitel & Tait 2016). Lastly, disclosing custom-developed vulnerabilities to an IVEP means wasted (financial) resources, and thus comes with no return of investment for the disclosing state. Anonymous disclosure could be an option for states in sharing the vulnerabilities without revealing their capability and know-how.

Second, it can be assumed that states might have different assessments regarding disclosing or hoarding vulnerabilities within an IVEP. One country could vote against disclosing it, because it uses it for its own offense, while others want to disclose it to the vendor. This might create international tension and requires an effective governance model that accounts for these types of disagreement.

Third, an IVEP regime introduces another layer of complexity. Coordinated Vulnerability Disclosure is already a complex and fragmented endeavour (Schulze 2019). Currently, bug disclosure operates mostly in a decentralized: researchers commit vulnerabilities directly to the vendor. The same is true for states with a VEP that decide to disclose. Introducing another layer, another organization that debates about the very same vulnerability that has been discussed on a national level, might be inefficient, since too much time goes by before the issue is patched. Additionally, an IVEP secretariat might be a profound target by hostile cyber-operations and thus might have difficulties in ensuring the security and privacy of meetings and vulnerability information. Another option could be, that members and civil-society researchers could disclose vulnerabilities to the IVEP secretariat voluntarily, thus increasing its reach

Fourth, since domestic retention of 0-days is temporary anyway, this fact could be an incentive to disclose 0-days at the end of their lifecycle.

As such, this is just a rough sketch of an IVEP and more research needs to be done.

4.2. 0-DAY EMISSIONS TRADING REGIME

If digital assets are no weapons, maybe the cognitive heuristic of an arms control regime is misleading anyway. Maybe an alternative paradigm could be utilized, that treats vulnerabilities as a by-product or a negative emission of industrialized software production. Vulnerabilities are mostly caused by the private sector, due to negligence, fast software innovation cycles, agile software development, outsourcing, bad quality assurance, and in-house vulnerability procedures. Since an IVEP regime only addresses the state-side of the problem, a vulnerability emission-trading regime could be used to create market incentives for more secure software design, resulting in less vulnerabilities. The international climate regime might be a role model, since it focuses on both state and private actors. Vulnerabilities in a globalized, tech-interdependent world are comparable CO2 emissions and climate change is comparable to the problem of global cyber-security: it is a global, collective action problem, plagued with free-riding and incompatible national-interests as well. The climate regime evolved in a step-by-step process over the last 50 years (Bodansky 2001). It faced similar problems like these identified for the cyber-domain in the chapters before, like competing ideologies (climate change denial, North vs. South) and the issue of verification and compliance.

The climate regime is complex, so I will focus only on one tool: emissions trading. Emissions are based on the idea, that a price is put on pollution, which creates an economic incentive to reduce emissions. A central authority must define a cap of allowed emissions per organization per year and watch over its compliance:

> "*Once the cap has been set and covered entities specified, tradable emissions allowances (rights to emit) are distributed (either auctioned or freely allocated, or some combination of these). Each allowance authorizes the release of a specified amount of Greenhouse Gas emissions, generally one ton of carbon dioxide equivalent (CO2e). The total number of allowances is equivalent to the overall emissions cap (e.g., if a cap of one million tons of emissions is set, one million one-ton allowances will be issued). Covered entities must submit allowances equivalent to the level of emissions for which they are responsible at the end of each of the program's compliance periods*" (Center for Climate Energy Solutions 2011).

This model could be translated to the software world. Currently, it is estimated, that 1000 lines of software code include 10-50 bugs, some of which are vulnerabilities and even fewer of them can be exploited by attackers. Every year, a certain number of vulnerabilities are patched by each software vendor per year. For example, Vulnerability sharing programs "together published 1,026 vulnerabilities, of which 425 (44 percent) target Microsoft, Apple, Oracle, Sun and Adobe products" (Frei 2014, 12). This could be a rough estimate for gauging the degree of tolerable 0-day emissions per year, as it scales with the size of a company and the number of software products it releases. Thus, companies must buy a permit to exhaust more than say 100 vulnerabilities per year. Prices for allowances could be gauged by utilizing market prices that exploit brokers such as Zerodium pay to hackers. The income generated with a cap and trade regime could be redistributed for the mitigation of cyber-security incidents, bounty-payments for ethical hackers and vulnerability researchers, or for developing more secure software architectures.

5. DISCUSSION AND CONCLUSION

The two sketched approaches could help to alleviate some of the aforementioned problems of digital arms control regimes. With regard to 0-days, the definitional problems are considerably smaller compared to the issue of cyber-weapons. VEP processes by design address the dual-use nature of 0-days, for offensive and defensive purposes, and so would an IVEP process.

Combined with a 0-day emissions trading regime, the private/public dichotomy could also be addressed, since the vast majority of 0-day vulnerabilities is created by the industry. Both IVEP and 0-day emissions trading would regulate a clearly defined object, namely 0-days. Admittedly, the issue of verification and regime enforcement remains unsolved, as long as the attribution problem persists. Both an IVEP and an emissions regime would have effects on 0-day black markets since they are likely to address the price structure that black hat hackers are willing to pay for 0-days (Schulze 2019). If done correctly, an IVEP regime could counter power balances and asymmetries between more and less advanced companies and provide a mechanism for lower advanced states to supplement national VEPs. If the incentive structure is done right, it might also be in states interest to participate, however, there is a long way to go and details need to be sketched out. An IVEP and an emission regime also are ideologically neutral, and least regarding cyber vs. information security. 0-days are an issue in authoritarian and democratic countries alike. However, the issue of espionage and intelligence incentives is likely to remain unsolved with such a regime.

The purpose of this paper was to challenge the arms control paradigm for cyber-weapons. It was argued, that maybe this is not the right lens since it does not account for many of the characteristics of the digital domain. More private sector-oriented regimes like civil aviation or emissions-trading regimes could be more fruitful as an analogy. The paper proposed a very rough sketch of two-possible avenues to pursue, although many questions remain unsolved. Especially the attribution issue that lies at the core of cyber-security is a challenge. However, even arms control in the digital domain seems very unlikely at the moment, we should not forget that the situation looked equally grim for other types of regimes. The negative effects of Greenhouse Gas Emissions have been known for more than a hundred years now and the climate change regime, as inefficient as it currently is because it does not meaningfully stop climate change, only took shape in the last 30 years. A similar slow process can be expected in the digital domain.

References

Ablon, L.; Libicki, M. C.; Golay, A. A. (2014): Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. RAND.

Aitel, D.; Tait, M. (2016): Everything You Know About the Vulnerability Equities Process Is Wrong. Lawfare. Retrieved from https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.

Arimatsue, L. (2010): A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. In: Christian Czosseck und Katharina Ziolkowski (Hg.): 4th International Conference on Cyber Conflict. Tallinn.

Bendiek, A.; Schulze, M.(2019): Disinformation and elections to the European Parliament. Stiftung Wissenschaft und Politik.

Bodansky, D. (2001): The History of the Global Climate Change Regime. In: Urs Luterbacher (Hg.): International relations and global climate change. Cambridge, Mass.: MIT Press (Global environmental accord).

Borghard, E. D.; Lonergan, S. W. (2017): The Logic of Coercion in Cyberspace. In: *Security Studies* 26 (3), S. 452–481. DOI: 10.1080/09636412.2017.1306396.

Borghard, E. D.; Lonergan, S. W. (2018): Why Are There No Cyber Arms Control Agreements? Council on Foreign Relations. Retrieved from https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements.

Brockmann K.; Bauer, S.; Boulanin, V. (2019): BIO PLUS X: Arms Control and the Convergence of Biology and Emerging Technologies. Stockholm Peace Research Institute.

Buchanan, B. (2017): The Cybersecurity Dilemma. Hacking, Trust and Feat Between Nations: Oxford University Press (1).

Burgers, T.; Robinson, D. R. S. (2018): Keep Dreaming. Cyber Arms Control is Not a Viable Policy Option. In: *S+F* 36 (3), S. 140–145. DOI: 10.5771/0175-274X-2018-3-140.

Center for Climate Energy Solutions (2011): Climate Change 101. Cap and Trade.

CVE Database (2019). Retrieved from https://www.cvedetails.com/.

Davis, J. S. (2017): Stateless attribution. Toward international accountability in cyberspace. Santa Monica Calif.: RAND Corporation (Research report, RR-2081-MS).

Dumbacher, E. D. (2018): Limiting cyberwarfare. Applying arms-control models to an emerging technology. In: *The Nonproliferation Review* 25 (3-4), S. 203–222. DOI: 10.1080/10736700.2018.1515152.

Eilstrup-Sangiovanni, M. (2018): Why the World Needs an International Cyberwar Convention. In: *Philosophy & Technology* 31 (3), S. 379–407. DOI: 10.1007/s13347-017-0271-5.

Fidler, M. (2014): Anarchy or Regulation: Controlling the Global Trade in Zero-Day Vulnerabilities.

Fidler, M. (2015): Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis. In: *Journal of law and Policy for the Information Society* 11 (2). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2706199.

Ford, C. (2010): The Trouble with Cyber Arms Control. In: *The New Atlantis* Fall. Retrieved from https://www.thenewatlantis.com/docLib/20110301_TNA29Ford.pdf.

Frei, S. (2014): The Known Unknowns. Empirical Analysis of Publicly Unknown Security Vulnerabilities. NSS Labs. Retrieved from https://www.nsslabs.com/blog/measuring-known-unknowns-cyber-security.

Gannon, J.(2015): Wassenaar: Turning arms control into software control. Internet Governance Project. Retrieved from https://www.internetgovernance.org/2015/05/25/wassenaar-turning-arms-control-into-software-control/.

Geers, K. (2010): Cyber Weapons Convention. In: *Computer Law & Security Review* 26 (5), S. 547–551. DOI: 10.1016/j.clsr.2010.07.005.

Guerrero-Saade, J. A.; Raiu, C. (2017): Walking in your enemy's shadow: when fourth-party collection becomes attribution hell. Kaspersky Labs. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170728/Guerrero-Saade-Raiu-VB2017.pdf.

Hansen, L.; Nissenbaum, H. (2009): Digital Disaster, Cyber Security, and the Copenhagen School. In: *International Studies Quarterly* 53, S. 1155–1175.

Healey, J. (2016): The U.S. Government and Zero-Day Vulnerablities. From Pre-Heartbleed to Shadow Brokers. In: *Journal of International Affairs* November.

Henriksen, A. (2019): The end of the road for the UN GGE process. The future regulation of cyberspace. In: *Journal of Cybersecurity* 5 (1), S. 425. DOI: 10.1093/cybsec/tyy009.

Herpig, S.; Schwartz, A. (2019): The Future of Vulnerabilities Equities Processes Around the World. Lawfare. Retrieved from https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

Ruhrmann, I. (2015): Neue Ansätze für die Rüstungskontrolle bei Cyber-Konlfikten. In: Douglas Cunningham, Petra Hofstedt, Klaus Meer, Ingo Schmitt (Hg.): Informatik 2015. Lecture Notes in Informatics. Bonn: Gesellschaft für Informatik.

Jervis, R.(1978): Cooperation Under the Security Dilemma. In: *World Politics* 2 (30). Retrieved from 167-214.

Kaplan, F. M. (2016): Dark territory. First Simon & Schuster paperback export edition.

Klimburg, A. (2017): The Darkening Web. The war for cyberspace. New York: Penguin Press.

Lawson, S. (2013): Beyond Cyber-Doom. Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. In: *Journal of Information Technology & Politics* 10 (1), S. 86–103. DOI: 10.1080/19331681.2012.759059.

Lewis, J. (2010): Cyberwarfare and its impact on international security. 19 February 2009, United Nations, New York. New York: United Nations (United Nations Publication, 19).

Lindsay, J. R. (2013): Stuxnet and the Limits of Cyber Warfare. In: *Security Studies* 22 (3), S. 365–404. DOI: 10.1080/09636412.2013.816122.

Maurer, T. (2017): Cyber Mercenaries: Cambridge University Press.

Müller, H. (2000): Compliance Politics: A Critical Analysis of Multilateral Arms Control Treaty Enforcement. In: *The Nonproliferation Review* Summer.

Nye, J. (2014): The Regime Complex for Managing Global Cyber Activities. Hg. v. Chatham House. Global Commission on Internet Gocernance.

Nye, J. (2015): The World Needs an Arms-control Treaty for Cybersecurity. Belfer Center for Science and International Affairs. Retrieved from https://www.belfercenter.org/publication/world-needs-arms-control-treaty-cybersecurity.

Pawlak, P.(2016): Confidence-Building Measures in Cyberspace Current Debates and Trends. In: Anna-Maria Osula und Henry Roigas (Hg.): International Cyber Norms. Legal, Policy & Industry Perspectives. Tallinn.

Radsan, A. J.(2007): The Unresolved Equation of Espionage and International Law. In: *Michigan Journal of International Law* 28 (3).

Reinhold, T.; Reuter, C. (2019): Arms Control and its Applicability to Cyberspace. In: Christian Reuter (Hg.): Information Technology for Peace and Security. Wiesbaden: Springer Fachmedien Wiesbaden, S. 207–231.

Rid, T.(2018): Mythos Cyberwar. Über digitale Spionage Sabotage und andere Gefahren. Unter Mitarbeit von Bettina Engels und Michael Adrian. Hamburg: Edition Körber. Retrieved from https://www.deutschlandfunk.de/thomas-rid-mythos-cyberwar.1310.de.html?dram:article_id=429262.

Schulze, M. (2017): Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. In: *MaC* 5 (1), S. 54. DOI: 10.17645/mac.v5i1.805.

Schulze, M. (2019): Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik. Stiftung Wissenschaft und Politik.

Schulze, M.; Herpig, S. (2018): Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them. Council on Foreign Relations.

Online:https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them.

Smeets, M.(2018a): A matter of time. On the transitory nature of cyberweapons. In: *Journal of Strategic Studies* 41 (1-2), S. 6–32. DOI: 10.1080/01402390.2017.1288107.

Smeets, M. (2018b): The Strategic Promise of Offensive Cyber Operations. In: *Strategic Studies Quarterly* Fall, S. 90–113.

Tikk, E. (2017): Cyber-Arms Control without arms? In: Tommi Koivula und Karariina Simonen (Hg.): Arms control in Europe. Regimes, trends and threats. Helsinki: National Defence University (National Defence University Series 1, Research publications, No. 16).

United Nations institute for Disarmament Research (2018): Preventing and Mitigating ICT-Related Conflit. United Nations institute for Disarmament Research. Cyber Stability Conference.

Counting Cyber Weapons – New Approaches to Regulate and Control Destructive Cyber Tools

Thomas Reinhold

Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt

[#4-paper]

Abstract

The cyberspace increasingly becomes an important domain for military activities and regular hacking incidents underline the necessity for effective defensive measures. The development of offensive capabilities (often dubbed "cyber weapons") on the other hand raises questions, how such military tools can get secured and cyber arms races prevented by measures of arms control. Whereas the domain cyberspace with its specific features prevents the application of established measures, the computer sciences provides approaches that can get applied or adapted for the specific tasks of arms control and especially its practical measures of verification. The contribution will discuss these possibilities, highlight applicable scenarios and identifies further research questions.

1. Introduction and Related Work

Over the last several years, cyber attacks had become a regularly used measure within interstate conflicts. Although the attribution of these attacks to specific state actors is seldom sufficient, the disturbance, disruption or even destruction of IT systems increasingly becomes a realistic threat for states. Under this impression and the comprehension of the interconnectedness and dependencies of modern societies from IT systems and their services, a growing number of states worldwide have started to recognize the cyberspace as the next military domain (UNIDIR, 2013). Beside preparations for defensive measures, tactics and the necessary tools, the strategic planning of some military forces also involves the establishment of offensive capabilities. Where some states argue that this is a necessary prerequisite for deterring foreign malicious actors (McKenzie, 2017), others understand such capacities as appropriate measures to react to cyber attacks by actively disturbing or even destroying the attacker's IT systems (Brangetto et al., 2014). Unfortunately, for a growing number of states cyber weapons are also becoming a regular part of their military, strategic and tactical planning within the complex military corpus (UK Government, 2016; USA-DOD, 2018). Whereas these projects "create facts", the international community still struggles with agreeing on binding norms of state behavior and questions how established rules of international law apply to this new domain (Tikk & Kerttunen, 2017). These debates include the challenge of determining an appropriate response to lawfully regulate the ongoing militarization of cyberspace, the questions of how to slow down the cyber armament and prevent an arms race in this domain. Nevertheless, in the last years important attempts have been conducted nationally and internationally to propose and develop such standards as well as political measures for confidence building in cyberspace (Tikk, Homburger et al., 2017). Exemplary for this is the work of the OSCE (OSCE, 2016b, 2016a) and the UN (UN-GGE, 2012, 2015) as well as individual states and alliances such as the "Paris Call for Trust and Security in Cyberspace" (France-Gov, 2018) or the "Commonwealth Cyber Declaration" (Commonwealth, 2018). A very important contribution had been made by the first and second versions of the Tallinn Manuals (NATO, 2013; Schmitt & Vihul, 2017) by discussing the applicability of existing rules of international law to the cyberspace and the actions of states in this domain in times of war and peace. On the other side, the attempts of confining the ongoing cyber arms race by applying the concepts of established practical measures of arms control, non-proliferation or the "lessons learned" from other military technological developments still come quickly to a stop (Alwardt et al., 2017; Neuneck, 2014; Reinhold, 2019; Reinhold & Reuter, 2019). Besides misleading political perceptions of the cyberspace and its working principles, the specific technical features of the cyberspace, that differ from other, and physical domains prevent the application of existing knowledge and procedures (Burgers & Robinson, 2018; Geers, 2010). This fact becomes exemplary obvious by the currently missing, commonly shared and binding definition for the concept of cyber weapons.

This term is - despite its widely usage - a very misleading expression. In difference to conventional military weapons, the cyberspace offers multiple different ways to spy, influence, disrupt or destroy foreign IT systems. The methods and tools differ for varying actors but all of them result more or less in the intrusion of IT systems and jeopardize its intended functionality, a process that can either happen open and direct or concealed and successive. Most of the malicious tools of the cyberspace rely on the same "base material": the knowledge of vulnerabilities in IT products and its practical application as so called "exploits". These are necessary to circumvent IT protection measures and to deploy the malicious code - the so called "payload" - which executes the intended operations, either espionage and data theft or the interference with the running IT system and its services (Wrozek, 2017).

2. METHOD AND RESULTS

Based on the described situation and its challenges, the talk assesses the current state of the militarization of the cyberspace as well as the presumably existing or actively developed cyber weapons. It analyses the current scientific and political perspective on cyber weapons and discusses the technical assumptions of its functionality. Current definitions of cyber weapons concentrate on the intention or the usage of malicious IT tools (Mele, 2013; Rid & McBurney, 2012), which is sufficient for political agreements and norms that aim to regulate the handling, the usage or the trading of such malicious tools. In contrast, the argumentation of this contribution follows the premise that for practical arms control measures the very specific technological features of cyber weapons, that differ from other weaponized technologies need to get considered independently, without misleading comparisons or analogies to established approaches for other weapons technologies like conventional weapons, biological, chemical or nuclear weapons (Perkovich & Levite, 2017). Starting with an assessment of existing approaches of describing and categorizing cyber weapons (Herr, 2014; Maathuis et al., 2016, 2018; Mele, 2013; Rid, 2012), the contribution will provide a technical assessment of these particularities that need to get considered for cyberspace specific future arms control and non-proliferation approaches. An important part of this assessment is the identification and evaluation of physically measurable parameters that can be used to develop and implement practical arms control approaches (Reinhold, 2019).

Within the efforts and debates of arms control, an important element of peace and security politics of the last decades had been the challenge of limiting the deliberate or undeliberate destruction potential of weapons technologies. Regarding the militarization of the cyberspace the virtuality of this domain, its absence of physical boundaries and the seamless multiplication of code and data undermine most of the so far developed measures and procedures for securing weapon stockpiles or mutually controlling the military systems. For the challenge of restricting and monitoring specific cyber technologies, its military application or supervising agreed limits of stockpiles for cyber weapons it will be necessary to point out in detail which specific technical aspect, component, and functions are concerned and how its control can get implemented. Based on a discussion of the differences of physical domains in comparison to the cyberspace, the limitations of former arms control approaches and the challenges that arise from this situation, the contribution aims to provide an in-depth analysis of these specifics and design principles as well as of the cyberspace, as the underlying technology that differ from former weapon technologies. It follows the perspective of arms control which searches for the critical components and technical thresholds that transforms a technology, its development or deployment into a weapon (Shabashnyi, 2019) as an indicator for a necessary regulation or supervision.

In strong contrast to this problematic and apparently unsolvable situation, an in-depth review of the core mechanisms of practical arms control measures - counting, tracing and limiting - reveals, that similar challenges had already been dealt with in the computer sciences in many other contexts. Examples are digital rights management (DRM) systems that seek to verify or restrict the usage of digital goods - which is basically a question of non-proliferation - or the blockchain mechanism that provides reliable and tamper-proof storage of data and information within any kind of processes, a core necessity for arms trade regulation. Additional examples are networking techniques like the upcoming IPv6 that allows a unique, worldwide identification of any IT device or the border gateway protocol (BGP) which is used to define borders and self-contained entities with a clearly defined responsibility. Although only as a first step, the contribution follows the premise that these existing developments can be applied or adapted for the challenges of developing necessary practical measures for cyber arms control.

3. Discussion and Conclusion

With its results, the contribution aims to present new approaches to arms control for the cyberspace on the basis of established computer science technologies. It will illustrate the steps to assess, develop and implement the necessary measures and evaluate its prospects, applicable scenarios as well as its limitations and possible pitfalls. In conclusion, it will give an outlook on what questions need further research and where computer scientists can contribute to the challenge of peace, security and international stability in the cyberspace.

References

Alwardt, C., Neuneck, G., & Kubiak, K. (2017). Nukleare Rüstungskontrolle. *Friedensforum*, vol. *5*. Retrieved from https://ifsh.de/no_cache/personal/neuneck/veroeffentlichungen/publication/ja-03655-2017/#c3655

Brangetto, P., Minárik, T. & Stinissen, J. (2014). From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications. *Legal Gazette*.

Burgers, T., Robinson, D. R. S. (2018). Keep Dreaming: Cyber Arms Control is Not a Viable Policy Option. *Sicherheit & Frieden*, vol. *36*, iss. 3, pp. 140–145. https://doi.org/10.5771/0175-274x-2018-3-140

Commonwealth. (2018). Commonwealth Cyber Declaration. www.thecommonwealth.org/commonwealth-cyber-declaration

France-Gov. (2018). Paris Call for Trust and Security in Cyberspace.

Geers, K. (2010). Cyber Weapons Convention. *Computer Law & Security Review*, vol. *26*

Herr, T. (2014). PrEP: A Framework for Malware and Cyber Weapons. *Journal of Information Warfare*, vol. *13*, pp. 87–106. https://doi.org/10.2307/26487013

Maathuis, C., Pieters, W. & Den Berg, J. V. (2016). Cyber weapons: a profiling framework. In *2016 International Conference on Cyber Conflict (CyCon U.S.)* (pp. 1–8). IEEE. https://doi.org/10.1109/CYCONUS.2016.7836621

Maathuis, C., Pieters, W. & Van Den Berg, J. (2018). A Computational Ontology for Cyber Operations. *Proceedings of the 17th European Conference on Cyber Warfare and Security, 278-288*. Retrieved from https://search.proquest.com/openview/f6ccddd62973bd89b136908879582004/1?pq-origsite=gscholar&cbl=396497.

McKenzie, Timothy M. (2017). *Is cyber deterrence possible?* Retrieved from https://catalog.loc.gov/vwebv/search?searchCode=LCCN&searchArg=2016052326&searchType=1&permalink=y

Mele, S. (2013). Cyber-weapons: legal and strategic aspects. Italian Institute of Strategic Studies “Niccolò Machiavelli.”

NATO. (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare. Retrieved from http://www.ccdcoe.org/249.html

Neuneck, G. (2014). Krieg im Internet? Zur Einhegung des Cyberwar. *Friedensgutachten 2014*.

OSCE. (2016a). Decision No. 5/16 - Osce Efforts Related to Reducing the Risks Of Conflict Stemming from the Use of Information And Communication Technologies. Hamburg. Retrieved from https://www.osce.org/cio/288086?download=true

OSCE. (2016b). OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies.

Perkovich, G. & Levite, A. E. (2017). From Understanding Cyber Conflict: Fourteen Analogies.

Reinhold, T. (2019). Cyberspace as Military Domain: Monitoring Cyberweapons. In D. Feldner (Ed.), Redesigning Organizations - Concepts for the Connected Society. Springer Nature, Switzerland.

Reinhold, T., Reuter, C. (2019). From Cyber War to Cyber Peace. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden, Germany: City: Wiesbaden Publisher: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4_7

Rid, Thomas, & McBurney, Peter. (2012). Cyber-Weapons. The RUSI Journal, vol. 157, iss. 1, pp. 6–13. https://doi.org/10.1080/03071847.2012.664354

Schmitt, M. N., & Vihul, L. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (M. N. Schmitt, Ed.). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

Shabashnyi, H. (2019). Gaining the advantage. Applying Cyber Kill Chain Methodology to Network Defense. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Tikk, E., Homburger, Z., Kerttunen, M., Adamson, L., DeBusser, E., Sander, B., Tsagourias, N. (2017). Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use Of Information and Communications Technology: A Commentary. Retrieved from https://www.un.org/disarmament/wp-content/uploads/2018/04/Civil-Society-2017.pdf

Tikk, E., & Kerttunen, M. (2017). The Alleged Demise of the UN GGE: An Autopsy and Eulogy.

UK Government. (2016). National Cyber Security Strategy 2016-2021.

UN-GGE. (2012). Developments in the field of information and telecommunication in the context of international security: Work of the UN first Committee 1998-2012. Retrieved from http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

UN-GGE. (2015). Consensus report 2015 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174. Retrieved from http://undocs.org/A/70/174

UNIDIR. (2013). The Cyber Index - International Security Trends and Realities. Retrieved from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

USA-DOD. (2018). National Cyber Strategy. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Wrozek, B. (2017). Cyber Kill Chain Methodology. Retrieved from http://m.isaca.org/chapters3/Charlotte/Events/Documents/Event Presentations/12062017/Cyber_Kill_Chain_Wrozek.pdf

Accessing Dual-Use in IT Development

THEA RIEBE AND CHRISTIAN REUTER

SCIENCE AND TECHNOLOGY FOR PEACE AND SECURITY (PEASEC), TECHNISCHE UNIVERSITÄT DARMSTADT

[#5-PAPER]

ABSTRACT

The use of information technology (IT) in peace, conflict and security raises some questions, i.e. whether the use of IT can be limited exclusively to so-called advantageous purposes and applications and whether improper use can be prevented. This ambivalence is called a dual-use dilemma, meaning that objects, knowledge and technology can find both useful and harmful applications. Dual-use questions have been addressed in various disciplines, in particular in nuclear technology and the production of nuclear weapons, but also in chemistry and biology. In all these disciplines, dual-use topics in technical development and education have been discussed and addressed. Nevertheless, the importance of dual-use differs slightly, depending on the technology and its risks, as well as its distribution and application. Nuclear technology is less accessible than biotechnology, which in turn is less accessible than IT.

1. INTRODUCTION

In 2016, NATO states recognized cyberspace as a military domain, in order to assess cyber operations as an attack or to become active themselves (NATO, 2016). Cyberspace forces are expanding worldwide, while the use of IT in all areas of life is increasing. This raises more than ever the question of evaluating research and development in computer science with regard to potential military uses of software developed for civilian use. In atomic physics, biology and chemistry, the dual-use risks were intensively studied (Altmann et al., 2017; Liebert et al., 2009; Tucker, 2012). These studies have also helped to identify techniques for evaluating and controlling these same risks and have provided the basis for the concept of Dual-Use Research of Concern (DURC). DURC refers to research, (new) technologies, or information that has the potential for beneficial and harmful applications (Oltmann, 2015). The question is therefore whether computer science can also be used to define an IT Research and Development of Concern that requires a context-based dual-use impact assessment and, similar to the life sciences, helps to reduce the potential for misuse during software development.

The challenge is that the respective dual-use risk depends on the state and process of research and development of the respective work, while the technology remains inherently ambivalent. In particular, software is characterized by its versatility of use and adaptation in conducive and harmful contexts, and by its indirect effect which differs substantially from directly harmful ABC weapons (Carr, 2013; Lin, 2016, 119). Nevertheless, in order to make evaluations and design decisions that take the dual-use risk into consideration, individual case studies are required which must be very context- and technology-specific. Such case studies not only evaluate a single technology, but also contribute to the development of formal and informal dual-use governance methods (Tucker, 2012, 30–39) and the evolution of the socio-technical safety culture.

2. STATE OF RESEARCH

Dual-use is widely and divergently applied and defined, as the term can refer to research, knowledge, as well as technologies and individual objects (Forge, 2010; Harris, 2016). An early assessment of the consequences or use of one's own research and development is particularly difficult if design decisions are possible with little effort (Collingridge, 1980). There are different methods for dual-use assessment, which are based on the assessment of technology consequences (Grunwald, 2002; Liebert, 2011). The methods are scenario-based and application-oriented, and must therefore always be integrated into the specific research or development project in order to be able to exclude the more pessimistic scenario by design adaptations on a case-by-case basis (von Schomberg, 2006).

For software development, it is precisely against the background of the securitization of cyberspace (Hansen & Nissenbaum, 2009), the military endeavour to comprehensively elucidate (Müller & Schörnig, 2006), and the increasing investment in strategic offensive development (Reinhold, 2016) the question of how developers can estimate the risk of misuse of their research and development.

So far, the dual-use debate in computer science has mainly led to cryptography (Vella, 2017) and to the proliferation of spyware through additions to the Wassenaar Agreement in 2013 and 2016 (Herr, 2016). And although software dual-use is becoming a problem again and again as part of weapons modernization (Bernhardt & Ruhmann, 2017; Reuter & Kaufhold, 2018b), empirical case studies on dual-use IT are lacking (Leng, 2013; Lin, 2016). On the one hand, modern software development is characterized by agile and iterative process models such as Extreme Programming and Scrum, in which developers and managers can react flexibly to changes in (customer) requirements (Dingsøyr et al., 2012). Therefore, it is obvious that dual-use potentials need to be checked not only in the initial planning of software, but process-accompanying. On the other hand, the flexibility in using software in different application contexts is the essential challenge for dual-use impact assessment and therefore must be fundamentally different from life sciences (Lin, 2016, 119). The aim is both to minimize risks by non-state actors, and to anticipate the risk of uncontrolled distribution of malware or misunderstandings between states.

Alongside the entrepreneurial analysis of influencers and moods, social media analytics tool are also playing an increasingly important role: On the one hand, they enable the identification of situations of use in social conflicts or crises (Reuter & Kaufhold, 2018a; Reuter et al., 2017), but also imply a particular potential for abuse in the context of cyber espionage (Neuneck, 2017) or (political) persecution. Therefore, the question arises how potential dual-use components and indicators can already be identified in software research and development.

3. REFERENCES

Altmann, J., Bernhardt, U., Nixdorff, K., Ruhmann, I., & Wöhrle, D. (2017). *Naturwissenschaft – Rüstung – Frieden*. (J. Altmann, U. Bernhardt, K. Nixdorff, I. Ruhmann, & D. Wöhrle, Eds.) (2nd ed.). Wiesbaden. https://doi.org/10.1007/978-3-658-01974-7

Bernhardt, U., & Ruhmann, I. (2017). Informatik. In J. Altmann, U. Bernhardt, K. Nixdorff, I. Ruhmann, & D. Wöhrle (Eds.), *Naturwissenschaft – Rüstung – Frieden* (pp. 337–448). https://doi.org/10.1007/978-3-658-01974-7

Carr, J. (2013). The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*, *69*(5), 32–37. https://doi.org/10.1177/0096340213501373

Collingridge, D. (1980). *The social control of technology*. New York: St. Martins Press.

Dingsøyr, T., Nerur, S., Balijepally, V., & Moe, N. B. (2012). A decade of agile methodologies: Towards explaining agile software development. *Journal of Systems and Software*, *85*(6), 1213–1221. https://doi.org/10.1016/j.jss.2012.02.033

Forge, J. (2010). A note on the definition of "dual use." *Science and Engineering Ethics*, *16*(1), 111–118. https://doi.org/10.1007/s11948-009-9159-9

Grunwald, A. (2002). *Technikfolgenabschätzung - Eine Einführung*. Berlin: Edition Sigma.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Harris, E. D. (Ed.). (2016). *Governance of Dual-Use Technologies: Theory and Practice*. Cambridge MA: American Academy of Arts & Sciences.

Herr, T. (2016). Malware counter-proliferation and the Wassenaar Arrangement. *International Conference on Cyber Conflict, CYCON*, *2016-Augus*, 175–190. https://doi.org/10.1109/CYCON.2016.7529434

Leng, C. (2013). *Die dunkle Seite: Informatik als Dual-Use-Technologie*. Retrieved from https://link.springer.com/content/pdf/10.1007%2Fs00287-012-0675-7.pdf

Liebert, W. (2011). Wissenschaft und gesellschaftliche Verantwortung. In M. Eger, B. Gondani, & R. Kröger (Eds.), *Verantwortungsvolle Hochschuldidaktik* (pp. 15–34). Berlin: Lit.

Liebert, W., Englert, M., & Pistner, C. (2009). *Kernwaffenrelevante Materialien und Präventive Rüstungskontrolle : Uranfreie Brennstoffe zur Plutoniumbeseitigung und Spallationsneutronenquellen*. *Deutsche Stiftung Friedensforschung*.

Lin, H. (2016). Governance of Information Technology and Cyber Weapons. In E. D. Harris (Ed.), *Governance of Dual-Use Technologies: Theorie and Practice* (pp. 112–157). American Academy of Arts & Sciences.

Müller, H., & Schörnig, N. (2006). *Rüstungsdynamik und Rüstungskontrolle: Eine exemplarische Einführung in die Internationalen Beziehungen*. Baden-Baden: Nomos.

NATO. Warsaw Summit Communiqué (2016). Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Neuneck, G. (2017). Krieg im Internet? Cyberwar in ethischer Reflexion. In I.-J. Werkner & K. Ebeling (Eds.), *Handbuch Friedensethik* (pp. 805–816). Wiesbaden. https://doi.org/10.1007/978-3-658-14686-3_58

Oltmann, S. (2015). Dual use research: investigation across multiple science disciplines. *Science and Engineering Ethics*, *21*(2), 327–341. https://doi.org/10.1007/s11948-014-9535-y

Reinhold, T. (2016). Cyberspace als Kriegsschauplatz? Herausforderungen für Völkerrecht und Sicherheitspolitik. Retrieved January 25, 2017, from http://www.bpb.de/apuz/232966/cyberspace-als-kriegsschauplatz?p=all

Reuter, C., & Kaufhold, M.-A. (2018a). Fifteen Years of Social Media in Emergencies: A Retrospective Review and Future Directions for Crisis Informatics. *Journal of Contingencies and Crisis Management (JCCM)*, *26*(1), 41–57. https://doi.org/10.1111/1468-5973.12196

Reuter, C., & Kaufhold, M.-A. (2018b). Informatik für Frieden und Sicherheit. In C. Reuter (Ed.), *Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement* (pp. 573–595). Wiesbaden, Germany: Springer Vieweg. https://doi.org/10.1007/978-3-658-19523-6_28

Reuter, C., Kaufhold, M.-A., Spielhofer, T., & Hahne, A. S. (2017). Social Media in Emergencies: A Representative Study on Citizens' Perception in Germany. *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing*, *1*(2), 1–19. https://doi.org/10.1145/3134725

Tucker, J. B. (2012). Innovation, Dual Use, and Security : Managing the Risks of Emerging Biological and Chemical Technologies. Cambridge.

Vella, V. (2017). Is There a Common Understanding of Dual-Use ?: The Case of Cryptography. *Strategic Trade Review*, *3*(4), 103–122.

von Schomberg, R. (2006). The Precautionary Principle and Its Normative Challenges. In E. Fischer, J. Jones, & R. von Schomberg (Eds.), *Implementing the Precautionary Principle: Perspectives and Prospects* (pp. 19–42). Edward Elgar: Cheltenham.

Varieties of Cybersecurity? The Institutional Foundations of Protecting Critical Infrastructures

MORITZ WEISS AND FELIX BIERMANN

GLOBAL GOVERNANCE AND PUBLIC POLICY, LUDWIG MAXIMILIAN UNIVERSITY OF MUNICH

[#6-PAPER]

1. GOVERNANCE, ACTORS AND CYBERSECURITY?

Studying cybersecurity implies investigating the interaction of technological determinants with the social world. Cyberspace is a material structure and, at the same time, an information environment operated and shaped by humans. In other words, it is “a ‘virtual’ layer of information riding on a physical layer of hardware” (Betz and Stevens, 2011: 37). The material side links it to territorial boundaries and thus to political authority (laws, property rights), whereas the information facet expands beyond territorially defined political organization (Lambach, 2019: 3). However, the organization of political authority over cyberspace is constantly evolving and inherently complex (Boeke, 2018: 3). What is even more, the interaction between an ever-greater number of actors makes spatial and temporal distances collapse. Attribution problems multiply and become more acute (Rid & Buchanan, 2014). It is thus essentially contested who makes for what reasons decisions on cybersecurity that always involve distributive consequences for societies. In other words, who are the key actors of securing cyberspace?

First, the state as manager of political authority (Genschel & Zangl, 2014) is increasingly committed to make decisions on cybersecurity and has recently enhanced its capacities to do so (Weiss & Jankauskas, 2019). The most intense efforts are clearly observable in the United States, China and, partly, Russia (Lindsay, 2015). Yet, states also need to draw on expertise of third parties, which are, however, often hard to control. Thus, the actor constellation within cyberspace is populated by two further powerful groups. Second, transnational organizations have a significant say in cyberspace. In contrast to postal systems or telecommunications, which are predominantly addressed within the International Telecommunication Union (ITU), cyberspace is not organized around one specialized (inter-state) organization of the United Nations. Instead, transnational organizations exercise authority with respect to specific functions (Glen, 2014). For instance, the Internet Assigned Numbers Authority (IANA) regulates domain names, IP addressing, and other Internet protocol resources. Meanwhile, it operates as part of the Internet Corporation for Assigned Names and Numbers (ICANN), which has evolved as an independent non-profit organization that has transitioned its functions to the global multi-stakeholder community instead of being a U.S. government agency. Last, but definitely not least, private actors in general and corporate firms, in particular, are the protagonists in constructing, operating and partly protecting this governance setting (Choucri, 2012: 40; Healey, 2013). For instance, the private sector controls about 90 percent of the critical infrastructure in the United States (U.S.) (Singer and Friedman, 2014: 15).

Against the backdrop of this actor constellation, our paper will focus on governance arrangements between, on the one hand, governments, and the latter group, on the other. More specifically, we seek to find out how national institutions shape the way that governments employ private actors to protect their critical infrastructures.

2. GOVERNMENTS AND CYBERSECURITY?

Governments' approaches to cybersecurity have been far from uniform. To the contrary, we observe considerable variation across states – ranging from (i) hierarchical capacity-building, (ii) the establishment of public-private partnerships (PPP), and (iii) a complete reliance on private actors. The main criterion on how to distinguish between these approaches is the extent to which a government exercises hierarchical authority over specific cybersecurity policies. In other words, does a government choose a state-driven (top-down) or operator-driven (bottom-up) approach? First, when the state literally steps in by creating additional capacity, the beneficiaries of the new technologies – mostly private actors – hardly bear the society-wide risks (Nye, 2017). State control is primarily preserved. Second, public-private partnerships are mostly an exchange relationship between the state and private actors; yet, they often lack performance, when they are unable to accommodate diverging interests (Carr, 2016). Finally, the provision of cybersecurity may also be outsourced to private actors, yet regulated by governments so that private actors carry the burden of protection and possibly the compensation for damage. Their competence becomes indispensable for governments, the longer they rely on these actors.

In our prior research, we found one predominant pattern of how most states sought to secure cyberspace (Weiss & Jankauskas, 2019). The nature of the cybersecurity problem induced the choice of more or less hierarchical control. While the logic of national security led governments to maintain close control over the defense against military attacks (i.e., threats), functional imperatives impelled them to mobilize third parties in order to address the diffuse cyberspace vulnerabilities (i.e., risks). Beyond this general pattern, however, another finding was similarly relevant; yet so far largely ignored. Within one domain, we found substantial variation between states: government responses to protect critical infrastructure vary and thus remained a lacuna. Some states employed hierarchical instruments with state agencies in charge, while others provided more leeway to private actors. Thus, our contribution to SCIENCE · PEACE · SECURITY '19 will ask why some governments protect critical infrastructures through hierarchical control, whereas others through softer forms of inducements?

3. WHAT DRIVES VARIETIES OF CYBERSECURITY?

Given similar challenges, but varying responses, we depart from the premise that domestic differences may account for the observable variation. Therefore, the coordination between the government and private actors is shaped by institutional foundations rather than by technological determinants. We argue that a comparative political economy and thus distinct types of institutional settings explain how governments design the protection of critical infrastructures. In an institutional setting, all stakeholders apply typical strategies, follow routine approaches to address challenges and share the same decision-making rules, so that stable expectations about future behavior are established. We suggest that different coordination mechanisms lead to comparative advantages, which generate a distinct logic of action within the national cybersecurity sector (De Vore & Weiss, 2014).

The extent of hierarchical control that governments exercise in their protection of critical infrastructures depends on the existence of formal and informal institutions that provide information for coordination. Our paper distinguishes between two ideal-typical institutional settings that we will apply to explore the United Kingdom and France respectively. While the UK's market- and contract-based institutions suggest non-hierarchical control mechanisms, strategic coordination and informal adjustments shape a more prominent role for the traditional national security state in France (Weiss, forthcoming). Thus, we expect a more bottom-up approach by the UK and, at the same time, a top-down approach in France. In both cases, however, we suggest that the distinct opportunities provided by the varying institutional settings generate incentives and routine practices, which are, in turn, assumed to shape a government's approach to providing cybersecurity. These theoretical suggestions are substantiated by an empirical exploration of the liberal United Kingdom and dirigiste France and how each of them sought to protect its critical infrastructure since the 2010s.

4. THE PROTECTION OF CRITICAL INFRASTRUCTURES IN THE UNITED KINGDOM AND FRANCE

What both the United Kingdom and France have in common, is their use of an operator-driven ("bottom - up") approach to identifying threats to critical infrastructures. In contrast to a top-down approach, governments have not taken a leading role in defining and prioritizing critical services. Instead, they have delegated this responsibility to private operators of critical infrastructures, whom they have identified as stakeholder-operators of critical infrastructure, also known as Vital Operators (VOs). These VOs are requested to identify and evaluate critical services and systems. In both the UK and France, the responsibility is assigned to the relevant VOs by a responsible government body, such as the Centre for the Protection of National Infrastructure (CPNI) for the UK and the French Network and Information Security Agency (ANSSI) (Breznitz, 2006).

In addition, the UK and France are involved in the same international institutions, such as the informal internet governance initiative Meridian Forum for Global Critical Infrastructure Protection. The latter is a forum for trust-building and consultation of more than 50 governments and global organizations like the United Nations Educational, Scientific and Cultural Organization (United Nations Institute for Disarmament Research, 2013). In a similar vein, both countries have been members of the European Union (EU) and thus transposed the directive on security of network and information systems NIS) into national laws (European Parliament and Council, 2016). The latter's objective is to outline the minimum essential information service areas (e.g.

traditional critical infrastructure operators, such as energy, health, water; plus, digital service providers, such as online marketplaces, online search engines and cloud computing services). Despite these commonalities, differences between the UK and France prevail.

The United Kingdom's approach to protecting critical infrastructures has been heavily influenced by the role model of the United States (esp. their increasing privatization and PPPs). For instance, the UK increasingly employed 'supervisory control and data acquisition systems' (SCADA systems), which allow for more central and remote control of critical infrastructure. Yet, they were also highly vulnerable, when they became connected to the internet (Carr, 2016: 45–53). The main challenge of private-sector involvement is that private owners of critical infrastructure accept responsibility for securing their systems only to the point that it is profitable. This implies that private owners tend to secure the critical infrastructure only to the extent that the cost of dealing with an outage promises to cost more than preventing it (Carr, 2016: 57). In 2015 the UK's government allocated £650 million to the Centre for the Protection of National Infrastructures (CPNI) to implement the National Cyber Security Programme. Of this funding, 20 percent went to public and private critical cyber infrastructure, which are used by the CPNI to provide guidance to critical infrastructure owners on cyber threats and operates information exchanges to facilitate public-private information-sharing on threats and protective measures (United Nations Institute for Disarmament Research, 2013: 50). In other words, private actors play a very important role in the UK's protection of critical infrastructures.

By contrast, France's government agency, called the French Network and Information Security Agency (ANSSI), is predominantly in charge of coordinating various actors responsible for cyberspace (Avant & Westerwinter, 2016). With its regulatory framework for Critical Infrastructures Information Protection (CIIP law), France has presented a policy to address the vulnerabilities generated by a dependence on a public-private partnership. The CIIP was passed into law in December 2013 and applies to "more than 200 public and private operators". Four main measures were introduced with its implementation: it obliged the operators to notify their cyber incidents; it set minimal security standards; it created a legal basis for the inspection of the operators to test their cybersecurity preparedness; and it laid the groundwork for more extreme measures "in the case of a major crisis, declared by the Prime Minister". The goal was to reduce the risk of potentially successful cyberattacks by exploitation of critical infrastructures. This effort was led and implemented by ANSSI. It directly reports to the Secretary General for Defense and National Security and is hierarchically a government agency (Weiss & Jankauskas, 2019). Moreover, the government has defined 12 vital sectors which are divided in three main areas as follows: the state sectors (Public Services, Military Operations, Judicial Functions, Space and Research), the civil protection sectors (Health, Water Management, Food) and lastly the areas of economic and social life of the nation (Energy, Electronic communications, Audiovisual and Information Systems, Transport, Economy, Industry). In turn, through the establishment of relevant mandates, the government defines a list of Vital Operators, whereby each operator is related to one critical sector (United Nations Institute for Disarmament Research, 2013: 21–22). In other words, the French government plays a more prominent role when it comes to organizing the protection of critical infrastructures.

5. CONCLUDING REMARKS

Our paper will start by theorizing the actor constellations in cyberspace. Subsequently, we will conceptualize how governments develop varying strategies

for protecting critical infrastructures. Our objective is to explain this variation by building on the institutional foundations of domestic political economies. This will provide a framework for approaching the different degrees of hierarchical control in the United Kingdom and France. The preceding section has already indicated some of the differences, which we will further explore in our paper. While the UK builds more strongly on public-private partnerships, France insists on a relatively strong role for state institutions.

We seek to make three contributions to scholarship. First, we close a gap in the literature on how varying governance responses to similar disruptive technologies are based on nationally predominant institutional settings. Second, we supplement our research program that has stressed the problem structure to shape the governance design of securing cyberspace by addressing the theoretically indeterminate governance of critical infrastructures. The integration of an intervening variable, varieties of institutional foundations, accounts for those instances, for which the initial distinction between risks and threats indicated rather than explained the choice of a governance design. Third, we seek to transfer theoretical concepts successful in explaining variation of traditional industries to the new digital economy. This will ultimately expand the scope of these theoretical approaches.

REFERENCES

Avant, D.D. and Westerwinter, O. (eds) (2016) The new power politics: Networks and transnational security governance, New York, NY: Oxford University Press.

Betz, D.J. and Stevens, T. (2011) Cyberspace and the state: Toward a strategy for cyberpower, Abingdon: Routledge.

Boeke, S. (2018) ‘National cyber crisis management: Different European approaches’, Governance 31(3): 449–64.

Breznitz, D. (2006) ‘Innovation-Based Industrial Policy in Emerging Economies? The Case of Israel's IT Industry’, Business and Politics 8(3).

Carr, M. (2016) ‘Public-private partnerships in national cyber-security strategies’, International Affairs 92(1): 43–62.

Choucri, N. (2012) Cyberpolitics in International Relations, Massachusetts Institute of Technology: The MIT Press.

De Vore, M.R. and Weiss, M. (2014) ‘Who’s in the cockpit? The political economy of collaborative aircraft decisions’, Review of International Political Economy 21(2): 497–533.

European Parliament and Council (2016) 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: NIS Directive.

Genschel, P. and Zangl, B. (2014) ‘State Transformations in OECD Countries’, Annual Review of Political Science 17(1): 337–54.

Glen, C.M. (2014) ‘Internet Governance: Territorializing Cyberspace?’, Politics & Policy 42(5): 635–57.

Healey, J. (2013) A Fierce domain: Conflict in cyberspace, 1986 to 2012, Washington, D.C. Cyber Conflict Studies Association.

Lambach, D. (2019) ‘The Territorialization of Cyberspace*’, International Studies Review 1(1): 19, doi:10.1093/isr/viz022.

Lindsay, J.R. (2015) ‘The Impact of China on Cybersecurity: Fiction and Friction’, International Security 39(3): 7–47.

Nye, J.S. (2017) ‘Deterrence and Dissuasion in Cyberspace’, International Security 41(3): 44–71.

Rid, T. and Buchanan, B. (2014) ‘Attributing Cyber Attacks’, Journal of Strategic Studies 38(1-2): 4–37.

Singer, P.W. and Friedman, A. (2014) Cybersecurity and cyberwar: What everyone needs to know, Oxford: Oxford University Press.

United Nations Institute for Disarmament Research (2013) ‘The Cyber Index: International Security Trends and Realities’, 2013, New York and Geneva: United Nations Institute for Disarmament Research.

Weiss, M. (forthcoming) ‘From Wealth to Power? The Failure of Layered Reforms in India’s Defense Sector’, Journal of Global Security Studies.

Weiss, M. and Jankauskas, V. (2019) ‘Securing Cyberspace: How States Design Governance Arrangement’, Governance 32(2): 259–75.

Threat Intelligence Application for Cyber Attribution

THEA RIEBE, MARC-ANDRÉ KAUFHOLD, TARUN KUMAR, THOMAS REINHOLD AND CHRISTIAN REUTER

SCIENCE AND TECHNOLOGY FOR PEACE AND SECURITY (PEASEC), TECHNISCHE UNIVERSITÄT DARMSTADT

[#7-PAPER]

ABSTRACT

Attribution consists of technical, legal and politically defined processes. However, the international community has not yet defined processes unilaterally, even though the UN GGE has proposed to address the increase of cyber operations. Taking existing threat exchange standards into account, this paper presents an approach to support efforts for more effective attribution by developing a platform with the common open source threat exchange formats STIX and MEAC. Furthermore, the platform is evaluated in terms of usability.

1. ATTRIBUTION OF ATTACKS IN CYBER SPACE

As in criminal courts, attribution is only a question of a degree of certainty, combining social and technical indicators in a legitimizing process (Davis et al., 2017; Rid & Buchanan, 2015). Following the recommendations of the UN Group of Governmental Experts in 2013, the UN members agreed that legal and technical attribution needs to be addressed as a key challenge to be able to act on harmful operations through the Security Council (Wolter, 2013). However, the details on implementing a unilaterally supported process for legal attribution is still highly controversial between key actors, such as the USA, Russia and China.

Cyber attribution has no universally accepted definition, various scholars interpret it differently. For example, Davis et al. claim that "the public attribution of a malicious cyber incident consists of identifying the responsible party behind the activity" (2017, V). For Wheeler & Larsen, attribution is "determining the identity or location of an attacker or an attacker’s intermediary" (Wheeler & Larsen, 2003, 1). In contrast, Rid & Buchanan state that "attribution is the art of answering a question as old as crime and punishment: who did it?" (2015, 3). Despite these variations, the common intent is to identify the attacker responsible for a malicious activity. The process of attribution not only helps to identify the motivation behind an attack but to learn about the technology involved in executing the attack (Davis et al., 2017; Rid & Buchanan, 2015). Attribution can thus be considered as the basis for acting against perpetrators. Furthermore, the process of attribution helps the affected entity to detect vulnerabilities that were exploited by the threat actor and to come up with preventive measures to strengthen its defence.

Technical attribution is defined as determining the identity or origin or both of an attacker or any other intermediaries that may or may not be willingly part of the attack (Hunker et al., 2008). Cyber attribution is complex and poses various problems: a) attribution cannot be performed with the strict use of technology only, b) attribution is not highly desirable in all situations because it would destroy the internet as a means of open and free communication and c) cyberattacks are not restricted to a particular region; they can span across regions, and d) the source of attack my not be the actual initiator. Hence cooperation from different jurisdictions is required with respect to attribution techniques (Hunker, 2008). Even though there are plenty of government entities, private firms and research organizations with sufficient capacity to conduct investigations for cyber attribution do not have a standardized methodology for conducting their research and use their own taxonomies for their findings (Davis, 2017).

Technical attribution paves the way for compliance with the legal framework and can be done without the context of International Humanitarian Law. Furthermore, in technical attribution, the perpetrator can have both criminal and political motives. Even though IT forensics and political attribution within the international community would use the same technology and perpetrators might even use each other’s exploits as in the example of WannaCry and NotPetya (Committee on Oversight and Government Reform, 2016), the debates are led separately. Notable examples include: the Stuxnet worm unleashed on an Iranian nuclear enrichment facility (Karnouskos, 2011), the breach into the U.S. Office of Personnel Management (OPM) that led to the theft of tens of millions of highly sensitive personnel records and the WannaCry ransomware attack. The threat actors responsible in each of these cases were identified by a combination of social and technical indicators using threat intelligence (Saalbach, 2019). Methods of threat intelligence become increasingly advanced. Nevertheless, they lack international standardization.

However, the sharing of threat-related information can leverage the collective knowledge of that sharing community and thus improve their security posture and defensive agility. In this regard, standardized threat exchange formats can play an important role, as well-structured threat information in line with shared standards can be used to facilitate threat information processing. Moreover, it is helpful in understanding the tactics, techniques and procedures of an attack (Johnson et al., 2016).

Attribution in cyberspace involves examining and interpreting hard to compare evidence (Davis, 2017). Despite the interpretive difficulties associated with cyberattack attribution, a variety of experts in cyber forensics agreed upon several common indicators that provide a basis for the assessment of responsibility. Indicators can be technical, such as text strings, command and control infrastructures and malware, but also political, such as the political interest in such a compromise, as in the example of Stuxnet. Other indicators are found through an investigation into all-source intelligence, socio-cultural and economic areas (Davis II John S, 2017).

The goal of this paper is to conceptualize a solution for producing threat intelligence and support credible attribution. This will be followed by an implementation of the proposed solution and an evaluation of results. The following research question will be addressed: **How can threat exchange platforms help to improve cyber attribution?**

2. CYBER THREAT INTELLIGENCE AND EXCHANGE FORMATS

Cyber threat intelligence is required to facilitate cyber attribution. To begin with, a cyber threat is defined as “any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.” (ENISA, 2009). Hence, an individual or a group posing a threat are considered to be threat actors. Threat information is to be understood as any information related to a threat which might be helpful to an organization that wants to protect itself against a threat or detect the activities of an actor. Major types of threat information include indicators, TTPs (tactics, techniques & procedures), security alerts, threat intelligence reports and tool configurations. Consequently, threat intelligence can be described as "threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes" (Johnson, 2016).

There are plenty of different threat exchange formats, some are open and other are closed source, which can be of use for threat intelligence and cyber attribution. In this platform STIX (Structured Threat Information Expression) and MAEC (Malware Attribute Enumeration and Characterization) are combined to be able to document the relationship between malware and threat information, that is crucial for the quality of technical attribution. **STIX** (OASIS Open, 2019) is the most popularly used standard and is able to model attack patterns, campaigns, identifies, indicators, intrusion sets, malware, reports, threat actors, tools and vulnerabilities. Even though there are plenty of other standards to describe specific aspects of a threat/malware, STIX was developed with a notion that there should be one standard which describes every aspect of a threat. Furthermore, **MAEC** captures detailed information about malware samples and is used by malware analysts to model behavior, collections, malware actions, malware families and malware instances. In contrast, STIX captures cyber threat information that includes only basic information about malware, but it proves to be applicable to a much wider audience.

3. REQUIREMENTS AND DESIGN OF A THREAT INTELLIGENCE PLATFORM

Based on a narrative literature review on cyber attribution, cyber threat intelligence, standards for threat exchange and existing threat intelligence platforms, which focused on scientific publications and technical documentations, we identified limitations as well as suggested improvements for threat intelligence platforms. Based on this, a set of 15 technical requirements was identified and subsumed into three design goals:

- **User Interface and API**: The interface should be responsive and easy to use with some basic authentication features. The API should give the possibility of adding and editing threat information such as malware samples.
- **Visualization**: The prototype should be able to visualize a cyberattack in the form of graphs, in which the plotted elements are nothing but the threat actors, their TTP’s, malware used, vulnerabilities exploited, and the correlation amongst them. By this, the correlation patterns can be known easily.
- **Use of Standards**: The prototype should be developed by implementing the standards STIX and MAEC only, which is the main priority and does not involve any customization.

Based on the initial set of requirements, we envision a human-centred development approach. Accordingly, we will implement a first version of the prototype and evaluate the functionality and usability of the prototype, which is intended as one input for the second iteration of prototype development and enhancement. For the evaluation, we plan to use scenario-based walkthroughs followed by semi-structured interviews with at least ten participants. Furthermore, participants will be encouraged to use the think-aloud protocol (Nielsen, 1992) during the walkthrough as it helps in understanding a participant's perception about the application, thereby leading to the discovery of desired functionality, usability issues and user preferences. The evaluation will improve the usability of the platform. However, further research and development on the communication and analysis of threats between states and international organisations need to be done.

4. ACKNOWLEDGEMENTS

This research was funded by the TU Darmstadt FIF-IANUS research project *IT Research of Concern*.

REFERENCES

Committee on Oversight and Government Reform. (2016). *The OPM Data Breach: How the Government Jeopardized Out National Security for More Than a Generation*.

Davis II John S, Benjamin Adam Boudreaux Jonathan William Welburn Jair Aguirre Cordaye Ogletree Geoffrey McGovern Michael Chase. (2017). *Stateless Attribution: Toward International Accountability in Cyberspace | RAND*. *Rand*. Retrieved from http://www.rand.org/pubs/research_reports/RR2081.html

Davis, John S. II, Boudreaux, Benjamin, Welburn, Jonathan William, Ogletree, Cordaye, McGovern, Geoffrey, & Chase, Michael S. (2017). *Stateless Attribution: Toward International Accountability in Cyberspace*. Retrieved from http://www.rand.org/pubs/research_reports/RR2081.html

ENISA. (2009). Glossary.

Hunker, Jeffrey, Hutchinson, Bob, & Margulies, Jonathan. (2008). *Role and Challenges for Sufficient Cyber-Attack Attribution*.

Johnson, Chris, Waltermire, David, & Badger, Lee. (2016). *Guide to Cyber Threat Information Sharing*.

Karnouskos, S. (2011). Stuxnet Worm Impact on Industrial Cyber-Physical System Security. In *Proceedings of the 37th Annual Conference of the IEEE Industrial Electronics Society*. Melbourne, Australia: IEEE.

Nielsen, Jakob. (1992). Evaluating the thinking-aloud technique for use by computer scientists. In H. R. Hartson & D. Hix (Eds.), *Advances in human-computer interaction* (pp. 69–82). New York: Hindawi Publishing Corp.

OASIS Open. (2019). Getting Started with STIX 2.0.

Rid, Thomas, & Buchanan, Ben E. N. (2015). Attributing Cyber Attacks. *The Journal of Strategic Studies*, vol. *38*, iss. 1–2, pp. 4–37. https://doi.org/10.1080/01402390.2014.977382

Saalbach, KLaus-Peter. (2019). Attribution of Cyber Attacks. In C. Reuter (Ed.), *Information Technology for Peace and Security* (pp. 279–304). Wiesbaden: Springer.

Wheeler, David A., & Larsen, Gregory N. (2003). *Techniques for Cyber Attack Attribution*.

Wolter, Detlev. (2013). The UN Takes a Big Step Forward on Cybersecurity. Retrieved from https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity#source

Social Media Misuse – Cultural Violence, Peace and Security in Digital Networks

MARC-ANDRÉ KAUFHOLD AND CHRISTIAN REUTER

SCIENCE AND TECHNOLOGY FOR PEACE AND SECURITY (PEASEC), TECHNISCHE UNIVERSITÄT DARMSTADT

[#8-PAPER]

ABSTRACT

Over the last decade, social media established an enormous impact on modern culture not only for everyday life uses, but also during natural and man-made crises and conflicts. For instance, Facebook was part of the Arabic Spring, in which the tool facilitated the communication and interaction between participants of political protests. However, social media is not only used for good purposes and offers potentials for misuse: fake news manipulate public discourses, cyber terrorism aims to recruit new members and disseminate ideologies, and social bots influence economic as well as political processes. Based on the notions of cultural violence and cultural peace as well as the phenomena of fake news, terrorism, and social bots, this paper outlines countermeasures to facilitate cultural peace and security.

1. INTRODUCTION AND RELATED WORK

Social media are defined as a “group of internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content” (Kaplan & Haenlein, 2010). Besides everyday life uses, such as self-promotion, relationship building, news posting or information searching (Robinson et al., 2017), social media are used by journalists for reporting, analysing and collecting information (Stieglitz et al., 2018), by organizations to monitor customer feedback and sentiment (Kaufhold et al., 2017) but also by citizens and emergency services to respond to crises, conflicts and disasters (Palen & Hughes, 2018). However, social media is not only used for good purposes and offers potentials for misuse, such as the dissemination of fake news or conduction of cyber terrorism (Kaufhold & Reuter, 2019). Sometimes, such misuse is amplified by social bots, which are “computer algorithms which automatically generate content and interact with other people in social media with the aim to imitate and influence their behaviour” (Ferrara et al., 2016). In this paper, we view social media misuse from the perspective of cultural violence.

In peace research, Galtung (2007) differentiates between direct, structural and cultural violence. While direct violence is the most visible form of violence (e.g. injuring or killing people), structural violence is defined as *“unjust economic, social and political conditions and institutions that harm people by preventing them from their basic needs”* (Campbell et al., 2010). Based on this, cultural violence describes *“all aspects of a culture that are used to justify direct or structural violence”* (Galtung, 2007). In his definition, Galtung mentions the six cultural areas of religion, ideology, language, art, empirical and formal science that are prone to cultural violence. Accordingly, Galtung (2007) differentiates direct violence as visible as well as structural and cultural violence as invisible types of violence. By introducing the term of cultural peace, which is understood as the absence of cultural violence (Werkner, 2017, 23), Galtung (2007) enhances the term of peace to the formula: “Peace = Direct Peace + Structural Peace + Cultural Peace”. To achieve cultural peace, actors must overcome attitudes and behavioural patterns that justify the appliance of violence (Werkner, 2017). Furthermore, malicious practices such as account hijacking and malware distribution via social media threaten civil security (Reuter, 2018).

2. Findings

Based on a narrative literature review, we identified characteristics of and measures against fake news, cyber terrorism and social bots within social media.

2.1. Fake News

Fake news can be defined as “news articles that are intentionally and verifiably false and could mislead readers” (Allcott & Gentzkow, 2017). They distinguish fake news from similar phenomena like unintentional reporting mistakes, rumours, conspiracy theories, obvious satire, and more. Similarly, Sängerlaub (2017) defines fake news as intended disinformation and describes three types of fake news: First, there are completely fictitious news which he refers to as fabricated content. Second, manipulated content is based on true information which is manipulated in some respects. Third, misinterpreted content refers to correct information which is quoted out of context or is intentionally misinterpreted by the author.

Gatekeeping	Gatekeeping is the process through which information, including fake news, is filtered for dissemination, e.g. for publication, broadcasting, social media, or some other mode of communication (Barzilai-Nahon, 2009).
Media Literacy	The purpose of media literacy, which is a multi-dimensional process allowing people to access, evaluate and create media, is to help people to protect themselves from the potentially negative effects of (mass) media (Potter, 2010).
Regulation/ Law	Laws may assist in fighting fake news and hate speech by forcing platforms to quickly delete illegal contents though they potentially threaten freedom of speech (Müller & Denner, 2017).
Algorithmic	The algorithmic detection of fake news comprises classification-based, propagation-based and survey-based approaches (Viviani & Pasi, 2017).

Table 2. Measures against fake news in social media

So far, there is no clear answer on how fake news can be approached the best. It is a complex task to identify solutions and responsibilities to prevent individuals and society from possible negative effects. Still, researchers have presented several approaches to detect fake news (Table 1).

2.2. CYBER TERRORISM

Cyber terrorism includes recruiting new members and disseminating ideologies (Reuter, Pätsch et al., 2017). Much research about terrorist organizations and social media deals with terrorist organizations in general or specifically with the so-called Islamic State (IS, ISIS, ISIL, DEASH). Media play a significant role in terrorism: "Without a letter of confession, a farewell video by the assassin or a last posting in the social network a bomb attack would be nothing else than a capital crime. Only through the terrorist communications strategy, the crime turns into a terrorist act." However, terrorists do "not rely on media-makers, themselves became the agent in this game" (Christoph, 2015). And there is a reason for this: "Terrorism can […] only gain in importance if it becomes meaningful on the media level". Therefore, social media offer "the advantage of immersion, which means the merger of medium and message. The credibility of terrorist narrations is strengthened by spreading it about supposedly reliable portals like YouTube" (Christoph, 2015). A variety of different measures to counter terrorism were identified in research (Table 2).

Clarification	Clarification means to try answering to the terrorist propaganda with logic to invalidate it. It is a complete clarification in terms of a statement, which clarifies unknown connections (Reuter, 2017).
Parody/Satire	Parody is a hilarious satirical imitation by distortion and exaggeration. The satire is a genre, which criticizes and stultifies events. Both aim at expressing mockery about serious issues (Reuter, 2017).
Hacking	Hacking refers to illegal activities, like the blocking of accounts and the appeal to the population to report suspected persons as well as legal activities by multiplying parodist media (Reuter, 2017).
Counter-Narratives	A narrative that goes against another narrative. Narratives are compelling storyline which can explain events convincingly and from which inferences can be drawn (Freedman, 2006).

Table 3. Measures against terrorism

2.3. SOCIAL BOTS

Social bots can be defined as *"computer algorithms which automatically generate content and interact with other people in social media with the aim to imitate and influence their behaviour"* (Ferrara, 2016). Their behaviours are already sophisticated as they can establish realistic social networks and produce credible content with human-like patterns (Ferrara, 2016). Amongst others, social bots are used for account hijacking, astroturfing, creation of fake accounts and dissemination of spam (Kaufhold, 2019). To counteract social bots, it is first necessary to identify the respective bot accounts. For this purpose, scholars of social bot detection have developed various approaches (Ferrara, 2016). Social bots may be determined through human engagement or through algorithmic analysis of features and social networks, both complemented by hybrid approaches (Table 3). Both improvements of the human-like behaviour and of detection systems can lead to an arms race similar to that observed for spam.

Crowdsourcing	Crowdsourcing relies on identification of social bots by human actors, following the underlying assumption of human beings as most able to recognize linguistic nuances like sarcasm, humour, or commitment (Wang et al., 2012).
Social Graph Analysis	Graph-based approaches model social networks visually as finite graphs, with nodes illustrating participants of the respective network and edges representing relationships (Yan, 2013).
Feature Analysis	Feature-based approaches execute identification by determining unique characteristics and behaviours of social bots. They are further differentiated between machine learning or entropy approaches (Ramalingam & Chinnaiah, 2018).
Hybrid Approach	Hybrid approaches combine different methods, such as adding features to a graph-based approach, to increase the accuracy of social bot detection (Gao et al., 2015).

Table 4. Approaches for social bot detection

3. Contribution

This paper examined three phenomena of social media misuse that inflict cultural violence and identified countermeasures which potentially improve cultural peace and security in social media. Based on the results, a differentiation of actors (human, machine) and intentions (malicious, positive) is provided in Table 4. Further research is encouraged to examine additional phenomena in social media, such as cultural diversity, and apply a more systematic review of existing misuse potentials and countermeasures to draw a more comprehensive picture.

		Actor	
		Human	**Machine**
Intention	**Malicious**	Fabricated Content, Misinterpreted Content, Manipulated Content, Propaganda, Recruitment	Account Hijacking, Astroturfing, Fake Accounts, Fake Posts, Spam
	Positive	Gatekeeping, Media Literacy, Laws, Clarification, Parody/Satire, Hacking, Counter-Narratives	Crowdsourcing, (Feature, Social Graph, Survey based or Hybrid) Detection Algorithms

Table 5. Actors and intentions for cultural violence and peace.

4. ACKNOWLEDGEMENTS

This research was funded within the research group "KontiKat" (Reuter, Kaufhold et al., 2017) of the German Federal Ministry of Education and Research (BMBF No. 13N14351) and the Collaborative Research Centre MAKI (SFB 1053) of the German Research Foundation. This abstract is a short version of an already published book section (Kaufhold, 2019).

REFERENCES

Allcott, Hunt, & Gentzkow, Matthew. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, vol. *31*, iss. 2, pp. 211–236. https://doi.org/10.1257/jep.31.2.211

Barzilai-Nahon, Karine. (2009). Gatekeeping: A critical review. *Annual Review of Information Science and Technology*, vol. *43*, iss. 1, pp. 1–79. https://doi.org/10.1002/aris.2009.1440430117

Campbell, Patricia J., MacKinnon, Aran S., & Stevens, Christy. (2010). *An Introduction to Global Studies*. Wiley-Blackwell.

Christoph, Stefan. (2015). Funktionslogik terroristischer Propaganda im bewegten Bild. *Journal for Deradicalization*, vol. *Fall/15*, iss. 4, pp. 145–205.

Ferrara, Emilio, Varol, Onur, Davis, Clayton, Menczer, Filippo, & Flammini, Alessandro. (2016). The Rise of Social Bots. *Communications of the ACM*, vol. *59*, iss. 7, pp. 96–104.

Freedman, Lawrence. (2006). *The Transformation of Strategic Affairs*. Routledge.

Galtung, Johan. (2007). *Frieden mit friedlichen Mitteln. Friede und Konflikt, Entwicklung und Kultur*. Münster: Agenda Verlag.

Gao, Peng, Gong, Neil Zhenqiang, Kulkarni, Sanjeev, Thomas, Kurt, & Mittal, Prateek. (2015). SybilFrame: A Defense-in-Depth Framework for Structure-Based Sybil Detection. In *Computing Research Repository*.

Kaplan, Andreas M., & Haenlein, Michael. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, vol. *53*, iss. 1, pp. 59–68. https://doi.org/10.1016/j.bushor.2009.09.003

Kaufhold, Marc-André, & Reuter, Christian. (2019). Cultural Violence and Peace in Social Media. In C. Reuter (Ed.), *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden, Germany: Springer Vieweg.

Kaufhold, Marc-André, Reuter, Christian, Ludwig, Thomas, & Scholl, Simon. (2017). Social Media Analytics: Eine Marktstudie im Krisenmanagement. In M. Eibl & M. Gaedke (Eds.), *INFORMATIK 2017, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik*. Bonn.

Müller, Philipp Dr., & Denner, Nora. (2017). *Was tun gegen “Fake News”?*

Palen, Leysia, & Hughes, Amanda L. (2018). Social Media in Disaster Communication. In H. Rodríguez, W. Donner & J. E. Trainor (Eds.), *Handbook of Disaster Research* (pp. 497–518). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-63254-4_24

Potter, W. James. (2010). The state of media literacy. *Journal of Broadcasting and Electronic Media*, vol. *54*, iss. 4, pp. 675–696. https://doi.org/10.1080/08838151.2011.521462

Ramalingam, Devakunchari, & Chinnaiah, Valliyammai. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. *Computers & Electrical Engineering*, vol. *65*, , pp. 165–177. https://doi.org/https://doi.org/10.1016/j.compeleceng.2017.05.020

Reuter, Christian. (2018). *Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen-und Sicherheitsmanagement*. Springer Vieweg.

Reuter, Christian, Kaufhold, Marc-André, Schorch, Marén, Gerwinski, Jan, Soost, Christian, Hassan, Sohaib S., … Wulf, Volker. (2017). Digitalisierung und Zivile Sicherheit: Zivilgesellschaftliche und betriebliche Kontinuität in Katastrophenlagen (KontiKat). In G. Hoch, H. Schröteler von Brandt, V. Stein & A. Schwarz (Eds.), *Sicherheit (DIAGONAL Jahrgang 38)* (pp. 207–224). Göttingen: Vandenhoeck & Ruprecht.

Reuter, Christian, Pätsch, Katja, & Runft, Elena. (2017). IT for Peace? Fighting Against Terrorism in Social Media – An Explorative Twitter Study. *I-Com: Journal of Interactive Media*, vol. *16*, iss. 2.

Robinson, Tom, Callahan, Clark, Boyle, Kristoffer, Rivera, Erica, & Cho, Janice K. (2017). I FB: A Q-Methodology Analysis of Why People 'Like'' Facebook.' *International Journal of Virtual Communities and Social Networking (IJVCSN)*, vol. *9*, iss. 2, pp. 46–61. https://doi.org/10.4018/IJVCSN.2017040103

Sängerlaub, Alexander. (2017). Deutschland vor der Bundestagswahl: Überall Fake News?!

Stieglitz, Stefan, Mirbabaie, Milad, Ross, Björn, & Neuberger, Christoph. (2018). Social media analytics – Challenges in topic discovery, data collection, and data preparation. *International Journal of Information Management*, vol. *39*, , pp. 156–168. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2017.12.002

Viviani, Marco, & Pasi, Gabriella. (2017). Credibility in social media: opinions, news, and health information—a survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. *7*, iss. 5, pp. e1209-- n/a. https://doi.org/10.1002/widm.1209

Wang, Gang, Wilson, Christo, Zhao, Xiaohan, Zhu, Yibo, Mohanlal, Manish, Zheng, Haitao, & Zhao, Ben Y. (2012). Serf and Turf: Crowdturfing for Fun and Profit. *Arxiv Preprint ArXiv:1111.5654*, pp. 10. https://doi.org/10.1145/2187836.2187928

Werkner, Ines-Jacqueline. (2017). Zum Friedensbegriff in der Friedensforschung. In I.-J. Werkner & K. Ebeling (Eds.), *Handbuch Friedensethik* (pp. 19–32). Springer Fachmedien.

Yan, Guanhua. (2013). Peri-Watchdog: Hunting for hidden botnets in the periphery of online social networks. *Computer Networks*, vol. *57*, iss. 2, pp. 540–555. https://doi.org/10.1016/j.comnet.2012.07.016

Fighting Misinformation on Twitter – the Plugin Based Approach TrustyTweet

KATRIN HARTWIG AND CHRISTIAN REUTER

SCIENCE AND TECHNOLOGY FOR PEACE AND SECURITY (PEASEC), TECHNISCHE UNIVERSITÄT DARMSTADT

[#9-PAPER]

ABSTRACT

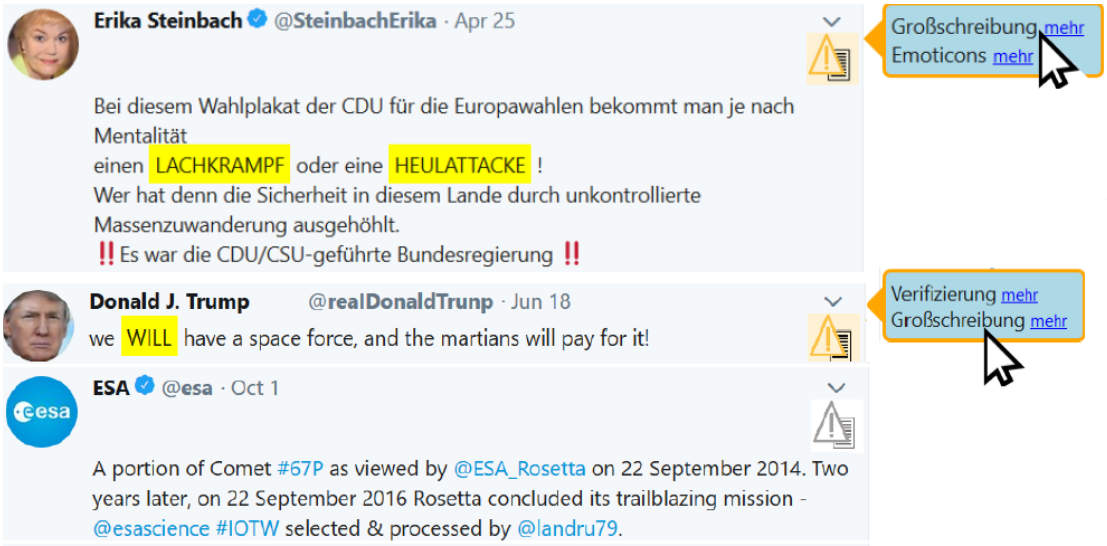
Finding a responsible way to address fake news on social media has become an urgent matter both in political and social contexts. Existing studies focus mainly on how to detect and label fake news. However, approaches to assist users in making their own assessments are largely missing. In this article we present a study on how an indicator-based white-box approach can support Twitter-users in assessing tweets. In a first step, we identified indicators for fake news that have shown to be promising in previous studies and that are suitable for our idea of a white-box approach. Building on that basis of indicators we then designed and implemented the browser-plugin TrustyTweet, which aims to assist users on Twitter in assessing tweets by showing politically neutral and intuitive warnings without creating reactance. Finally, we present the findings of our evaluations carried out with a total of 27 participants, which result in further design implications for approaches to assist users in dealing with fake news.

1. INTRODUCTION AND RELATED WORK

One of the big current questions in society and politics is how to deal with fake news. Studies have shown that it is essential to provide tools to support users on social media. Previous research has focused particularly on machine learning algorithms to detect and label fake news. For instance, Gupta et al. have designed a browser-plugin to automatically assess the credibility of contents on Twitter (Gupta, Kumaraguru, Castillo, & Meier, 2014). Further approaches (e.g. Fake News AI, http://www.fakenewsai.com) use machine learning techniques as well. On the other hand, some approaches are based on whitelists or blacklists (e.g. B.S. Detector, http://bsdetector.tech). When using black-box approaches, it is not possible to reason why a specific decision was made. Therefore, it runs the risk of creating reactance. We agree with other studies that it is necessary to improve media literacy to help users dealing with fake news sustainably (Müller & Denner, 2017; Stanoevska-Slabeva, 2017). Hence, white-box approaches are a crucial strategy. However, all presented applications and approaches are based on black-box methods. Even though the smartphone application Fake News Check (https://www.neue-wege-des-lernens.de/projekte/fake-news-check) provides the user with transparent reasons why contents might be fake, it does not automatically check for indicators and it comes with a big effort.

2. Our Approach

In our work, as described by Hartwig and Reuter (2019), we intend to contribute to the scientific discussion by theoretically exploring the potential of an indicator-based white-box approach to assist users on Twitter and more practically to design, implement and evaluate a consistent browser-plugin as an artefact regarding to the design science approach. The plugin includes a warning concerning six easily comprehensible and politically neutral indicators for fake news, detailed information about each indicator and a configuration-feature for personalization.



Erika Steinbach @SteinbachErika · Apr 25

Bei diesem Wahlplakat der CDU für die Europawahlen bekommt man je nach Mentalität
einen LACHKRAMPF oder eine HEULATTACKE !
Wer hat denn die Sicherheit in diesem Lande durch unkontrollierte Massenzuwanderung ausgehöhlt.
‼️ Es war die CDU/CSU-geführte Bundesregierung ‼️

Großschreibung mehr
Emoticons mehr

Donald J. Trump @realDonaldTrump · Jun 18

we WILL have a space force, and the martians will pay for it!

Verifizierung mehr
Großschreibung mehr

ESA @esa · Oct 1

A portion of Comet #67P as viewed by @ESA_Rosetta on 22 September 2014. Two years later, on 22 September 2016 Rosetta concluded its trailblazing mission - @esascience #IOTW selected & processed by @landru79.

Figure 1. Exemplary output of TrustyTweet for three tweets.

3. Contribution

We aimed to answer the following first research question: *How can we provide a transparent, politically neutral and objective assisting tool for users of social media?* Taking into account the empirical findings, we suggest that our indicator-based white-box approach can be considered suitable when applying the following five design implications: personalization to enhance autonomy, transparent and objective information, unambiguousness of warnings, personalized noticeability and minimization of false alarms. Moreover, we intended to answer the second research question: *Does a white-box approach counteract reactance and encourage a learning effect?* Our findings reveal that our white-box approach is promising to assist users on social media without creating reactance but encouraging a learning effect. Therefore, it can be considered a suitable alternative or supplement to black-box approaches.

4. Acknowledgements

This extended abstract is a summary of our previous published paper (Hartwig & Reuter, 2019).

REFERENCES

Gupta, A., Kumaraguru, P., Castillo, C., & Meier, P. (2014). TweetCred: Real-Time Credibility Assessmentof Content on Twitter. International Conference on Social Informatics, pp. 228-243.

Hartwig, K., & Reuter, C. (2019). TrustyTweet: An Indicator-based Browser-Plugin to Assist Users in Dealing with Fake News on Twitter. Proceedings of the International Conference on Wirtschaftsinformatik (WI).

Müller, P., & Denner, N. (2017). Was Tun Gegen „Fake News“? Friedrich Naumann Stiftung Für die Freiheit.

Stanoevska-Slabeva, K. (2017). Teaching Social Media Literacy with Storytelling and Social Media Curation. Twenty-third Americas Conference on Information Systems.

Responsible Data Usage in Smart Cities – Privacy in Everyday Life vs. Reacting to Emergencies

GINA MARIA SCHMIDBAUER-WOLF, FRANZISKA HERBERT AND CHRISTIAN REUTER

SCIENCE AND TECHNOLOGY FOR PEACE AND SECURITY (PEASEC), TECHNISCHE UNIVERSITÄT DARMSTADT

[#10-PAPER]

ABSTRACT

Smart cities want to provide a better life to their citizens, e.g. regarding health care, infrastructure, better safety and security. This can be achieved by using more and new technology and by interconnecting and analysing new and existent devices. Thus, public spaces and buildings will be equipped with more interconnected input and output modalities. This ongoing technologization of public spaces creates opportunities for making everyone's life more secure, while at the same time everyone's personal privacy is endangered. So how is this balancing act tackled and dealt with right now? What fears do citizens have regarding their security as well as their privacy? This paper provides first insights into the topic privacy in smart cities regarding that smart cities need data which can be provided by and of people. The paper raises the question if collecting people's data, and thus enabling smart cities, is ethical and if not, how it can be assured to be ethical.

1. WHAT IS A SMART CITY?

There exist different definitions of smart cities. While for some a smart city is a technical and infrastructural advanced and sustainable city (Baig et al., 2017; Khan et al., 2018), others see more implications, such as sustainability not only towards resources but also towards citizens as well as the citizen's wellbeing in form of healthcare, education and more (Clever et al., 2018; K. Zhang et al., 2017). Smart cities need technologies and more important an interlinking between these technologies, using e.g. the data of cars (Elmaghraby & Losavio, 2014), drones (Khan, 2018; Vattapparamban et al., 2016) or public space camera systems (H. Zhang et al., 2019). But in order to be smart and not only technologized, the socio-economic implications, which result from this technologization need to be examined (Allam, 2019) for cities to be truly smart and sustainable. Eckhoff and Wagner (2018) see smart cities as cities which "integrate information technology into every aspect of city life". They consider the wellbeing of their citizens just as one of the goals of smart cities while seeing economic growth as the other goal and thus highlight economical aspects which may be hidden behind the citizen's wellbeing in other definitions.

2. Privacy and Smart Cities

Since data needs to be collected in a smart city in order to be "smart", e.g. triggering emergency reactions, the data's and thus people's privacy needs to be taken into consideration. Elmaghraby et al. (2014, 1) phrase it as following: "Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go hand-in-hand with the continuous security challenges." They also see three general areas to be secured: "*(1) The ''privacy'' and confidentiality of the information (2) The integrity and authenticity of the information and (3) The availability of the information for its use and services".* When thinking about data usage in smart cities in emergency situations these three qualities need to be met, thus saying that privacy and IT security go hand in hand (Bartoli et al., 2011; K. Zhang, 2017). People's willingness to make their data available to smart cities and their privacy concerns depend on what they think their data is used for and who has access to it (van Zoonen, 2016). Hence, the citizens trust into their government is needed in order to implement an e-government which is able to help its citizens (Manda & Backhouse, 2016) and thus the "need for transparency and inclusivity in urban processes and systems" (Allam, 2019) needs to be taken into account.

It is evident that the data collected in a smart city can reveal habits or acts of people which they do not want to be known by anyone but themselves (Eckhoff, 2018; Elmaghraby, 2014) and the issue about smart cities is that their citizens are not able to opt out of being recorded or none of their data being used which makes smart cities a great danger for its citizens (Eckhoff, 2018). Existing Patterns and Guidelines which enforce the implementation of privacy such *as privacy by design* (Eckhoff, 2018) or *privacy requirements engineering* (Eckhoff, 2018) should be used when implementing and developing smart city applications such as existing privacy enhancing technologies. Martínez-Ballesté et al. (2013) examine how yet existing privacy enhancing technologies can be used in order to preserve people's privacy in smart cities ("*statistical disclosure control (SDC) , private information retrieval (PIR), privacy-preserving data mining (PPDM), location privacy, anonymity and pseudonyms, privacy in radio frequency identification (RFID), and privacy in video surveillance*"). One option to protect people's privacy would be to prevent "data over collection", meaning, that only the data needed by an application is collected by an application and/or available to this application (Li et al., 2016). This approach results in less analysable personal data, since less data is collected. But even if privacy is such an important and drastic topic which needs to be discussed when talking about smart cities, privacy seems to be no factor for measuring the "smartness" of a city (Eckhoff, 2018).

3. Using Smart City Data in Case of an Emergency Situation

Smart cities could provide different services and facilitation to people. Opposed to this benefits risks and challenges – e.g. regarding people's privacy – need to be taken into account. One smart city scenario could be to monitor public areas to make them safer. This could e.g. happen through the use of video surveillance or the use of thermographic cameras. Depending on which monitoring technique is used and how gained data is used, the safety and security of these places may be increased but also eventually the privacy of people being there is reduced. Also, data produced by people's devices, such as smartphones, could be used and analyzed without further surveillance devices. Using this data provided by people being in a smart city could yield towards a smart safe city, with *safe city* being a city "safe from both external and internal threats to their well-being" (Allam, 2019). This protection of people in a city would fulfil the need for a city to be smart regarding the improvement of citizen's health and life conditions. It could also enable efficient use of resources in everyday life but also in crisis, emergency or safety critical situations and thus could enable an easier recovery from disastrous events. In short, ideally smart safe cities could prevent, reduce and help but also rebuild after disastrous or crisis events.

While data minimization indeed serves people's privacy, additional data could also be used in people's favour for some cases, such as emergency situations. Nonetheless, not every type of data can or shall be used for an emergency situation. Therefore, we conclude it would be best to know beforehand which data can be used in emergency situations and collect just this data. The question arises how this data should be collected best, when every app should only read and collect the data it really needs. Is it still possible to implement emergency and security applications as ubiquitous city enhancements under these circumstances which use data gained by third parties? Or must specific devices be implemented for this case which need this data and hence are allowed to collect this specific data? Can systems which don't need to be approved, activated or acquired by every affected person (e.g. video surveillance-based systems) operate and at the same time respect people's privacy? Is it even okay to want to "protect" every person in a city or is this skipping of the people's real consent to this – neither an assumed consent, nor an enforced consent – even ethical? Are there frameworks for such ethical [1] development and thus usage of surveillance technologies in smart cities?

REFERENCES

Allam, Zaheer. (2019). The Emergence of Anti-Privacy and Control at the Nexus between the Concepts of Safe City and Smart City. *Smart Cities*, vol. *2*, iss. 1, pp. 96–105. https://doi.org/10.3390/smartcities2010007

Baig, Zubair A., Szewczyk, Patryk, Valli, Craig, Rabadia, Priya, Hannay, Peter, Chernyshev, Maxim, … Peacock, Matthew. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*. https://doi.org/10.1016/j.diin.2017.06.015

Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D. (2011). Security and Privacy in your Smart City. *Roceedings of the Barcelona Smart Cities Congress*, vol. *292*, , pp. 1–6. Retrieved from https://pdfs.semanticscholar.org/a8eb/00601cdb94ff6bbfc03118f3fcb7575ba07a.pdf

[1] Clever et al. (2018) propose some ethical challenges and emphasize the need to consider them when developing smart cities but yet no solutions

Clever, Sawyer, Crago, Tyler, Polka, Alex, Al-Jaroodi, Jameela, & Mohamed, Nader. (2018). Ethical Analyses of Smart City Applications. *Urban Science*, vol. *2*, iss. 4, pp. 96. https://doi.org/10.3390/urbansci2040096

Eckhoff, David, & Wagner, Isabel. (2018). Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys and Tutorials*, vol. *20*, iss. 1, pp. 489–516. https://doi.org/10.1109/COMST.2017.2748998

Elmaghraby, Adel S., & Losavio, Michael M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, vol. *5*, iss. 4, pp. 491–497. https://doi.org/10.1016/j.jare.2014.02.006

Khan, Muhammad Asghar, Safi, Engr Alamgir, Khan, Inam Ullah, & Alvi, Bilal Ahmed. (2018). Drones for Good in Smart Cities : A Review. *International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC)*.

Li, Yibin, Dai, Wenyun, Ming, Zhong, & Qiu, Meikang. (2016). Privacy Protection for Preventing Data Over-Collection in Smart City. *IEEE Transactions on Computers*, vol. *65*, iss. 5, pp. 1339–1350. https://doi.org/10.1109/TC.2015.2470247

Manda, MI, & Backhouse, Judy. (2016). Addressing trust, security and privacy concerns in e-government integration, interoperability and information sharing through policy: a case of South Africa. *E International Conference on Information Resources Management (CONF-IRM)*, pp. 67. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1009&context=confirm2016

Martínez-Ballesté, Antoni, Perez-Martinez, Pablo, Solanas, Agusti, Martínez-Ballesté, Antoni, & Pablo A. Pérez-Martínez, and Agusti Solanas. (2013). The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Communications Magazine*, vol. *51*, iss. 6, pp. 136–141. https://doi.org/10.1109/MCOM.2013.6525606

van Zoonen, Liesbet. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, vol. *33*, iss. 3, pp. 472–480. https://doi.org/10.1016/j.giq.2016.06.004

Vattapparamban, Edwin, Güvenç, Ismail, Yurekli, Ali I., Akkaya, Kemal, & Uluağaç, Selcuk. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. *2016 International Wireless Communications and Mobile Computing Conference, IWCMC 2016*, pp. 216–221. https://doi.org/10.1109/IWCMC.2016.7577060.

Zhang, Hanqi, Guo, Jianfeng, Deng, Chao, Fan, Ying, & Gu, Fu. (2019). Can video surveillance systems promote the perception of safety? Evidence from surveys on residents in Beijing, China. *Sustainability (Switzerland)*, vol. *11*, iss. 6. https://doi.org/10.3390/su11061595.

Zhang, Kuan, Ni, Jianbing, Yang, Kan, Liang, Xiaohui, Ren, Ju, & Shen, Xuemin Sherman. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, vol. *23*, iss. 1, pp. 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM.

Track II: Nuclear Nonproliferation and Disarmament

Track Chair:

Malte Göttsche

Nuclear Verification and Disarmament Group, AICES Graduate School and III. Institute of Physics B, RWTH Aachen University

Introduction

Today, the nuclear arms control architecture is threatened: The INF Treaty collapsed, and a qualitative arms race is underway. The future of the New START treaty is unclear. The North Korean nuclear program poses a threat to international security. At the same time, missile defence plans and the modernization of nuclear arsenals impede arms control efforts. The withdrawal of the United States from the Joint Comprehensive Plan of Action has the potential to curb non-proliferation efforts. While a large number of non-nuclear weapon states concluded negotiations on the Treaty on the Prohibition of Nuclear Weapons, there is little progress with regard to a Fissile Material Cutoff Treaty. Long-term pathways towards Global Zero remain unclear. As all of these issues have inherent technical components, scientific contributions are required to understand and solve them. Among those are for instance assessments of technical capabilities and the development of transparency and verification approaches as they are required to enable substantive arms control and disarmament measures.

To discuss nuclear arms control and non-proliferation, SCIENCE · PEACE · SECURITY invited contributions from the fields of physics and engineering, as well as policy relating to technical issues.

Nuclear Archaeology – Understanding Fissile Material Inventories for Nuclear Disarmament

Malte Göttsche

Nuclear Verification and Disarmament Group, AICES Graduate School and III. Institute of Physics B, RWTH Aachen University

[#11-paper]

Abstract

Uncertainties about global weapons-usable fissile material stockpiles are large. Also, states themselves observe differences between inventories known today and expected inventories based on their production records. This motivates the growing research field of nuclear archaeology, which is dedicated to reconstructing fissile material histories. It can comprise measurements in shut-down facilities and of radioactive wastes, analysing documentation of fuel cycle operations and carrying out related simulations. Even though not called nuclear archaeology, there have been past activities in several states where some of the mentioned methods were required to verify non-proliferation and disarmament. They imply that similar tasks will be important in the future. Therefore, future policy objectives and verification challenges are studied where conducting nuclear archaeology would be required or at least beneficial.

1. Introduction

While there is extensive experience in verifying both the correctness and completeness of nuclear material declarations issued by non-weapon states that are members of the Non-Proliferation Treaty (NPT), there is a lack of methods to verify the completeness of nuclear material baseline (or initial) declarations, i.e. the first verified declaration a state makes upon entering an agreement.

Also, nuclear weapon states face challenges in assessing the completeness of their inventories. The fissile material production uncertainty is very large, and even states themselves have had difficulty reconciling production records with physical inventories.

As was attempted after South Africa had joined the NPT in 1991 (see Baeckmann, 1990), the most promising approach to verify the completeness and correctness of baseline declarations is the reconstruction of the state's fissile material production history (Glaser & Göttsche, 2017). This is called nuclear archaeology, a concept introduced in 1990 (Hippel, 1990).

2. NUCLEAR ARCHAEOLOGY

In order to reconstruct past fissile material production, a first approach is performing modern fuel cycle simulations. Codes that are more accurate than those used decades ago could be utilized. Re-calculating production based on records has indeed been a major aspect of the verification in South Africa. A complementary approach, which nuclear archaeology research has focused on, is measuring nuclear waste and samples from shut-down production facilities.

2.1. SCENARIOS FOR NONPROLIFERATION, DISARMAMENT AND TRANSPARENCY

Nuclear security: Undertaking a process of fully characterizing and accounting for all weapons-usable materials by applying nuclear archaeology methods would create immediate security benefits. Conducting nuclear archaeology to improve states' own inventory assessments would act as a confidence-building measures that they take their nuclear security commitments seriously. Furthermore, such states – no matter whether nuclear or non-nuclear weapon state, would have a stronger case when demanding other states to better assess and secure their fissile materials.

Fissile material transparency: As existing arms control measures are under attack, the prospect for new initiatives remains grim, and the divide between non-nuclear and nuclear weapons states in the NPT context deepens, new confidence-building initiatives are required, and have been demanded: It was agreed at the 2010 NPT Review Conference that, "as a confidence-building measure, all the nuclear-weapon States are encouraged to agree as soon as possible on a standard reporting form […]" (NPT, 2010) including fissile material inventories. To-date, only the U.S. and U.K. have issued fissile material declarations. Confidence in these declarations could be built by holding an international exercise, where the methodology of reconstructing fissile material inventories is discussed, or where even an inspection could be carried to assess a part of an existing declaration.

Verified declarations for disarmament: Even if verification of warhead dismantlement will be taking place, existing fissile material stocks could be used to build new warheads. States must at some point declare the complete stocks of weapons-usable fissile materials they possess and allow for verification, in order to create confidence in and enable stability of arms reduction processes (Fuller et al., 2014). A verification process must build confidence that no large amounts of weapons-usable materials stocks are deliberately hidden. Undeclared storage facilities, however, do not need to have any remotely detectable signatures, for example using satellite imagery or wide-area environmental sampling. Their detection probability is low. Therefore, nuclear archaeology is the most promising method.

REFERENCES

A. von Baeckmann, G. Dillon, D. Perricos, "Nuclear Verification in South Africa," IAEA Bulletin 1/1995, 1995.

A. Glaser and M. Göttsche, Fissile Material Stockpile Declarations and Cooperative Nuclear Archaeology," in FM(C)T Meeting Series, Verifiable Declarations of Fissile Material Stocks: Challenges and Solutions, United Nations Institute for Disarmament Research Resources, 2017.

F. von Hippel, “Warhead and Fissile-material Declarations," in Reversing the Arms Race: How to Achieve and Verify Deep Reductions in the Nuclear Arsenals, New York, Gordon and Breach Science Publishers, 1990.

2010 NPT Review Conference Final Document, vol. 1, NPT/CONF.2010/50, New York, 2010.

J. Fuller, J. Carlson, M. Göttsche, et al., New Tools and New Actors to Reduce Nuclear Risks: Verifying Baseline Declarations of Nuclear Materials and Warheads, ed. Nuclear Threat Initiative, 2014.

Reactor Archaeology – Reconstruction of Operational Parameters from Isotope Ratios Measured in Structural Reactor Elements

Lukas Rademacher, Malte Göttsche and Madalina Wittel

Nuclear Verification and Disarmament Group, AICES Graduate School and III. Institute of Physics B, RWTH Aachen University

[#12-paper]

1. Introduction

The present stocks of nuclear material are estimated to be enough to build nearly 10 times the surmised number of existing warheads. Plutonium produced in reactors plays a central role in modern nuclear weapons and makes up the main part of the stocks - it exists in sufficient quantities for the production of more than 7 times the current arsenals. A comprehensive disarmament verification regime, therefore, requires the consideration of both nuclear warheads and these material stocks. Baseline declarations about the available amounts of fissile materials will have to be made by each country. However, they may lack credibility: either because of missing or highly uncertain data or even due to the suspicion of intentional deceit. Verification of these declarations requires a scientific method for crosschecking provided documentation with taken and analyzed measurements. To this end, we propose to extend the field of “reactor archaeology” that has traditionally been used to reconstruct neutron fluence (flux integrated over time), which is related to the produced amount of plutonium and allows for an estimation.

The fundamental principle of our proposed method relies on the “Graphite Isotope Ratio Method” (GIRM), a procedure developed to derive neutron fluence of a graphite reactor over its whole lifetime from ratios of stable trace-isotopes (Fetter, 1993). Further studies have extended the methods principles for usage on different types of reactors (Gasner & Glaser, 2011) or to differentiate between Plutonium and Tritium production modes (de Troullioud de Lanversin, Göttsche & Glaser, 2018).

2. Method

GIRM measurements are performed after shut-down and focus on trace isotopes that have been created in structural reactor components from the irradiation during the reactors operational period. They are then combined into isotope ratios which indicate neutron fluence, which is in turn linked to Plutonium production. We propose to extend GIRM to be able to assess other parameters in addition to fluence, e.g. times at which the reactor was operated or reactor power, which we collectively call "reactor parameters". To achieve this, in contrast to the existing method which only looks at stable or long-lived isotopes, one must specifically include shorter lived isotopes to gather information about parameters linked to the time dimension, for example shutdown time. In the context of a verification measurement performed years after a decades-spanning operation time "shorter" still refers to several years at the least.

Our investigation will make use of numerical methods as part of an algorithm to reconstruct reactor parameters, performing repeated sampling and simulation of input parameters until the isotopic ratios the simulation calculates are sufficiently close to the actual measurement. It will use the OpenBU code framework currently being developed by Julien de Troullioud de Lanversin at Princeton University, an open source burnup code running in conjunction with OpenMC neutron simulations. The available information from the state declarations as well as other sources can be used to construct an initial set of reactor parameters to run a full simulation on. To avoid the large computation resource requirements linked to Monte-Carlo simulations the ensuing sampling can be performed in a standalone computation mode decoupled from Monte-Carlo simulations, making use of the low expected variations in the actual neutron spectrum.

In the process of developing the algorithm we will consider the isotopes present in the material after irradiation and examine their suitability, or more precisely that of their ratios, to provide information on the reactor parameters. This will result in a selection of feasible ratios, most likely varying over different ranges of input parameters, to reconstruct parameters at good precision. Important selection criteria here are the presence and measurability of the respective isotopes as well as their dependence on input parameters, in particular differences to the dependencies of other included ratios.

We will also determine a set of reactor parameters that can be reconstructed from this. An initial set of preferred parameters could be obtained based on their respective importance for plutonium production; other important criteria to be evaluated are the precision that can be gained from the available isotope ratios as well as the consistency of the neutron spectrum approximation in the uncoupled simulations in respect to variations of the reactor parameter.

The final goal is a complete algorithm that could be used to verify a production declaration using measurement data obtained from the structural components within reasonable limits to time and computation power.

REFERENCES

Fetter, S. (1993). Nuclear archaeology: Verifying declarations of fissile-material production, Science & Global Security, 3,3-4, 237-259

Gasner, A. & Glaser, A. (2011). Nuclear Archaeology for Heavy-Water-Moderated Plutonium Production Reactors, Science & Global Security, 19,3, 223-233

de Troullioud de Lanversin, J., Göttsche, M. & Glaser, A. (2018). Nuclear Archaeology to Distinguish Plutonium and Tritium Production Modes in Heavy-Water Reactors, Science & Global Security, 26,2-3, 70-90

Verification Technologies for Nuclear Arms Control Treaties: Research Results and Prospects

GERALD KIRCHNER

CARL FRIEDRICH VON WEIZSÄCKER-CENTER FOR SCIENCE AND PEACE RESEARCH (ZNF), UNIVERSITY OF HAMBURG

[#13-PAPER]

1. Introduction

The availability of approved, reliable and robust verification procedures and technologies is an essential requisite for the existing nuclear arms control treaties, i.e. the Nuclear Non-Proliferation Treaty and the Comprehensive Nuclear Test Ban Treaty. Their verification regimes include numerous documentation and reporting requirements, but center on adequate on-site and remote measurement technologies to verify the compliance of signature states with their treaty obligations. Not surprisingly, past experience has shown that these verification technologies need to be enhanced or complemented by others for closing gaps, which were not anticipated when establishing the verification scheme. Their development is an important element of physics-based science peace research.

No treaty exists between the nuclear weapon states on nuclear disarmament nor is it expected to be negotiated within the near future. However, with the International Partnership for Nuclear Disarmament Verification (IPNDV) an international coordinated initiative has been established for developing verification regimes in support of future negotiations (Niemeyer et al., 2019).

In the following, examples are given of recent physical verification research results in the author's institute and future prospects.

2. Example 1: Verification of the Comprehensive Nuclear Test Ban Treaty

For verifying this treaty, a global International Monitoring System has been established, which monitors and evaluates radionuclide, seismic, infrasound and hydroacoustic signals. For suspect seismic events, confirmation of its nuclear origin is provided for by detection of the four longer-lived radioactive xenon isotopes in air. However, the operation of the monitoring network has shown that this approach is restricted due to unexpectedly high emissions of radioactive xenon radionuclides by civil nuclear facilities (Saey, 2009). Therefore, it may be attractive to complement the xenon analyses by measuring concentrations of Ar-37, as this radionuclide is produced by activation of rock calcium during an underground nuclear explosion. Information on anthropogenic emissions of this radioisotope by nuclear reactors were missing and have been generated by a research project at our institute.

Argon-37 is not produced by nuclear fission, but by neutron capture in Ar-36, which is a minor isotope of natural argon present in air, and in calcium by a (n,α)-reaction in Ca-40. Production pathways in light water reactors include (i) within the reactor core the activation of argon in air dissolved in the water moderator and of calcium present as impurity in fuel, and (ii) outside of the pressure vessel the activation of argon in air and of the calcium present in the concrete of the biological shield.

Our calculations, which have been validated by measurements, show that Ar-37 by these various pathways is small and after dilution in the atmosphere rapidly become lower than its natural background. Thus, Ar-37 is attractive for verifying the Comprehensive Test Ban Treaty. Next steps will include the development of sensitive and fast detectors and their test at some of the existing radionuclide monitoring laboratories.

3. Example 2: Nuclear Disarmament Verification

The major challenge for any verification regime for nuclear disarmament verification is given by the nuclear weapons states' interest in keeping almost all construction details of nuclear warheads confidential. Within the International Partnership of Nuclear Disarmament Verification, a concept has been developed, which combines qualitative measurements of the presence of fissile material and of high explosives with high sensitivity measurements of their absence (e.g. in scrap containers). Focusing on the dismantlement process of a warhead, which is highly attractive for potential diversion of fissile material, this concept will be tested by a one-week practical exercise which is jointly prepared by FZ Jülich and our institute (Niemeyer, 2019). Its results are expected to provide confidence that the concept can be applied for verifying a future nuclear disarmament treaty, but also to give input for future refinement of the generic concept.

4. Acknowledgements

Financial support of this research provided by the German Foundation for Peace Research and by the German Foreign Office is gratefully acknowledged.

References

Niemeyer, I., Kirchner, G., Neuneck, G. (2019). Building Global Verification Expertisee – the German Contributions in the International Partnership for Nuclear Disarmament Verification (IPNDV). In F. Sevini, A. De Luca, E. Stringa (Eds.), ESARDA 41th Annual Meeting, Stresa, 14. - 16. 5. 2019. European Commission, Report EUR 28795 EN, 345-353.

Saey, P.R.J. (2009). The influence of radiopharmaceutical isotope production on the global radioxenon background. J. Environmental Radioactivity 100, 396-406.

Technical and Legal Challenges for Germany to Join the Treaty on the Prohibition of Nuclear Weapons

MORITZ KÜTT

INSTITUTE FOR PEACE RESEARCH AND SECURITY POLICY (ISFH), UNIVERSITY OF HAMBURG

[#14-PAPER]

ABSTRACT

On October 18, 2018, the German Bundestag discussed and voted on a motion calling upon the government to sign the Treaty on the Prohibition of Nuclear Weapons (TPNW). The motion was not approved, but has been supported by Die Linke and the Green Party. The TPNW prohibits the development, possession, use and threat of use of nuclear weapons. This presentation will discuss the technical and legal challenges Germany would face if it were to join the treaty, and the steps that would need to be taken prior to ratification and after the treaty enters into force.

First, I will assess the obligation for states party to the treaty never to "[a]llow any stationing, installation or deployment of any nuclear weapons or other nuclear explosive devices in its territory or at any place under its jurisdiction or control." At the height of the cold war, more than 4000 nuclear weapons were stored in over 200 different sites on German soil. This number has since decreased drastically, and it is currently estimated that Germany hosts twenty tactical nuclear weapons owned by the United States in one location. The removal of these weapons would be a necessary step on the path to German accession to the TPNW. Verification options that could accompany the removal process will also be discussed.

Second, I will analyze the legal changes that Germany would need to undertake to transform the treaty obligations into German law. Several regulations are already in place, such as the ban on the production of nuclear weapons codified in article 17 of the *Kriegswaffenkontrollgesetz*. Furthermore, as a member of NATO, Germany is part of a "nuclear alliance". It is the current understanding that NATO members might aid other member states with nuclear weapons. I will summarize the current debate on the relationship between TPNW obligations and NATO membership.

1. INTRODUCTION

On October 18, 2018, the German Bundestag discussed and voted on a motion calling upon the government to sign the Treaty on the Prohibition of Nuclear Weapons (Bundestag, 2018). The Treaty on the Prohibition of Nuclear Weapons (TPNW) is the latest framework to join the existing body of international law on the subject of nuclear weapons. During the 2016 United Nations General Assembly, a resolution that required states to negotiate "a legally binding instrument to prohibit nuclear weapons, leading towards their total elimination" received 113 votes in favor (UNGA A/RES/71/258). 124 countries met in two sessions in 2017 to negotiate and adopt a treaty text. Currently, 70 countries have signed the TPNW, 23 countries have ratified the treaty (UNODA, 2019). The treaty will enter into force as soon as 50 states deposit their instruments of ratification (Article 15).

Germany, along with every other NATO member state except the Netherlands, did not take part in the negotiations leading up to the adoption of the TPNW. As of today, Germany has not signed the treaty, although it is the general policy of the German government to work towards a world without nuclear weapons (Böhmer, 2017). Two German parties, *Die Linke and Bündnis 90/ Die* Grünen supported the 2018 motion in the German Bundestag, while the other parties voted against it or abstained.

The TPNW prohibits the development, possession, use and threat of use of nuclear weapons. It also includes a special obligation for states party to the treaty never to "[a]llow any stationing, installation or deployment of any nuclear weapons or other nuclear explosive devices in its territory or at any place under its jurisdiction or control." (Article 1.1.g). At the height of the cold war, more than 4000 nuclear weapons were stored in over 200 different sites on German soil (Rabe, 1984). The number has decreased drastically since then, and it is currently estimated that Germany hosts 20 tactical nuclear weapons owned by the United States at the Büchel airbase (Kristensen & Korda, 2019). During the Cold War, a larger number of other countries hosted U.S. and Soviet nuclear weapons on their soil. Today, the only other countries hosting weapons are Belgium, Netherlands, Italy, and Turkey.

Ninety days after Germany ratifies the treaty, it enters into force for Germany, assuming that the treaty, in general, has already entered into force. No later than 30 days after entry into force, Germany has to declare that it hosts nuclear weapons of a different country on its soil (Article 2.1.c). Those weapons have to be removed as soon as possible, within a deadline that will be set by the first Meeting of States Parties. After the weapons have been removed, Germany would declare the fulfilment of its obligation to the UN Secretary General (Article 4.4). No verification of the removal is required, but voluntary measures could include opening storage sites to international inspectors, who could then verify that no nuclear weapons are remaining in these facilities. Inspectors could also verify the conversion of the German dual-capable Tornado airplanes. Potentially, one could prove that the storage site held weapons immediately after removal based on neutron activated concrete in the bunkers.

Article 3 of the treaty requires Germany to adopt agreements on safeguards with the International Atomic Energy Agency (IAEA). Germany has ratified the Comprehensive Safeguards Agreement (INFCIRC/153), as required by the Nuclear Non-Proliferation Treaty (NPT). The TPNW Article 3.2 requires such an agreement as a minimum standard. Germany has also ratified the Additional Protocol (INFCIRC/540), which grants the International Atomic Energy Agency extended rights during inspections. This agreement is voluntary both under the NPT and the TPNW, but TPNW Article 3.1 requires Germany to "maintain its International Atomic Energy Agency safeguards obligations in force at the time of entry into force of this Treaty."

In the German legal system, international agreements have to be approved with a special treaty law ("*Vertragsgesetz*"). According to Article 5 ("National Implementation"), Germany will be required to adopt legal measures to prevent activities prohibited under the treaty. Currently, the legal system already in place in Germany includes numerous measures prohibiting development, production, acquisition, import, export and transport of nuclear weapons in various legal codes (Kriegswaffenkontrollgesetz, Strafgesetzbuch, Verordnung zur Durchführung des Außenwirtschaftsgesetzes, Gesetz über das Zollkriminalamt und die Zollfahndungsämter). These codes specifically define a nuclear weapon as a device that contains (or is made to contain) nuclear fuels or radioactive isotopes for the purpose of mass destruction, mass damage or mass poisoning. Parts of such devices are also considered nuclear weapons. The legal obligations also refer to the definition in the Brussels Treaty of 1954, which prohibits Germany from acquiring atomic weapons (Brussels Treaty, 1954).

None of the existing legal codes listed above regulates the threat of use of nuclear weapons. New legal provisions could be required here, as the TPNW does go so far as to specifically prohibit such threats (Article 1.1.d). Additional legal measures could further prohibit the stationing of nuclear weapons on German soil. Currently, German law includes a special exception to allow weapon-related activities as part of NATO activities (Article 16, *Kriegswaffenkontrollgesetz*). This article likely would have to be revoked to comply with the TPNW.

According to NATO’s 2010 Strategic Concept, "as long as there are nuclear weapons in the world, NATO will remain a nuclear Alliance" (NATO, 2010). However, NATO’s founding treaty, in fact, does not make any reference to nuclear weapons. Furthermore, Germany is a member of the Nuclear Planning Group, which allows it to participate in NATO nuclear policy making. It also supports the 2010 Strategic Concept, which was adopted by consensus. The provisions in the concept casts Germany as a "nuclear umbrella" state, because it receives security guarantees that stipulate the possible use of U.S. nuclear weapons to defend Germany. The TPNW prohibits member states to "assist, encourage or induce, in any way, anyone to engage in any activity prohibited to a State Party under this Treaty;" (Article 1.1.e). Nuclear umbrella agreements could be considered "encouragement," and as such would have to be renounced to comply with the TPNW (NPA, 2018; IHRC, 2018). A U.S. "Non-Paper" on possible implications of a Nuclear Ban Treaty supports the fact the umbrella agreements would need to be renounced (NATO, 2016).

Upon joining the TPNW, Germany would have to leave the Nuclear Planning Group, and make clear that the nuclear-weapons-related provisions in the 2010 Strategic Concept would not apply to Germany anymore. Although such a move would not be viewed favourably by other NATO countries, there are examples of individual national policy choices within NATO. Denmark, Norway and Spain do not allow deployment of nuclear weapons in peacetime, while Iceland and Lithuania refuse to host nuclear weapons under any circumstances (Eide, 2014). Germany remaining in NATO while joining the TPNW would also be in line with NATO's commitment to work towards a world free of nuclear weapons.

REFERENCES

Böhmer, M. (2017). Bundestagsprotokoll 18/239, Plenary Meeting, June 21, 2017.

Brussels Treaty (1954). Text of Modified Brussels Treaty (Paris, 23 October 1954). URL: Retrieved from http://www.cvce.eu/obj/modified_brussels_treaty_paris_23_october_1954-en-7d182408-0ff6-432e-b793-0d1065ebe695.htm

Bundestag (2018). Bundestagsprotokoll 19/58, Plenary Meeting, October 18, 2018, p. 6501.

Eide, S.-I. L. A Ban on Nuclear Weapons: What's in It for Nato? - Why Nato States Should Not Be Worried About a Ban on Nuclear Weapons. International Law and Policy Institute, 2014.

IHRC/International Human Rights Clinic (2018). Nuclear Umbrella Arrangements and the Treaty on the Prohibition of Nuclear Weapons. URL: http://hrp.law.harvard.edu/wp-content/uploads/2018/06/NuclearUmbrellaArrangementsTreatyProhibition.pdf.

Kristensen, H. M., Korda, M. (2019). United States Nuclear Forces, 2019, Bulletin of the Atomic Scientists, 75, 3, 122–34. DOI: 10.1080/00963402.2019.1606503.

NATO (2010). Active Engagement, Modern Defence - Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

NATO (2016). United States Non-Paper: Defense Impacts of Potential United Nations General Assembly Nuclear Weapons Ban Treaty, AC/333-N(2016)0029 (INV), October 17, 2016.

NPA / Norwegian People's Aid (2018). Nuclear Weapons Ban Monitor - Preliminary Research. URL: Retrieved from http://www.icanw.org/wp-content/uploads/2018/05/Nuclear-Weapons-Ban-Monitor.pdf

Rabe, K.-K. (1984). Atomwaffen-Standorte in der Bundesrepublik. Forschungsinstitut für Friedenspolitik.

UNODA/United Nations Office of Disarmament Affairs (2019). Disarmament Treaties Database. URL: Retrieved from http://disarmament.un.org/treaties/t/tpnw

Fissile Materials, Nuclear Proliferation and HEU Elimination

MATTHIAS ENGLERT

INSTITUTE FOR APPLIED ECOLOGY

[#15-PAPER]

ABSTRACT

Minimization of the civil use of highly enriched uranium (HEU) is one of the cornerstones of international nonproliferation efforts. The aim is to prevent the access of states, subnational actors or terrorists to fissile material suitable to build nuclear weapons. This short paper presents some of the current issues regarding HEU use, production technologies and HEU minimization efforts.

1. FISSILE MATERIALS AND NUCLEAR PROLIFERATION

Highly Enriched Uranium - HEU is a special fissile material that can be used in nuclear weapons. In the civilian nuclear sector HEU is used to fuel research and power reactors, for naval propulsion and to produce isotopes for medical purposes.

More than seven decades after the construction of the first nuclear weapons the main barrier to build nuclear weapons today still is access to sufficient quantities of nuclear weapons-relevant materials and less the construction of a functioning nuclear explosive device. The procurement of fissile material is, so to speak, the decisive bottleneck through which state and sub-state actors must pass before they can build a nuclear explosive device.

Highly enriched uranium is particularly attractive for military or terrorist use because, unlike plutonium, weapons, they can be built with relatively simple designs. The Proliferation risks of highly enriched uranium are associated with HEU stocks and uranium enrichment technologies. For example, uranium enrichment plants, especially gas centrifuge plants, can easily be converted from LEU production to HEU production. Also, HEU has to be stored and transported. HEU can be diverted or stolen from the civilian sector and then used for military or terrorist purposes. In non-nuclear-weapon states, stocks and production technologies are subject to safeguards by the International Atomic Energy Agency (IAEA).

The minimization of civilian use of highly enriched uranium has been one of the priority activities worldwide since the end of the 1970s to reduce the risk of nuclear proliferation and nuclear terrorism. Internationally, the norm was established that enrichments of the isotope uranium-235 with more than 20% by weight in uranium are classified as highly enriched uranium (HEU) and those below as low enriched uranium (LEU).

2. HEU

The mass of uranium for a nuclear weapon (or the critical mass) is significantly reduced the higher the percentage of the uranium isotope U-235 in the uranium metal. The lower the critical mass, the higher the attractiveness of the highly enriched uranium for weapon use. For military applications, weapons-grade HEU with an enrichment above 90% is therefore preferred. Today, there is a broad international consensus that the 20% enrichment limit is a viable choice for differentiating between HEU and LEU. The definition originally dates back to the 1950s (Atoms for Peace). Today, the IAEA defines uranium with an enrichment greater than or equal to 20% as highly enriched uranium and classifies HEU as "direct use" material.

The chemical form in which the uranium is present plays no role in this classification. However, the effort for a proliferator to acquire HEU for a weapon application depends on the respective processing steps necessary to generate metallic HEU that could be used in a weapon. The Department of Energy of the USA defines (Department of Energy, 2012) the need for nuclear material monitoring in a graded safeguards table for Special Nuclear Materials (SNM) located at a specific location. The sub-allocation serves to classify different categories of unirradiated, highly enriched uranium into different monitoring needs. However, HEU is always considered to be a "special nuclear material".

3. HEU PRODUCTION

In strict legal terms, international treaties do not restrict a state from using highly enriched uranium for civilian purposes or producing it itself for civilian purposes. The signatory states of the Non-Proliferation Treaty are only obliged to report such a procedure to the IAEA.

Today HEU is produced with gas centrifuge technology, a technology which is in the reach of the technical capabilities of most countries worldwide. Problematic developments in nuclear proliferation in the last two decades involved the spread and covert acquisition of centrifuge enrichment capabilities by countries such as Iran and North Korea

However, with the exception of North Korea and Pakistan, new production of HEU has been abandoned worldwide in the 1990s. After a long moratorium, Russia resumed HEU production in 2012. It is reported that the need for HEU fuel of the German research reactor FRM-II contributed to this worrisome development (Glaser & Podvig, 2017). In nuclear weapons states such as Russia, HEU still plays a major role either as a commodity or for the domestic energy and research programs, e.g. the recent use of HEU to fuel the Russian fast reactor program.

Not much is known about the North Korean enrichment program. However, it can be safely assumed that North Korea produces HEU in its gas centrifuge facilities.

Not often talked about: other countries also enhance and expand their centrifuge capabilities such as Pakistan or Brazil.

In Iran, the nuclear program is mostly frozen since the Iran Nuclear Deal (JCPOA). Recently tensions between Iran and the US are on the rise after the US left the JCPOA. Iran threatens to resume its enrichment program. The IAEA never found evidence that Iran produced enrichment levels beyond 20% with its gas centrifuge facilities. However, Iran’s latent nuclear capabilities allow Iran to engage actively in the form of “weaponless” nuclear deterrence. Iran with its capability to enrich uranium follows the historic role model of other virtual nuclear weapon states such as Germany and will set another case for the future treatment of uranium enrichment technologies in international security and international norms.

4. HEU ELIMINATION AND REACTOR CONVERSION

Internationally there is a great interest to reduce the risks associated with civil HEU use. One major challenge is the use of HEU as research reactor fuel. Other challenges would be the use of HEU for medical isotope production or the conversion of naval propulsion reactors.

4.1. REACTOR CONVERSION

A major focus of the efforts to minimise the civil use of HEU is to convert the fuel of research reactors from the use of highly enriched uranium to the use of low enriched uranium. Research reactors are the largest civilian users of highly enriched uranium. The reduction of enrichment has to be compensated by the amount of fissionable uranium-235 in the reactor core either by a larger quantity of fuel (volume increase) or by a higher density of the fuel. Following the qualification of uranium silicide fuels (U3Si2) with a higher density of up to 4.8 g/cm3 in the 1980s, a number of research reactors worldwide were converted from HEU to LEU (below 20% enrichment in U-235) with the aid of the new fuel.

On the one hand, the conversion of research reactors from the use of HEU to the use of low-enriched uranium was quite successful. But the complexity to qualify suitable high-density Uranium-Molybdenum (UMo) fuels to convert high flux reactors from HEU to LEU also caused difficulties in the conversion efforts. Still, the annual demand for HEU for research reactors is the highest compared to other civilian applications.

4.2. THE GERMAN RESEARCH REACTOR MUNICH II (FRM-II)

Since all research reactors in Germany except FRM-II have been converted to LEU or decommissioned, today's conversion efforts concentrate on FRM-II. The reactor's HEU design dates back to the 1980s. It was not until 1994 that the nuclear licensing procedure was started, despite the fact that since the 1980s, a norm existed not to commission any new research reactors with a design based on HEU fuel. A main exception to this norm until today is the FRM-II, which went critical in 2004.

In Germany, efforts to convert research reactors in the 1980s were supported by the development of denser uranium silicide fuels in the "Programme for the reduction of enrichment in research reactors" (AF Programme). The development programme - financed with 50 million Deutsche Mark - originally served to convert the West German research reactors in Jülich, Berlin, Munich (FRM-I) and Geesthacht.

However, the uranium silicide fuels originally developed for the LEU conversion in the fuel development program were reused with high enrichment for the FRM-II in order to design a reactor core that was as compact as possible with an optimized power to volume ratio. This misappropriation of the uranium silicide fuel, developed for conversion purposes, together with the very compact fuel element and the restrictions on dimensional changes, is now the difficulty of why a conversion of the FRM-II to LEU is so technically challenging.

Due to years of criticism and the change of federal government, the Federal Ministry of Education and Research (BMBF) convened a commission of experts in 1998 to discuss various conversion options. The compromise in 2001 finally provided for commissioning with HEU uranium silicide fuel and subsequent conversion to less than 50% enrichment by the end of 2010, depending on the status of the development of high-density fuels. The reactor finally went into operation in 2004. The FRM was initially supplied with HEU from European "remaining stocks" and then from Russian production.

The date of conversion of FRM-II to LEU use depends on the availability of suitable high-density fuels with an even higher density than the 1980s uranium silicide fuels developed for reactor conversion back then. After it became clear in 2008 that the development of new high-density fuels would not be completed by 2010, the original FRM-II conversion agreement was amended in 2010. The 2010 amendment to the original agreement between Bavaria and the Federal Government stipulates that an agreement will be reached between the parties concerned and the operator by the end of 2016 as to whether the reactor can be converted by the end of 2018.

The more recent fuel developments towards even higher densities are based on uranium-molybdenum (UMo) alloys either as dispersion fuel or monolithic fuel. Both fuel types encountered unexpected development difficulties. The dispersion fuels showed an unstable swelling behavior under irradiation, which could only be partially eliminated so far. In the case of monolithic fuels, after initial problems with irradiation have been largely solved, fuel manufacturing is the main problem. At present, a conversion of the FRM-II with these new high-density UMo fuels cannot be expected within the next ten years.

There are essentially two options currently available (2019):

- Wait: postpone FRM-II conversion until new high-density uranium-molybdenum fuels are qualified and available. Until then, further operation will be carried out with the current uranium silicide HEU fuel. This option results effectively in no conversion during the first quarter century of reactor operation.
- Two-Step Conversion: As a first step - short term conversion with currently available or short term licensable uranium silicide fuels with a density of 4.8 g/cm3 or more to an enrichment much less than 93%, ideally less than 50%. The aim should be to achieve the lowest possible enrichment by exploiting geometric changes in the fuel element. The US National Academy of Sciences 2016 (NAS 2016) recommended such an intermediate step on the way to a longer-term conversion with the new high-density fuels. As a second step – conversion to less than 20% enrichment as soon as the high-density fuels become available.

The conversion of FRM-II is complex, a whole range of possibilities, but also different interests must be weighed against each other. The goal of less than 20% enrichment should, however, be pursued intensively by all actors.

4.3. HEU REPATRIATION

Another success is the fuel repatriation programs. Historically, the supplier countries for the HEU were the USA and Russia. As early as 1992, the USA adopted the so-called "Schumer Amendment", which excludes the export of HEU from enrichment above 20%.

Many fresh and spent fuel assemblies containing HEU have already been returned to the supplier countries (USA, Russia) as part of the take-back programmes. The original "Off-Site Fuels Policy" of the USA (1964-1988) to take back delivered HEU was extended in 1996 to support the conversion of research reactors to LEU. As part of the Global Threat Reduction Initiative, the programme was continued from 2004-2015 (Foreign Research Reactor Spent Nuclear Fuel Acceptance Programme) and has been continued by the Office of Material Management and Minimization (M3) since 2015. In addition, there is a US-funded program for the return of HEU in spent fuel, formerly from the Soviet Union (Russian Research Reactor Fuel Return (RRRFR) Program). In both programmes, HEU was also returned from Germany to the countries of origin.

REFERENCES

Department of Energy. (2012). Nuclear Materials Control and Accountability. Department of Energy.

Glaser, A., & Podvig, P. (8. November 2017). Production of new highly enriched uranium in Russia for the FRM-II in Germany. Retrieved 05. 06 2019 von International Panel on Fissile Materials: Retrieved from http://fissilematerials.org/blog/2017/11/production_of_new_highly_.html

National Academies of Sciences, Enginieering, and Medicine. 2016. Reducing the Use of Highly Enriched Uranium in Civilian Research Reactors. Washington, DC: The National Academies Press. https://doi.org/10.17226/21818

Nuclear Archaeology – Reconstructing Reactor Histories from Reprocessing Waste

Antonio Figueroa and Malte Göttsche

Nuclear Verification and Disarmament Group, AICES Graduate School and III. Institute of Physics B, RWTH Aachen University

[#16-ext.-abstract]

Extended Abstract

Nuclear archaeology is a field dedicated to the reconstruction and quantification of the past production of weapons-usable fissile materials. In the context of nuclear disarmament, the verification of both nuclear warheads and fissile material stocks is crucial (Podvig, 2016). With regard to aggregate plutonium production estimates in a reactor's lifetime, the Graphite Isotope Ratio Method (GIRM) (Fetter, 1993; Gesh, 2004), proposed in 1993, has been developed and tested the most. This method consists of the study of trace isotopes – initially present as impurities in graphite to deduce the lifetime cumulative neutron flux inside the reactor. Similar methods are currently under development which apply an equivalent analysis to heavy water moderated nuclear reactors (Gasner & Glaser, 2011).

Although effective, these techniques cannot be applied once the reactor site has been decommissioned. In addition, they do not address the issue of verifying historical operation records and their consistency with measurements. In this case, we examine the possibilities and limitations of exploiting measurements of reprocessing waste isotopic composition to reduce uncertainty in fissile material declarations and production records, especially those dating back to early production operations. This is done through the inference of parameters related to the operational history of reactors such as burnup and cooling time, based on measurements of such waste. In the current work, we build upon initial studies on the method (Figueroa & Göttsche, 2019; Göttsche, De Troullioud De Lanversin, & Tietze-Jaensch, 2017).

For the first stage of this project, we create a computer model of the savannah river plutonium production reactor K. Due to the complexity of this model, it is impossible to obtain a mathematical formula to estimate the reactor input parameter values related to a given isotope measurement, which is our goal. Instead, we run several forward simulations with the montecarlo code Serpent 2 ("Serpent - A Monte Carlo Reactor Physics Burnup Calculation Code," n.d.) to identify outputs close enough to the measurements, a procedure similar to traditional optimization approaches. To do that, we have developed a surrogate model that can be used as a computationally less expensive way to obtain an approximation to the results from an actual simulation. This is done through the use of gaussian process regression which provides an interpolated prediction at a non-simulated point based on the set of forward simulations (Rasmussen & Williams, 2006).

In the second stage, we use the surrogate model, in conjunction with the Bayesian inference framework, to solve the inverse problem of deducing the reactor batch operational history given a reprocessing waste measurement. This framework provides a solid probabilistic approach to inverse problems in which not only a solution can be inferred, but also the uncertainty in the measurement and model can be propagated into the estimated solution, producing a probability distribution for each parameter under study. A key point of this methodology is the possibility to include information such as state declarations, operational records, intelligence reports/analyses and process expertise among others, that gives it an edge in comparison to other techniques. This feature works by limiting the space of possible solutions, confirming existing information or providing awareness in the case of inconsistent information sources that could indicate at best incomplete information or at worst, cheating.

For a proof of principle, we design and examine a group of scenarios involving a fissile material production declaration by a state, which has to be verified. For this, we consider the case of reconstructing burnup and cooling time for an operation consisting of: a single batch with only basic information on the general limits of the parameters, a single batch but now simulating the presence of operational records, a mixture of waste from two batches of the same reactor with different parameters, a mixture of waste from two batches with simulated operational records and finally, a waste mixture of two batches where the simulated records provide wrong information.

The Bayesian inference is conducted with the software PyMC3 (Salvatier, Wiecki, & Fonnesbeck, 2016). We observe that the reconstruction of such parameters is possible, as well as their correct combination and mixing proportion, provided additional information is included in the analysis. Additionally, irregularities in operational histories declarations can be detected due to the contradictory results they produce during the inference process. This is particularly important in the scenario of a mixture of 2 waste batches, where a declaring party might try to hide a very low burnup campaign - associated with weapons grade plutonium – by mixing its waste with that of a higher burnup campaign.

Much research is still to be done to explore the limitations of this methodology, namely the largest number of parameters that can be inferred from a waste measurement, and the use of isotope ratios, which should allow for uncertainty reduction in measurements from tanks with non-homogeneous waste.

REFERENCES

Fetter, S. (1993). “Nuclear Archaeology: Verifying Declarations of Fissile-Material Production”. Science & Global Security 3, 1993: 237-259.

Figueroa, A., Göttsche, M. (2019). Nuclear Archaeology: Reconstructing Reactor Histories From Reprocessing Waste, ESARDA 2019

Gesh, C. (2004). “A Graphite Isotope Ratio Method Primer - A Method for Estimating Plutonium Production in Graphite Moderated Reactors.” PNNL-14568, Richland, Washington, USA.

Gasner, A., Glaser, A. (2011). “Nuclear Archaeology for Heavy-Water-Moderated Plutonium Production Reactors.” Science & Global Security 19, 2011: 223-233.

Göttsche, M., Troullioud de Lanversin, J.,Tietze-Jaensch, H. (2017). Examining Reprocessing Waste to Help Estimate Past Plutonium Production, 58th Annual INMM Meeting, July 16-20, 2017, Indian Wells, California, United States.

Podvig P. (2016). *Verifiable Declarations of Fissile Material Stocks: Challenges and Solutions*, UNIDIR

Rasmussen C.E., Williams C.K.I. (2006). *Gaussian Processes for Machine Learning*, Massachusetts Institute of Technology

Salvatier J., Wiecki T.V., Fonnesbeck C. (2016) Probabilistic programming in Python using PyMC3. PeerJ Computer Science 2:e55 DOI: 10.7717/peerj-cs.55.

Serpent, A Continuous-energy Monte Carlo Reactor Physics Burnup Calculation Code. Retrieved from http://Monte Carlo.vtt.fi/index.htm

Prospects for Spent Nuclear Fuel Safeguarding with Antineutrino Detectors

MADALINA WITTEL AND MALTE GÖTTSCHE

NUCLEAR VERIFICATION AND DISARMAMENT GROUP, AICES GRADUATE SCHOOL AND III. INSTITUTE OF PHYSICS B, RWTH AACHEN UNIVERSITY

[#17-EXT.-ABSTRACT]

EXTENDED ABSTRACT

A large amount of spent nuclear fuel (SNF) has been produced both in civilian as well as in military applications of nuclear energy in the past decades. The International Atomic Energy Agency (IAEA) evaluated the global cumulative amount of spent fuel at the end of 2014 at approximately 380,500 tonnes heavy metal, with about 10,000 tonnes of heavy metal of SNF discharged yearly (International Atomic Energy Agency, 2015). Thus, presently, more than 430,000 tonnes heavy metal of spent fuel are stored around the world. Moreover, due to the growing demand for (clean) energy, several countries like China, India, Russia and the United Arab Emirates are planning to augment their nuclear capacity which would, in turn, lead to an even faster increase in the quantity of spent fuel.

The Institute for Science and International Security (Institute for Science and International Security, n.d.) estimated that, at the end of 2014, the global amount of irradiated (i.e. present in spent fuel) and unirradiated (directly usable for nuclear weapons) plutonium was approximately 2,400 tonnes (D. Albright, S. Kelleher-Vergantini, D. Schnur, 2015). The presence of fissile material in the spent fuel constitutes an important verification challenge since it could be diverted for weapons production.

Several techniques can be employed for safeguarding the spent fuel, e.g. seals, video monitoring, remote radiation detection, etc. However, as the amount of SNF in storage accumulates, the probability that one of these monitoring techniques may fail also increases with time. Should such a failure occur, especially in the case of cask seals, the contents of the affected casks can no longer be accounted for? Measuring the radiation that escapes from a cask with a damaged seal can demonstrate that its content is radioactive, however, it cannot provide enough information to determine if any amount of spent fuel is missing. Neutron or photon radiography techniques may also not be feasible in this case due to the heavy shielding of the cask.

In order to verify the content of the cask and restore the continuity of knowledge, a tomographic technique based on cosmic muons was proposed and is currently under consideration (J.M. Durham et al., 2018). A complementary approach, first proposed in (P. Huber et al., 2017), envisages measuring the anti-neutrino emissions coming directly from the spent fuel itself for long term monitoring and for ensuring continuity of knowledge.

This approach relies on the fact that the main source of radioactivity in spent fuel comes from beta-decaying isotopes, i.e. the SNF is an abundant source of anti-neutrinos. While many isotopes have rather short half-lives (in the order of several hours or a few days), a few like ^{90}Sr ($T_{1/2}$ = 28.78a) and ^{137}Cs ($T_{1/2}$ = 30.17a) still contribute, even decades later. The low energy (< 10 MeV) anti-neutrinos can constitute a valuable source of information about the amount and content of the spent fuel in storage. Furthermore, due to their weakly interacting nature, with cross-sections lower than 10^{-38} cm^2, they inevitably escape even large amounts of shielding. This application of anti-neutrino measurements, carried out with liquid argon detectors, represents the focus of this paper.

The idea of using liquid-argon time projection chambers (LArTPC) for neutrino detection was first proposed by Carlo Rubbia in 1977 (C. Rubbia, 1977). A LArTPC consists of a large volume of liquid argon, cooled at 87K (-186.15° C), encompassed by a high-voltage cathode on one side and an anode on the opposite surface. In addition, several read-out wire planes are also located on the anode side.

When an (anti-)neutrino interacts via charged or neutral current exchange with an argon atom, i.e. either with the orbital electrons or the nucleus itself, the emergent charged particles ionise and excite further argon atoms along their trajectory. The emitted free electrons drift in the liquid argon, under the force of the electric field, until they reach the read-out wires, in which they generate small currents. In addition, the excited argon atoms also emit scintillation light in the ultraviolet range (λ=128nm) which can be measured with photosensors (PMTs).

One of the main advantages of LArTPCs is that they are *imaging* detectors - providing a three-dimensional reconstruction of the tracks left by the charged particles emerging from an anti-neutrino interaction. This is crucial for ensuring a good background rejection, e.g. based on topological criteria like the track length. Furthermore, argon (^{40}Ar) is, in fact, denser than both water and oil-based scintillator materials which are typically used in neutrino detectors. In contrast to these types of detectors, which rely on the inverse beta decay process for neutrino-observation, the main neutrino interaction in liquid argon is elastic scattering which has no kinematic threshold. Lastly, since argon constitutes approximately 1% of Earth's atmosphere, especially the ^{40}Ar isotope with an abundance of 99.6%, it is usually cheap to produce (and to liquify) and it is commercially available.

In our study, we compare the event rate expected in two container-sized, i.e. 80 tonnes, liquid argon and water-Cherenkov detectors, respectively. We show that, even though the expected event rates are rather low in both cases, the performance of the LArTPCs is comparable to that of the water-Cherenkov detectors, in particular, due to the kinematic threshold of the inverse beta decay reaction.

The LArTPC technology is presently developed and validated by the neutrino physics community, thus aligning the nuclear verification efforts with the forefront of fundamental science. Furthermore, as the technology matures, we demonstrate that utilising it for spent fuel safeguarding is worth investigating.

References

Albright, D.; Kelleher-Vergantini, S; Schnur, D. (2015). Plutonium and Highly Enriched Uranium Inventories. Institute for Science and International Security.

Durham, J.D. et al. (2018). Verification of Spent Nuclear Fuel in Sealed Dry Storage Casks via Measurements of Cosmic-Ray Muon Scattering. Phys. Rev. Applied, 044013. doi:10.1103/PhysRevApplied.9.044013

Huber, P. et al. (2017). Antineutrino Monitoring of Spent Nuclear Fuel. Phys. Rev. Applied, 054050. doi:10.1103/PhysRevApplied.8.054050

Institute for Science and International Security. (n.d.). Von www.isis-online.org abgerufen

International Atomic Energy Agency. (2015). Nuclear Technology Review. Vienna, Austria: IAEA. Retrieved from https://www.iaea.org/sites/default/files/ntr2015.pdf

Rubbia, C. (1977). The Liquid Argon Time Projection Chamber: A New Concept for Neutrino Detectors . CERN-EP-INT-77-08.

The Unintended Consequences of U.S. Nonproliferation Policies on ROK Nuclear Development

JONAS SIEGEL

SCHOOL OF PUBLIC POLICY, UNIVERSITY OF MARYLAND

[#18-EXT.-ABSTRACT]

EXTENDED ABSTRACT

This research reassesses the effect of U.S. nuclear nonproliferation policies aimed at limiting access to the back-end of the fuel cycle technologies, such as spent fuel reprocessing, in the ROK. Since the start of the Republic of Korea's nuclear program, the country's scientists have been interested in developing the capability to reprocess spent nuclear fuel. The 1968 "Long-Term Nuclear Power Development Plan" first articulated the ROK desire to develop a reprocessing capability as part of a broader commercial nuclear power program. With limited indigenous uranium resources, ROK scientists were eager to make the most of the energy content in commercial fuel and to expand the ROK's scientific and industrial capabilities.

In the early 1970s, the director of the Korean Institute for Science and Technology and a former director of the Korea Atomic Energy Research Institute (KAERI) Choi Hyung Sup played an important role in the development of this plan and was perhaps the strongest ROK advocate of developing a reprocessing capability. Choi was also approached by President Park Chung-Hee in 1971 and asked to lead the effort to acquire the technological capability to develop nuclear weapons. Park and then-KAERI director Yun Yong-gu knew that the already articulated desire for a reprocessing capability would serve the purpose of building up a ROK nuclear weapons capability as well. As such, they travelled to France to begin the negotiation for the sale of a reprocessing plant from SGNT.

The nuclear weapons proliferation risk presented by even a small reprocessing plant was made plain by the 1974 Indian nuclear explosion, in which Indian scientists used a reprocessing facility derived from U.S. technology to reprocess fuel from a Canadian research reactor to obtain the necessary plutonium for the explosive device. Concerned about a similar risk from the ROK nuclear program, U.S. officials denied ROK requests for direct reprocessing assistance and persuaded Park and Choi to cancel the order for the French reprocessing plant in exchange for a package of additional nuclear cooperative activities, including the promise to study the possibility of building a multinational reprocessing facility in Asia involving the ROK and others, help in developing a light-water nuclear fuel fabrication facility, training for ROK scientists, and a range of research and development collaboration. The ROK's decision to cancel the plant was also influenced by Canadian threats to put off an order for a commercial CANDU reactor—which the ROK wanted in order to diversify its nuclear program and increase its energy security—if it didn't cancel the plant.

In addition to winning the ROK additional U.S. nuclear cooperation, this episode had other effects: ROK scientists and officials became wary of relying on the United States as a supplier of nuclear technology and know-how. Indeed, when the ROK eventually negotiated the transfer of fuel fabrication technology, it did so with a German supplier for light-water reactor fuel and with Canadian nuclear authorities for heavy-water reactor fuel.

The cancellation of the French reprocessing facility purchase was not the end of ROK efforts to develop a domestic reprocessing capability. Throughout the 1980s, ROK officials tried in vain to engage U.S. officials and others in the development of the back-end of the fuel cycle facilities in the ROK. First, ROK scientists approached U.S. officials about developing a so-called Tandem process facility, but U.S. officials shut down this effort by not providing consent to the ROK to process U.S.-origin spent fuel in the facility and not agreeing to the location of or safeguard arrangements for the facility.

Well aware of U.S. proliferation concerns, ROK scientists tried again to obtain U.S. assistance in spent fuel processing with the development of the DUPIC process, starting in 1991. This time around, ROK scientists emphasized the degree to which, in their eyes, DUPIC presented less of a proliferation risk compared to traditional spent fuel reprocessing, because it didn't involve chemically separating plutonium from the rest of the spent fuel. Not only did the United States consent to the DUPIC program and assist in developing safeguards technologies that could be deployed at DUPIC facilities, but it ultimately provided sensitive technological assistance to the ROK to help it develop the remote-control technology necessary for hot-cell operations. The actual DUPIC fuel-fabrication process, however, was developed between ROK and Canadian scientists, a partnership that deliberately excluded American involvement so as to avoid U.S. nonproliferation obstruction.

Still eager for a back-end of the fuel cycle capability, in the late 1990s, ROK scientists began to develop a system called pyro-processing, which similarly promised to limit the proliferation risk of processing spent nuclear fuel and to reduce the amount of high-level waste in need of long-term disposal. Encouraged by a U.S. presidential administration that was eager to develop a new role for the United States in the global nuclear energy system, ROK officials developed a facility that would prepare spent nuclear fuel for the process. Despite ROK's enthusiasm and interest in this development route, the U.S. again withheld consent for the ROK to process U.S.–origin spent nuclear fuel—effectively stalling the entire process.

While U.S. nonproliferation policies have been effective in limiting ROK access to and experience with the back-end of the fuel cycle technologies, what have been the unintended costs of this influence? This review suggests that U.S. nonproliferation policies have inadvertently increased the spread of technological know-how about different types of back-end of the fuel cycle technologies, despite their stated goal of limiting proliferation. The ROK desire for back-end of the fuel cycle technologies has not diminished over time, and ROK scientists have simply shifted their focus to other potential technological avenues when stymied by U.S. policies. Would some of these later technologies have developed even if the U.S. initially consented to the ROK purchase of the French reprocessing facility? Maybe. But ROK scientists would have had far less reason to extend their technological understanding over time if they had a more willing partner in the United States.

The U.S. denial of back-end of the fuel cycle technologies also increased the incentives of South Korean officials to diversify ROK nuclear supply chains. A certain amount of diversification was always part of South Korean development plans, but the ROK moved more quickly in this direction than it would otherwise have because of uncertainty in U.S. supplies. The regular shifts in U.S. policy maker support for certain ROK capabilities, particularly in regards to pyroprocessing, also increased the resentments of ROK nuclear scientists at a time when the ROK was seemingly more committed to the nonproliferation regime than ever before.

Future Technological and Political Arms Races – Challenges for Research and Implementation

GÖTZ NEUNECK

INSTITUTE FOR PEACE RESEARCH AND SECURITY POLICY (ISFH), UNIVERSITY OF HAMBURG

[#19-ABSTRACT]

ABSTRACT

Given the erosion of existing arms control treaties (such as INF or the START-process) as well as the growing pace of new technological developments, global security and peace are confronted with new challenges, technically and politically. New technical arms races are on the horizon in several domains such as cyber and outer space which are poorly regulated with regard to military applications. On offensive-defensive arms competition is evolving in the strategic field such as offensive delivery systems and missile defence. Manoeuvrable supersonic cruise missiles, hypervelocity gliders, anti-missile interceptors and cyberweapons can threaten the offensive oriented nuclear balance. Additionally, new capabilities in the field of Artificial Intelligence are complicating the strategic debate. Classical nuclear arms control is based on parity of key weapon systems, offensive ballistic missiles and the verification of delivery systems. Politically, the great power competition between the US, Russia and China is heating up the debate politically. New arms races on scientific-technological fields are in the making. New innovative concepts have to be elaborated and science has to be part of this endeavour. The talk will give some recommendations for further research questions and fields.

Track III: Biological/ Chemical Weapons

Track Chair:

Mirko Himmel

Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg

Introduction

With the end of the Cold War, the use of biological or chemical weapons became more and more unlikely as means of warfare. Furthermore, the increasing global implementation of both, the Biological and Chemical Weapons Convention (BWC, CWC) has been perceived as promising sign for a persistent international ban of these weapons. The frequent use of chemical weapons (CW) in the course of the civil war in Syria, as well as the alleged use of nerve agents for assassination attempts in Malaysia and Great Britain by state actors, now puts the chemical weapons ban under pressure. In a politically tense atmosphere, a severe loss of trust can be recognised among CWC States Parties. Important questions such as the investigation of the alleged use of chemical weapons cannot any longer be solved in a constructive manner.

The political situation within the BWC regime is different, but not much better. There is still no agreed verification mechanism for this important arms control treaty. Compliance monitoring is relying in part on in-transparent methods. Science and technology are evolving fast, but a structured review of relevant developments is lacking. Within this context, political progress is slow and BWC States Parties experience difficulties to agree on necessary steps fostering the biological weapons ban. The adoption of new production concepts in the chemical industries, dual use aspects of new genetic engineering techniques as well as the convergence between biology and chemistry are some of the future challenges for biological and chemical arms control. Here, science can contribute to a better understanding of technical aspects of CBW. Compliance monitoring and the analysis of alleged CBW use can now be supported by open source information. Does the question remain how to make this information accessible? Fresh thinking is required to tackle all these problems.

To discuss challenges and possibilities for biological and chemical arms control, SCIENCE · PEACE · SECURITY invited contributions from the fields of biology, medicine, chemistry, from international arms control organisations as well as policy relating to technical issues.

Scientific Methods for Improving Biological and Chemical Arms Control

Mirko Himmel

Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg

[#20-abstract]

Abstract

Chemical arms control relies predominately on agreed inspection and verification procedures. The international Organisation for the Prohibition of Chemical Weapons (OPCW) supports the implementation of the Chemical Weapons Convention (CWC) and provides technical and scientific assistance to Member States. There is an increasing demand for integration of new scientific methods in the OPCW's work as reflected by several reports of the organisation's Scientific Advisory Board. New methods for chemical arms control include remote sensing technologies, chemical forensics, the use of open source information and computer-based algorithms for the assessment of toxic chemicals.

The Biological and Toxin Weapons Convention (BTWC) lacks a verification mechanism. Confidence Building Measures, which submission is not legally-binding, allow only in part to assess the compliance of Member States. Therefore, compliance monitoring relies on alternative methods and could include in the future the analysis of open source information. Other scientific methods for monitoring industry-scale process in selected production environments could be of use also for a more comprehensive monitoring approach.

Altogether, science can contribute to a better understanding of technical aspects of CBW. Compliance monitoring and the analysis of alleged CBW use can now be supported by open source information. But the question remains how to make this information accessible? An integrated analytical approach is required to address these challenges both in the BTWC and CWC context.

Additive Manufacturing and Biological Weapons: Assessing Proliferation Risks and Challenges to Export Control

KOLJA BROCKMANN

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE (SIPRI)

[#21-LONG-PAPER]

ABSTRACT

Additive manufacturing (AM), or 3D printing, has seen a renaissance in the last few years, particularly due to the huge popularity and growth of the range of affordable AM machines and the funding and strategic investment that has poured into the wider industry. AM applications related to the development, production and delivery of biological weapons have only more recently been identified as a possible source of concern. AM poses a number of challenges for export control, including the decentralization of production, a shift in skill requirements and an increased reliance on intangible transfers of technology. Developments in the printing of laboratory equipment and drone components and in the bioprinting of tissue potentially pose biological weapon proliferation risks. While relevant applications of AM currently still require considerable talent recruitment and process development efforts, particularly the digitized and automated nature of AM will likely mean that these barriers will be successively removed. It is thus important to neither under- nor overestimate the immediate impact of these technological developments and engage with all stakeholders to carefully monitor the nuanced risk picture currently faced and prevent AM from becoming an enabler of biological weapon proliferation.

1. INTRODUCTION

Additive manufacturing (AM), often referred to as “3D printing”, describes a range of manufacturing processes in which an object of almost any shape is built by adding and fusing together layers of material. While AM has a long history as a rapid prototyping technology, it has more recently seen a renaissance, particularly due to the huge popularity and growth of the range of affordable AM machines using plastic polymers and the funding and strategic investment that has poured into the wider industry. The technique used by many of the simple desktop AM machines is similar to the functioning of a common desktop printer, thus often referred to as

"3D printers". However, AM includes a variety of manufacturing techniques. These include techniques to build objects made of metal or alloys with characteristics such as corrosion resistance, making them relevant for the production and development of weapons (Bundestag Committee on Education, Research and Technology Assessment, 2017). Products that have been additively manufactured to date range from basic forms of small arms to key components of rocket engines.

While aerospace and missile applications of AM have received significant attention in the last few years, AM applications related to the development, production and delivery of biological weapons (BW) have only more recently been identified as a possible source of concern. Both the Biological and Toxin Weapons Convention (BWC), the principal non-proliferation treaty banning the development, possession, stockpiling and transfer of BW, and the Australia Group, the multilateral export control regime concerned with BW and chemical weapons (CW), have recently started considering threats resulting from or facilitated by AM (Australia Group, 2019). Advances in and the greater availability of AM machines and technology have raised particular concerns as a profound challenge to the effective implementation of export controls (Brockmann & Bauer, 2018). Export controls have traditionally focused on controlling the physical movement of goods across national borders, while the implementation of controls on transfers of technology has proven much more difficult. Controls on tangible goods, such as AM machines, key components and feedstock materials, remain a cornerstone of the application of export controls to AM. However, AM enables an intangible transfer of technology, such as an email or another digital file transfer, to deliver a significant amount of the information required for the automatic production of an object and could thus enable proliferation, including to BW programmes. Most AM applications in the BW field are still developing, thus resulting in a nuanced risk picture. Nevertheless, these risks and the impact on BW proliferation are expected to grow as the technology matures and the specific skills required for effectively leveraging AM become more common.

There is only a limited literature that has investigated the technological capabilities of AM to contribute to a BW programme and BW proliferation and arms control challenges that result. The bi-annual assessments by a group of experts convened by the Swiss Spiez Laboratory, published in the "Spiez Convergence" reports (Spiez Laboratory, 2016; Spiez Laboratory, 2018), provide concise technical assessments of the capabilities of AM for BW and CW applications. A recent series of papers on "Emergence & Convergence" by the US National Defense University is another notable exception, particularly stressing the impact of the digitisation of emerging technologies, including AM (Bajema, 2018). Building on the work published in SIPRI's report "Bio Plus X: Arms Control and the Convergence of Biology and Emerging Technologies" (Brockmann et al., 2019), this paper first discusses AM technologies and in particular bioprinting, as well as the challenges AM poses to export control. It then discusses three specific areas of application of AM for the development, production and delivery of biological weapons. It concludes with a summary of the resulting risk picture and select policy recommendations.

2. Export control challenges and biological weapon proliferation risks posed by additive manufacturing

2.1. Additive manufacturing and bioprinting technology

AM is often treated as if it were one unitary technology, however, it is better described as a category of automated manufacturing techniques. The main commonality of these techniques is the deposition and fusing of layers of materials. These techniques can be used to build an object of virtually any shape or form, reducing the loss of material and enabling more complex objects and new performance characteristics (Fey, 2017). An increasing variety of materials can be used as feedstocks to produce objects using these techniques, including polymers, resins, metal powders and so-called bioinks.

One technique that is currently receiving particular attention is bioprinting (Noor et al., 2019; Derakhshanfar et al., 2018). In contrast to the inanimate materials used as feedstock by other AM techniques, bioprinting constructs objects made from biological materials such as living cells. Using bioinks involves the added complexity of their high sensitivity to environmental conditions, growth and differentiation factors, and the particularities of the construction of tissue. In bioprinting, the bioinks are deposited using, for example, small nozzles for extrusion or an inkjet to achieve precisely layered arrangements of cells and support structures (Ji & Guvendiren, 2017). These materials then grow into functional tissue based on the cells' biological processes.

2.2. Export control challenges posed by additive manufacturing

AM promises to bring production to the end-user. It could decentralize production and thus reduce the need for the physical transportation of goods across borders (Palmer, 2015). AM is also said to be "deskilling" certain aspects of manufacturing, making it easier for producers with less knowledge and experience to produce more complex products. This characterisation should however be used with caution and it is better to view AM as causing a shift in knowledge and skill requirements rather than their reduction. However, AM does threaten to provide a substitute for other, controlled production techniques and the associated equipment, thus potentially enabling the circumvention of the barriers imposed by export controls. Perhaps more crucial than the new performance characteristics it enables is the increased digitization and automation of this production technology. As such, it further increases the importance of intangible transfers of technology—particularly the digital build files which encode both the characteristics of the object to be produced and the commands for the AM machine—which can easily be transferred for example via e-mail (Stewart, 2016; Brockmann, 2018). Compared to physical goods, digital transfers of technical data are harder to track and control (Bromley and Maletta, 2018). Moreover, the specialized audit capabilities to verify compliance with technology export controls are still very rare. States must, therefore, rely on intelligence and law enforcement information to detect illicit transfers and internal compliance mechanisms in companies are ever more important.

2.3. Potential applications of additive manufacturing in biological weapons development, production and delivery

AM has a range of potential applications in the development, production and delivery of biological weapons. All of these are still evolving—as with almost all AM technologies—and thus provide a moving target for regulatory measures (Spiez Laboratory, 2016). Among the many potentially relevant applications of AM, three are worth particular consideration:

Printing of production or laboratory equipment

AM can be used to print components of production and laboratory equipment and other items required for the production of biological weapons. In this way, AM could limit the footprint—acquisition of particular equipment, materials and specialized knowledge—of a clandestine biological weapon development or production effort. There are however also several technical barriers that currently remain: Especially when using polymers, chemical compatibility and resistance still limit the range of materials that can be used (Spiez Laboratory, 2018; Heikkinen et al., 2018). Moreover, there has so far only been limited testing of relevant properties of products and how printed items interact with chemicals and biomaterials. While AM may offer an alternative production pathway for some parts and equipment, it currently only results in a modest substitution effect as much of the equipment that is of concern can already be acquired through commercial providers for laboratories and the pharmaceutical industry. Using new AM techniques for this purpose likely still involves more significant technical expertise, knowledge and process development requirements (Fairchild et al., 2017). This means that only under very specific circumstances an actor may choose to pursue this pathway to manufacture production or laboratory equipment.

Bioprinting of tissue samples

Among the many positive applications of bioprinting in medicine (Ventola, 2014), the printing of tissue for pharmacological testing is potentially also relevant in the context of the development of biological weapons (Spiez Laboratory, 2016). Such synthetic tissue is already being used to test pharmaceutical compounds for toxicity and other characteristics. As this technology matures, bioprinted samples may be used for biomedical research and testing that is involved in the development of biological weapons (Zilinskas & Mauger, 2015). For example, bioprinted tissue could be used to assess specific interactions between biological agents and certain tissue types under conditions that are otherwise difficult to simulate. However, these techniques are not uniquely enabling (Fairchild et al., 2017). Established methods, such as animal testing, are currently still more accessible and require a more common set of knowledge and skills. While bioinks and suitable printers are commercially available, the knowledge required to take advantage of this technology is less accessible to an actor with malicious intent.

Printing of delivery systems or their components

Potential risk scenarios like terrorists using adapted commercial drones to disperse a biological weapon have long been known to experts (Bajema, 2018). The use of AM to produce components for delivery systems such as drones contributes to making their designs more adaptable, increase their capabilities and could thus make them more suitable for use as a delivery system for biological weapons. Plans and build files for printable parts of commercially available drones are openly shared in the do-it-yourself (DIY) community. Simultaneously, the capabilities and customizability of off-the-shelf drones have also increased (Dura, 2018). Certain spray tanks and types of nozzles that are already subject to export controls can be produced using AM. However, the relatively low level of sophistication of these parts means that they do not necessarily present a major obstacle to their acquisition by a state or a non-state actor.

3. Nuanced risk picture and select policy recommendations

The applications of AM relevant to the development, production and delivery of biological weapons are still relatively unknown. However, developments in bioprinting, as well as in the printing of drone components and laboratory equipment, continue at a rapid pace due to commercial and scientific interests—and an active DIY community. While relevant applications of AM currently still require considerable talent recruitment and process development efforts, particularly the digitized and automated nature of AM will likely mean that these barriers will be successively removed. Although the convergence of biotechnology and AM currently only produces moderate biological weapon proliferation risks, these are expected to increase (Brockmann et al., 2019). It is thus important to neither under- nor overestimate the immediate impact.

Discussions in the AG on if and how to exert controls over the transfer of relevant goods and technologies area are therefore confronted by a difficult array of challenges. These include tracking advances in a rapidly evolving set of technologies and defining the associated risks. At the same time, export controls should not stifle developments for civilian applications of these technologies. Many of the challenges posed by AM extend beyond the biological and chemical weapons context and are relevant to missiles and the nuclear and conventional arms fields (Brockmann, 2018; Brockmann & Kelley, 2018). Thus, they are of interest to all the export control regimes. Members of the regimes should therefore consider it as a topic for possible dialogue between the regimes, in particular regarding potential technical parameters for controls on AM machines and controlling intangible transfers of technical data that are used in AM.

At the same time, while export controls are currently a focus of regulatory discussions in the context of AM, meeting the challenges it creates in connection with biological weapons requires a more comprehensive approach. As such, discussions in both the BWC and the AG also need to pay attention to the role of research ethics and risk mitigation procedures in relevant research fields. This would include a stronger emphasis on raising awareness about possible weapons applications at relevant universities, research institutes and in DIY communities, as well as the development of stronger industry compliance and due diligence standards (Bauer et al., 2017). States thus need to engage with all stakeholders and carefully monitor the nuanced risk picture currently faced to prevent AM from becoming an enabler of biological weapon proliferation.

References

Australia Group. (2019, July 15). *Statement by the Chair of the 2019 Australia Group Plenary* (Press release). URL: Retrieved from https://australiagroup.net/en/2019-ag-plenary-statement.html

Bajema, N. E. (2018). WMD in the digital age: understanding the impact of emerging technologies. *Emergence & Convergence Research Paper*, 4. Washington D.C., USA: National Defence University.

Brockmann, K. (2019, July 29). Advances in 3D printing technology: Increasing biological weapon proliferation risks? *WritePeace Blog*. Retrieved from https://www.sipri.org/commentary/blog/2019/advances-3d-printing-technology-increasing-biological-weapon-proliferation-risks

Brockmann, K. (2018, August 1). 3D-printable guns and why controls on technical data matter. *WritePeace Blog*. Retrieved from https://www.sipri.org/commentary/blog/2018/3d-printable-guns-and-why-export-controls-technical-data-matter

Brockmann, K., & Bauer, S. (2018). *3D printing and missile technology controls.* Stockholm, Sweden: SIPRI.

Brockmann, K., & Kelley, R. (2018). The Challenge of Emerging Technologies to Non-proliferation Efforts: Controlling Additive Manufacturing and Intangible Transfers of Technology. Stockholm, Sweden: SIPRI.

Brockmann, K., Bauer, S., & Boulanin, V. (2019). *Bio Plus X: Arms Control and the Convergence of Biology and Emerging Technologies*. Stockholm, Sweden: SIPRI.

Bromley, M., & Maletta, G. (2018). The Challenge of Software and Technology Transfers to Non-proliferation Efforts: Implementing and Complying with Export Controls. Stockholm, Sweden: SIPRI.

Bundestag Committee on Education, Research and Technology Assessment. (2017). *Technikfolgenabschätzung (TA): Additive Fertigungsverfahren (3-D-Druck)*. Drucksache no. 18/13455.

Derakhshanfar, S., Mbeleck, R., Xu, K., Zhang, X., Zhong, W., & Xing, M. (2018). 3D bioprinting for biomedical devices and tissue engineering: A review of recent trends and advances. *Bioactive materials*, 3(2), 144–156.

Dura, K. (2018, October 13). The reality of armed, commercial drones. *The National Interest*. Retrieved from https://nationalinterest.org/blog/buzz/reality-armed-commercial-drones-33396

Fairchild, S., Kennedy, C. R. M., Mauger, P., Savage, T. J. & Zilinskas, R. A. (2017) Findings from the 2016 Symposium on Export Control of Emerging Biotechnologies, *James Martin Center for Nonproliferation Studies (CNS) Occasional Paper*, 26. Monterey, USA: Middlebury Institute of International Studies.

Fey, Marko. (2017). 3D Printing and International Security: Risks and Challenges of an Emerging Technology. *PRIF Report*, 144. Frankfurt, Germany: Peace Research Institute Frankfurt.

Heikkinen, I. T. S., Kauppinen, C., Liu, Z., Asikainen, S. M., Spoljaric, S., Seppälä, J. V., Savin, H., & Pearce, J. M. (2018) Chemical compatibility of fused filament fabrication-based 3-D printed components with solutions commonly used in semiconductor wet processing. *Additive Manufacturing*, 23, 99–107.

Ji, S., & Guvendiren, M. (2017). Recent Advances in Bioink Design for 3D Bioprinting of Tissues and Organs. *Frontiers in bioengineering and biotechnology*, 5, 23.

Noor, N., Shapira, A., Edri, R., Gal, I., Wertheim, L., & Dvir, T. 3D Printing of Personalized Thick and Perfusable Cardiac Patches and Hearts. *Advanced Science*, 6, 1–10.

Palmer, M. (2015). Ship a design, not a product! Is 3D printing a threat to export controls? *World ECR*, 43, 30-31.

Spiez Laboratory. (2016). *Spiez Convergence: Report on the Second Workshop, 5–8 September 2016*. Spiez, Switzerland: Spiez Laboratory.

Spiez Laboratory. (2018). *Spiez Convergence: Report on the Third Workshop, 11–14 September 2018*. Spiez, Switzerland: Spiez Laboratory.

Stewart, I. J. (2016). *Examining Intangible Controls*. London, UK: Project Alpha, Centre for Science and Security Studies, King's College London.

Ventola, C. L. (2014). Medical applications for 3D printing: current and projected uses. *Pharmacy and Therapeutics*, 39(10), 704–711.

Zilinskas, R. A. & Mauger, P. (2015). Biotechnology E-commerce: A Disruptive Challenge to Biological Arms Control. *James Martin Center for Nonproliferation Studies (CNS) Occasional Paper*, 21. Monterey, USA: Middlebury Institute of International Studies.

Gene Drive – Technology with Dual-Use Potential?

JOHANNES L. FRIEß

UNIVERSITY OF NATURAL RESOURCES AND LIFE SCIENCES, VIENNA (BOKU), INSTITUTE FOR SAFETY/SECURITY AND RISK SCIENCES

[#22-PAPER]

ABSTRACT

Synthetic gene drives are a novel technology which is heavily researched on. This genetic technology can be used to, over a number of generations, either drive selected traits into the majority of the population or suppress unwanted population. This promises to shape whole wild populations or even species according to our will. GDs may be applied in the fields of public health, for agricultural, and in ecology conservation. Currently, however, the technology is far from controllable in its spatiotemporal spread. It has to be feared that a suppression of invasive rodents in New Zealand would spread to the continents, likely tipping over established ecological networks for many generations. Proponents of the technology eagerly stride forward in their ambition to release the first gene drives into the wild, preferably sooner than later, while gene drives still pose an enormous challenge to regulators and policy makers. It is obvious that this topic harbors a high conflict potential even without mentioning potential military or adverse applications. Exploratory scenario settings for different proposed or imaginable applications shall provide an insight into potential benefits, issues, problems, failures and conflicts that might arise from this rather premature technology that has already been called a silver bullet.

1. INTRODUCTION

In a gene drive (GD), genetically manipulated organisms with customized traits are released into wild populations. These gene drive organisms (GDOs) are designed to pass their transgenic trait on to their offspring in a higher ratio than would usually be possible due to the Mendelian laws of inheritance. Depending on the customized trait — over generations — this Super-Mendelian inheritance allows the GDOs to either drive their genes into the vast majority of a population to change its properties or cause a population suppression of an unwanted species. However, the confineability of a GD is still questionable, posing the risk of uncontrolled spread, harboring unpredictable ecological consequences up to the global conversion or suppression of a whole species and effects cascading from that. Although limitation strategies are researched upon (Min et al. 2017a, 2017b; Noble et al. 2016; Wu et al. 2016), none has yet reached a stage beyond initial laboratory experiments.

GDOs will be released into wild habitats instead of artificial, agricultural ecosystems and corresponding genetic alterations will irreversibly remain for multiple generations instead of just one crop season. Conventional GMOs are meant not to proliferate, while GDOs are designed to do exactly that and even more successfully than their wild conspecifics. Thus, the technology collides with the regulations for the release of conventional genetically modified organisms (GMOs) (Simon et al. 2018). Moreover, a GD once released will not adhere to national boundaries. Since some species that should be suppressed or altered may be protected in some and regarded as pests in other countries, a unified regulation is direly needed. Even more so, the advent of GD-research shows an imminent threat of the technology to become a business plan for the agro-industry where more and more ideas are spun to manipulate agricultural pest insects. On the other hand, the US military research agency (DARPA) is currently the biggest funding agency for GD-research (~$ 100 million) (ETC Group and Heinrich-Böll-Stiftung 2018), looking for a way to detect GDs in the wild that have been released by error or malintent ("DARPA: Safe Genes,"). Implying a certain fear that GD technology may be weaponized and secretly deployed against crop plants or even humans. Taken together, the character of the technology and possible impacts of side effects and misuse show that certain applications of GDs bear a high conflict and possibly even dual-use potential.

2. METHOD AND RESULTS

Three prospective, exploratory scenarios will be developed in order to provide insights into the political, legal, as well as ethical challenges and blind-sides for the potential application of gene-drives. By using an inductive methodology, the scenarios will be built up step-wise according to the existing knowledge of technical as well as institutional and regulatory contexts for potential GD applications.

The scenarios are based on gene drive applications in agriculture, public health and conservation. Each scenario will be scrutinized according to their intended, beneficious consequences, their potential unintended side effects and possible accidental consequences. Furthermore, the responsibility of governance and regulation will be assessed as well as the liability in the case of negative consequences.

These scenarios are planned to give useful insights into the potentially upcoming socio-political issues and conflict potentials linked to gene drive technology. Thereby they contribute to (pre-emptive) policy and regulatory development but also fundamentally seek to raise awareness among a diverse set of stakeholders for the complex social, political, and ethical challenges associated with the application of gene drives and their release into the ecosystem.

REFERENCES

DARPA: Safe Genes. (n.D.) Retrieved from https://www.darpa.mil/program/safe-genes.

Montenegro de Wit, M. (2019). Gene driving the farm: who decides, who owns, and who benefits?. *Agroecology and Sustainable Food Systems*, 1-21..

Min, J., Noble, C., Najjar, D., & Esvelt, K. (2017). Daisy quorum drives for the genetic restoration of wild populations. *BioRxiv*, 115618.

Min, J., Noble, C., Najjar, D., & Esvelt, K. M. (2017). Daisyfield gene drive systems harness repeated genomic elements as a generational clock to limit spread. *BioRxiv*, 104877.

Montenegro de Wit, M. (2019). Gene driving the farm: who decides, who owns, and who benefits?. *Agroecology and Sustainable Food Systems*, 1-21.

Noble, C., Min, J., Olejarz, J., Buchthal, J., Chavez, A., Smidler, A. L., & Esvelt, K. M. (2019). Daisy-chain gene drives for the alteration of local populations. *Proceedings of the National Academy of Sciences*, *116*(17), 8275-8282.

Simon, S., Otto, M., & Engelhard, M. (2018). Synthetic gene drive: between continuity and novelty: Crucial differences between gene drive and genetically modified organisms require an adapted risk assessment for their use. *EMBO reports*, *19*(5), e45760.

Wu, B., Luo, L., & Gao, X. J. (2016). Cas9-triggered chain ablation of cas9 as a gene drive brake. *Nature biotechnology*, *34*(2), 137.

Three Decades of Chemical Weapons Destruction: Lessons for WMD Abolition

PAUL F. WALKER

INSTITUTE FOR PEACE RESEARCH AND SECURITY POLICY (IFSH), UNIVERSITY OF HAMBURG, AND ARMS CONTROL ASSOCIATION (ACA), WASHINGTON DC, USA

[#23-EXT.-ABSTRACT]

EXTENDED ABSTRACT

The Chemical Weapons Convention (CWC) was opened for signature in January, 1993, and entered into force four years later, April 29, 1997. Today it includes 193 States Parties, with only four countries – Egypt, Israel, North Korea, and South Sudan – remaining outside the treaty regime. Of these four, Israel has signed but not ratified the treaty. There is also another important country, Taiwan, which is not a member due to the opposition of China against any inclusion of Taiwan in any multilateral regime. Taiwan, however, contains one of the world's largest chemical industries and therefore remains important to the CWC.

The CWC is, therefore, the most universal of all arms control and disarmament treaties with the most States Parties of any multilateral regime today except the United Nations. It is therefore useful to look at the CWC as a model weapons abolition treaty, and to draw conclusions regarding successful weapons abolition regimes.

The CWC's implementing agency, the Organization for the Prohibition of Chemical Weapons (OPCW), is located in The Hague, The Netherlands, with about 475 international employees and an annual budget of 70 million Euros. The treaty is very comprehensive in banning all chemical weapons, including development, production, testing, stockpiling, and use. It does not ban limited research in chemical agents for defensive purposes, and also does not ban the use of riot control agents (RCAs) such as tear gas for non-military purposes.

The CWC mandates the declaration and verified elimination of all chemical weapons programs and stockpiles and has therefore overseen the safe and permanent destruction of declared chemical weapons stockpiles in eight countries to date – Albania, India, Iraq, Libya, Russia, South Korea, Syria, and the United States. These eight CW possessor countries have declared a total of 72,304 metric tons of chemical agents, of which 70,199 metric tons, about 97%, have already been safely eliminated as of June 30, 1999.

The United States was the first country to begin destruction of its large stockpile in 1990, seven years before the CWC entered into force but partly as a result of the prior bilateral agreements between Russia and the US in the late 1980s to unilaterally and reciprocally eliminate their CW stockpiles. The US had nine large CW stockpiles holding 28,577 metric tons (31,501 US tons) in 1990, but was able to destroy 1,436 metric tons by the CWC's entry into force (EIF) in 1997. So the US total was 27,141 metric tons (29,918 US tons) at EIF. Of these totals, 26,671 metric tons have now been destroyed, about 93%, leaving two stockpiles currently operating at Blue Grass, Kentucky, and Pueblo, Colorado. These are both scheduled to finish destruction by the end of 2023. Total costs for this program will exceed $40 billion, more than twenty times initial program estimates from the 1980s.

The Russian Federation declared the largest stockpile total, 40,000 metric tons of chemical agents at seven large stockpiles and began operating its first destruction facility in 2002, twelve years after the US began destruction. Russia completed its first-stage destruction process after fifteen years in 2017, although several hundred thousand tons of liquid toxic waste from its neutralization process still remain to be treated in second-stage processes. The total cost of Russia's program is estimated at $10 billion, with about a quarter of this provided by the Global Partnership (US, UK, Germany, Canada, and several other national contributors).

The other CWC States Parties which declared and destroyed their CW stockpiles are Albania (16 metric tons destroyed by 2007); South Korea (605 metric tons [estimated] destroyed by 2008); India (1,055 metric tons [estimated] destroyed by 2009); Libya (26 metric tons destroyed by 2014); Iraq which encased two large concrete bunkers with unknown amounts of chemical weapons and agents by 2014; and Syria (1,308 metric tons destroyed by 2014). Each of these former possessor countries has its own unique story to tell.

There have been many challenges to these stockpile destruction efforts, perhaps the largest being the enormous and unpredictable costs involved. At least five countries – Albania, India, Iraq, Libya, Russia, and Syria – have relied on foreign financial and technical support, while three countries – India, South Korea, and the United States – have funded their own programs. A second major challenge has been the development of safe and reliable technologies for destruction of these dangerous agents and related materials including explosives and rocket propellant; major disputes have broken out between high-temperature processes, especially incineration, and wet-chemistry processes, especially neutralization. Environmental and public health regulators have generally chosen neutralization as more manageable and measurable, while militaries have preferred incineration as faster and more mature.

A third major challenge has been the ongoing inspection and verification of destruction, especially since the most recent use of chemical weapons in the Syrian conflict since 2012. Although Syria declared its chemical weapons stockpile – 1,308 metric tons – in 2013 when it joined the CWC, and allowed its destruction by the US, Germany, Finland, and the UK, it has been shown that chemical weapons attacks have continued in Syria through 2018. The Fact-Finding Mission (FFM) of the OPCW has shown that chlorine, mustard, and sarin nerve agent have been used numerous times, and the Joint Investigative Mechanism found that the Syrian military and the Islamic State were both the perpetrators of these attacks.

Another example of the use of deadly chemical agents has been the assassination of Kim Jong-nam, the half-brother of North Korean leader Kim Jong-un, in Kuala Lumpur, Malaysia on February 13, 2017, with VX nerve agent. This murder was undertaken by North Korean agents but North Korea does not belong to the CWC. It clearly illustrated that North Korea has the ability to produce the most advanced nerve agents, and the country is thought to deploy over 5,000 metric tons of agents in chemical artillery shells.

Another important assassination attempt took place in March, 2018 when the former Russian spy, Sergei Skripal, and his daughter, Julia, were attacked with a military-grade nerve agent in Salisbury, UK. Fortunately, they both survived the attack, reportedly by two Russian agents, but two other UK citizens were subsequently injured four months later after finding the nerve agent disguised as a perfume bottle; one victim, Dawn Sturgess, died as a result of this. This crime has been raised in the OPCW meetings since then, but Russia denies any responsibility for the attack.

Two additional challenges to note include the need for all CWC States Parties to declare their past chemical weapons-related activities and to annually report all activities, including imports and exports of scheduled chemicals, to the OPCW. All States Parties must also fully implement the treaty domestically by establishing a National Authority and legislative initiatives. Only about 50-60% of States Parties today have met these obligations. And lastly, the OPCW and CWC require much more public support and awareness of this international effort to ban a whole class of weapons of mass destruction; while the OPCW has made progress with the establishment of an Advisory Board on Education and Outreach (ABEO), and non-governmental organizations have established a network of NGOs and civil society stakeholders – the “CWC Coalition,” much more needs to be done.

In conclusion, eight broad lessons for weapons abolition can be noted: (1) Treaty implementation requires broad national and public support, both financially and politically. (2) An experienced and effective inspectorate and verification group are needed to build confidence in the regime. (3) On-site and challenge inspection options are required. (4) Annual reporting requirements for States Parties must be enforced. (5) A Scientific Advisory Board (SAB) is critical to track technology development and relevance. (6) Public outreach, training, awareness-raising, and capacity-building are critical to strengthen the treaty regime. (7) Investigative mechanisms are necessary for examining allegations of use of banned agents and weapons and for identifying perpetrators, both state and non-state. And (8) capable and licensed laboratories for sample testing and forensic analysis are critical to treaty implementation.

The Chemical Weapons Convention is an excellent model for other international arms control, disarmament, and abolition treaties and is clearly helping to build a more safe and secure world.[1]

[1] Further information can be found at www.opcw.org

Science and (Bio)Chemical Disarmament: Friends or Foes?

JONATHAN E. FORMAN

SCIENCE POLICY ADVISER AND SECRETARY TO THE SCIENTIFIC ADVISORY BOARD ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS

[#24-EXT.-ABSTRACT]

EXTENDED ABSTRACT

The Chemical Weapons Convention is a treaty underpinned by science and technology, with implementation requiring broad scientific and engineering skills and knowledge. This is clearly seen at an operational level where toxic chemicals must be destroyed, chemical analysis and inspection of chemical production facilities are required, assistance and training for response to chemical incidents must be provided and all the Nation States party to the treaty are encouraged to use science itself as a tool for international cooperation for economic and technological development. Furthermore, decision makers serving in policymaking organs of international arms control, disarmament and non-proliferation instruments often consider and review information with significant scientific dimensions, requiring they have adequate levels of scientific literacy and access to scientific advisors. Yet, a ban on chemical weapons is often viewed from a perspective of mistrust to science of chemistry – the scientific discipline most closely associated with this class of weapons of mass destruction.

Twenty-first century scientific and technological development is a trans-disciplinary, dynamic and rapidly evolving endeavour that is enabled by the emergence of new and innovative technologies, and the repurposing of existing technologies for unanticipated new applications. New advances across the chemical sciences come forward through ideas and tools originating from sectors outside this discipline (and chemistry itself influences other scientific disciplines in a similar manner), and relevant developments may not be easily recognized by a scientific review limited to chemical-specific fora. For those viewing science with distrust and concern over its potential misuse, the ecosystem of scientific and technological change brings uncertainty on what impact it may have on disarmament and non-proliferation. Those assessing impact of technological change on the Chemical Weapons Convention are confronted with many potential challenges for treaty implementation not the least of which is the challenge of recognizing where to look, and how to identify relevant advances. A significant challenge of scientific advancement viewed through a prism of distrust, is the risk of losing access to critical knowledge about known chemistry and chemicals of relevance to the treaty. Advances, however, can also be enabling for treaty implementation, providing opportunities for recognising when something

is “unusual” or out of place – focusing on warning signs in place of simply a new scientific development or innovation.

The presentation discussed areas of concern often associated with posing a risk to the Convention Weapons Convention, along with how science is advancing and what is driving it forward. Approaches to addressing the inevitable scientific and technological evolution, that in future, will influence the operating environment of chemical weapons (and other) non-proliferation and disarmament regimes were also explored. A lack of scientific literacy puts implementation of a chemical disarmament and non-proliferation at risk of being ineffective, demanding that science be viewed not from a perspective of fear, but from with practical views on the capabilities necessary for success.

Dual Use Research of Concern – Who Talks About What with Whom?

Jan Opper

Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg

[#25-EXT.-ABSTRACT]

Extended Abstract

Dual use research of concern or DURC for short became a widely discussed topic within the life sciences. One commonly used definition for DURC is: “[Research that] Based on current understanding, can be reasonably anticipated to provide knowledge, products, or technologies that could be directly misapplied by others to pose a threat to public health, agriculture, plants, animals, the environment, or materiel.”(National Science Advisory Board for Biosecurity, 2006, 4). The misuse of biological agents for hostile purposes might be older than the study of said agents themselves. Germs have been used as weapons in various instances throughout history. Since World War I preparations for biological warfare took place in some states, reaching a peak during the Cold War where biological warfare agents where produced on industrial scale on both sides of the Iron Curtain (for history of bio-weapons production and use see various authors in: Lentzos, 2016). The 1972 Convention on the Prohibition of Biological and Toxin Weapons (BWC) categorically banned any possession of pathogens and toxins in quantities large enough for non-peaceful purposes by member states (UNOG, 1972).

However, 2001 saw a renewed concern in the possibility of bioweapons usage, this time primarily by non-state actors. The case of “Ameritrax” as well as a general fear that terrorists might conduct attacks with weapons of mass destruction brought biological weapons back on the international security agenda (Vogel, 2016). Recent breakthroughs in the life sciences, namely in synthetic biology and genome editing, led to the fear that malicious actors might (mis-)use this research for their own purposes. In this respect, the international debate surrounding gain-of-function experiments with genetically engineered influenza virus strains is of importance. Two laboratories, one in the USA and one in Europe submitted manuscripts including details of the work which gave raise to concern due to the perceived misuse potential. The European research group headed by Ron Fouchier genetic analyzed the spread of avian influenza between mammals and conducted experiments that led to the successful infection of ferrets with a modified H5N1 virus through the air. While Fouchiers experiment itself can be designated as a success as it produced the desired results, many in the biosecurity community feared that the knowledge gained through his research could be used for hostile purposes. This brings us to a fundamental difference between the current DURC discussion and the discussion about non-proliferation of biological weapons during the Cold War: While Cold War non-proliferation measures were mainly focused on the control over the flow of materials necessary to build WMD the regulation of DURC will be mainly concerned with control of the knowledge that might be used to create or use pathogens for non-peaceful purposes.

Currently, there is a demand for the implementation of DURC regulations at different levels. However, even the very broad DURC definition mentioned above is not uncontested and there is no agreement on what kind of DURC regulation would be adequate, who should be the regulating body or what would fall under such a regulation. Over the last years, a number of proposals on how to handle the security implications of DURC have been put forwards by international organizations, national governments, non-governmental organizations, including scholarly academies and individual researchers participating in the current debate. Germany started some time ago to makes efforts in regulating DURC. The National Ethics Council (Ethikrat, 2015) as well the Leopoldina scholarly society (e.g.: Hacker, Fritsch, and Deutsche Akademie der Naturforscher Leopoldina, 2015) put forward proposals on dealing with DURC and research with security implications in a broader sense. At the same time, government agencies are active on the EU level to achieve a harmonized regulation (e.g.: European Commission, DG Research and Directorate E: Biotechnology, Agriculture and Food Research, 2004)

Regulations and their concrete content are one type of what is called a policy in the social sciences. Policies are concerned with the concrete output of political process. Negotiating what kind of regulation is needed for DURC (even if such negotiations are informal) is precisely that - a political process (Fuhse, 2005 with reference to Easton, 1965, 349 f.) The Oxford Handbook of Public Policy Studies describes Policy as “[…] the business end of political science” […](Oxford Handbooks, 2009). Policies, as the outcome of political processes, are usually concerned with the question of “who gets what and when” (Lasswell, 1936). or maybe more fitting in the current case of the DURC debate: who is allowed to do what and when, because here we look at a restricting policy rather than one that deals explicitly with the distribution of goods and services. Policy making is often seen as a “rational” undertaking in which experts and decision makers identify a clear-cut problem, consider alternative approaches to address the problem, find the “best” solution to it and implement this solution effectively (Fischer, 2007, 98 f.). However, when taking a social constructivist stance, policies are no longer the impartial solutions to clearly defined problems they are often presented as.

Social Constructivists argue that there is no such thing as objective truth or knowledge. Instead, what we perceive as reality is produced (or constructed) and reproduced through discursive means and while we as a society share certain basic concepts (this is what we call culture, a system that lets us understand each other and accept certain knowledge as universally “true” (Hall, 1997, 4 ff.), specific knowledge, e.g. the specific properties of a technology, is often contested (for policies see: Fischer, 2007, 100 ff.; Yanow, 2000, 5 ff. for technology see: Grint & Woolgar, 1992)

The same holds true for policy making. Analysing policies can reveal which kind of knowledge is perceived as “true” by its makers. Policy has certain experiences, values and interests, that let seem see problems in a specific light. Those values are reflected within the polices they create and are reproduced through the enactment of those policies. Thus, policies create meaning in their respective issue area (Yanow, 1996, 2000, 5ff.). Such an approach takes a closer look at the policies regulating DURC and treats policy documents itself as data. Using interpretive methods, in particular content analysis, can reveal the meanings, knowledge and values contained in the policy documents, make them comparable and allow insights in the "local" knowledge of different policy actors e.g. how they organise ideas and concepts (Yanow, 2000, 20 ff.; Wright, Shore & Pero, 2011, 3). Since policies are not only a reflection of their maker's values but an entity that constructs meaning itself, they are a window into the larger process of DURC regulation (Wright & Reinhold, 2011, 108; Yanow, 1996). What is proposed here is taking into consideration German and EU policy documents in order to show how actors approach DURC regulation in Germany and how they understand DURC. Important questions are for example how actors define DURC research and what is included in this definition and what not. Another interesting question is what kind of measures should be taken and who should be responsible for implementing them. While the first approach asks for the conception of DURC by the actors, the second set of questions are more concerned with how actors order their environment. This is very relevant to practitioners in the field since they have to deal with regulations once they are adopted. Here, deconstructing what is presented as 'objective' knowledge in the discussion can open a space for actors and knowledge that is usually overlooked and introduce it into the policy making process. This would allow researchers and their knowledge to contribute more to the policy making process.

REFERENCES

Easton, D. (1965). A Systems Analysis of Political Life. New York: Wiley.

Deutscher Ethikrat (2015). *Biosicherheit – Freiheit Und Verantwortung in Der Wissenschaft*. Jahrbuch Für Wissenschaft Und Ethik 19, 1.

European Commission, DG Research, and Directorate E: Biotechnology, Agriculture and Food Research. (2004). *Ethical Implications of Scientific Research on Bioweapons and Prevention of Bioterrorism.*

Fischer, F. (2007). Policy Analysis in Critical Perspective. *Critical Policy Studies* 1, 1, 97–109.

Fuhse, J. (2005). David Easton. In J. Fuhse (ed.), Theorien des politischen Systems: David Easton und Niklas Luhmann. Eine Einführung (*20–63)*. Wiesbaden: VS Verlag.

Grint, K., & Woolgar, S. (1992). Computers, Guns, and Roses. Science, Technology, & Human Values, 17, 3, 366–380.

Hacker, J., Fritsch, J., & Deutsche Akademie der Naturforscher Leopoldina (Hrsg.). (2015). Freiheit und Verantwortung der Wissenschaften: Rechtfertigen die Erfolgschancen von Forschung ihre potentiellen Risiken? ; Dokumentation des Symposiums der Nationalen Akademie der Wissenschaften Leopoldina, der Deutschen Forschungsgemeinschaft und des Deutschen Ethikrates am 3. Nov. 2014 in Halle (Saale). Halle: Dt. Akad. der Naturforscher Leopoldina, Nationale Akad. der Wiss.

Hall, S. (ed.). (1997). Representation: Cultural representations and signifying practices. London; Thousand Oaks: Sage.

Herfst, S., Schrauwen, E. J. A., Linster, M., Chutinimitkul, S., Wit, E., Munster, V., Fouchier, R. (2012). *Airborne transmission of influenza A/H5N1 virus between ferrets.* Science, 336(6088), 1534–1541.

Lasswell, H. D. (1936). Politics: Who Gets What, When, How. New York; London: Whittlesey House McGraw-Hill Book Co.

Lentzos, F., (ed). (2016). *Biological Threats in the 21st Century*. London; Singapore: Imperial College Press.

National Science Advisory Board for Biosecurity. (2006). *NSABB Draft Guidance Documents.*

Oxford Handbooks. (2009). Oxford Handbook of Public Policy. Retrieved from http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199548453.001.0001/oxfordhb-9780199548453.

UNOG. (1972). Übereinkommen über Das Verbot Der Entwicklung, Herstellung Und Lagerung Bakteriologischer (Biologischer) Waffen Und von Toxinwaffen Sowie über Die Vernichtung Solcher Waffen. Retrieved from https://www.unog.ch/80256EDD006B8954/(httpAssets)/C4048678A93B6934C1257188004848D0/$file/BWC-text-English.pdf.

Vogel, K. M. (2016). Aftershocks of the 2001 Anthrax Attacks. In F. Lentzos (ed.), *Biological threats in the 21st century (211–237).* London; Singapore: Imperial College Press.

Wright, S., & Reinhold, S. (2011). „Studying Through“: A Strategy for Studying Political Transformation. Or Sex, Lies and British Politics. In S. Wright, C. Shore, & D. Pero (ed.), P*olicy Worlds* (86–104). New York; Oxford: Berghahn Books.

Wright, S., Shore, C., & Pero, D. (ed.). (2011). *Policy Worlds*. New York; Oxford: Berghahn Books.

Yanow, D. (1996). How does a policy mean? Interpreting policy and organizational actions. Washington, D.C: Georgetown University Press.

Yanow, D. (2000). Conducting interpretive policy analysis. Thousand Oaks, Calif: Sage Publications.

Misuse Potential of Systems Biology – New Challenges for Biological Arms Control?

KATHRYN NIXDORFF

BIOLOGY, TECHNISCHE UNIVERSITÄT DARMSTADT

[#26-EXT.-ABSTRACT]

EXTENDED ABSTRACT

Systems biology aims to understand how vital, complex physiological systems function, and how these systems interact with one another to function as a whole. In a systems biology approach in the life sciences, experimental data concerning the gene, protein, and informational responses of biological processes gained through wet lab studies are integrated into computer-assisted mathematical models designed to describe the structure of the system and its response to perturbations (Kumar, Pathak, Gupta, Gaur, & Pandey, D., 2015). The aim is to learn about relations among components of a system that cannot be identified by using traditional reductionist methods that study only individual units in a complex biological process. This procedure can provide a better understanding of the system's dynamics, which is the key to determining biological mechanisms and understanding disease (Hood et al., 2012). The field of systems biology is not new, but rather has its origin in mathematical theories of systems control dating back to the beginning of the 20th century. What is new is the convergence of high-throughput methodology for obtaining biological data and computational processing power that have led to a re-definition and expansion of the field (McDermott**,** Samudrala**,** Bumgarner**,** Montgomery & Ireton, 2009**;** Naylor & Chen, 2010)**.**

This research is yielding an enormous amount of information about specific targets of vital physiological processes and how these might respond to a perturbation. An example would be perturbation by a pharmacological therapeutic, thus paving the way for the innovative design of better drug candidates, which could be greatly beneficial in the diagnosis and treatment of complex diseases. At the same time, these studies have implications for biochemical security. In particular, work in this area has extended the spectrum of biological threat agents beyond the classical categories of microorganisms and toxins to include biochemical bioregulators, which to a great extent regulate the proper function of vital processes within the nervous, endocrine and immune systems. The bioregulators of relevance here are neurotransmitters/neuropeptides, hormones and cytokines. Accordingly, systems biology methods have been used to study host-microbe interactions and in particular host-parasite relations (Adarem et al., 2011) to aid in understanding infectious diseases. Systems biology has also been used to study immune functions (Wu & Chen, 2016) as well as intricate processes in the nervous system (Diaz-Beltran, Cano, Wall & Esteban, 2013; De Luca, Colangelo, Alberghina & Papa, 2018). In addition, this type of holistic approach has been actively applied to the investigation of complex diseases such as cancer (Filipp, 2017). Naturally, all these studies are directed at gaining information that can be decisive in steering vital physiological processes in a positive direction towards better health and well-being.

Normally, bioregulators are produced in optimal amounts to ensure the regulatory balance and proper function of physiological processes including respiration, heartbeat, body temperature, cognition, mood and immune responses. However, if they are produced in amounts greater or less than optimal, this causes an imbalance of physiological responses that can lead to dysfunction, damage and even death. A case in point is the much-publicized mousepox experiment published in 2001 (Jackson et al., 2001). In an attempt to control a plague of rodents in Australia, researchers developed a vaccine using a genetically engineered mousepox virus as vector, against which the mice were immune. They added a gene to the virus that encoded a protein on the surface of mouse oocytes designed to trigger an antibody response to the protein that would prevent fertilization. In order to boost the antibody response, the researchers added another gene encoding an immune system cytokine, interleukin-4 (IL-4), known to enhance antibody responses in general. However, as an unexpected result, the inoculated mice died. Apparently, overproduction of IL-4 suppressed the function of killer T cells necessary to contain the viral infection. The outcome of this study was the creation of a virus with enhanced lethality instead of a contraceptive (Ylönen, 2001). This example illustrates how overproduction of a bioregulator that is normally beneficial can be deadly as a result of imbalance of processes in a system as a whole, and underscores the need for a holistic approach in the study of interactions of components in vital systems.

When bioregulators as novel biochemical threat agents are combined with improved means of delivering these agents to their targets, you have the potential for the creation of novel biochemical weapons. Improved methods of delivery are most evident in connection with the administration of biochemical therapeutics in experimental and clinical studies. While methods of targeted delivery of therapeutics to treat disease do not exactly mimic those that would be most practical for delivery of biochemical agents as weapons, it is still possible to come to certain conclusions in these studies about the feasibility of the use of such methods for delivering biochemical agents for terroristic or biological warfare purposes.

The two fields of work that appear to be most relevant for both therapeutic purposes and biochemical warfare are viral and non-viral vector-directed delivery technologies, which are being actively applied in both clinical and experimental studies as part of cancer treatment, gene and immunotherapy. Non-viral vectors, sometimes referred to as nanorobots, are being developed to overcome some negative aspects of using viruses such as safety, immunity against viruses that diminish their effectiveness or limited transport capacity. Nanotechnology has played a fundamental role in many developments through the construction of defined nanoparticles for facilitated uptake through the tissues. Improvements in specific targeting and gene transfer efficacy of viral and non-viral vectors have made them much more feasible delivery systems. In particular, the delivery of viral and non-viral vectors over the aerosol route is increasingly being explored so that this is rapidly becoming a definitive option in therapeutic settings (Nixdorff, 2018). Aerosol delivery is also the preferred means of dissemination of biological warfare agents.

Biochemical security concerns in systems biology are embedded in the larger domain of cyberbiosecurity, which addresses the security vulnerabilities at the interface of the life sciences and digital worlds. There are many areas of interface, but one that has received much attention lately are robotic platforms known as cloud laboratories, operated by computers that receive a work order (software programming of the needed procedure and sequence of steps) carried out by an assemblage of machines (Cyberbiosecurity, 2019).

Biochemical bioregulators are relevant agents of concern for both the Biological Weapons Convention and the Chemical Weapons Convention. While the potential for misuse is certainly given, it is most difficult to assess just how actual the risk of misuse is in effect. In the end, the feasibility of delivering biochemical agents as weapons for terrorist or warfare purposes can only be determined by direct testing of the specific agents in a designated scenario. Nevertheless, there remains a need to be proactive in approaches to deal with the misuse potential of this research area. In particular, the expansion of the threat spectrum into new categories of agents has not received proper consideration either in the deliberations on how to come to grips with the dual-use issues involved or in actual formulation of oversight policies at national and international levels. The misuse potential of bioregulators as well as the feasibility of using such agents as weapons first received prominent attention when the Committee on Advances in Technology and the Prevention of their Application to Next Generation Bioterrorism and Biological Warfare Threats (the Lemon-Relman Committee) of the United States National Academies examined more closely the work of earlier investigators (Kagan, 2001; Dando, 2001; Wheelis, 2002) and issued its report in 2006 (National Research Council, 2006). Since that time, however, there has been little effort in formulating security policies so as to extend the categories of dual-use research of concern described in the Fink Committee Report (National Research Council, 2004) to include experiments with biochemical bioregulators in the context of systems biology research.

In Germany, the German Research Foundation (DFG) and the National Academy of Sciences, Leopoldina, have formulated recommendations (DFG & Leopoldina, 2014) for dealing with security-relevant research in all disciplines. Their recommendations, which revolve around dual use research of concern, include all the basic elements of an oversight programme, to be established on a voluntary basis. A Joint Committee of DFG and Leopoldina is assisting with the establishment of these recommendations at universities and other research institutions in Germany. Progress can be followed in regular reports along with other information available on the Joint Committee website (https://www.leopoldina.org/ueber-uns/kooperationen/gemeinsamer-ausschuss-dual-use).

REFERENCES

Aderem, A., Adkins, J.N., Ansong, C., Galagan, J., Kaiser, S., Korth, M.J., Law, G.N., McDermott, J.G., Proll, S.C., Rosenberger, C., Schoolnik, G. & Katze, M.G. (2011) A Systems Biology Approach to Infectious Disease Research: Innovating the Pathogen-Host Research Paradigm. *mBio*, Vol. 2, No. 1, Article e00325-10, 4 p.

Cyberbiosecurity (2019) See the special issue of *Frontiers in Bioengineering and Biotechnology* Vol. 7. Available at https://www.frontiersin.org/articles/10.3389/fbioe.2019.00235/full.

Dando, M. (2001) Genomics, Bioregulators, Cell Receptors and Potential Biological Weapons. *Defense Analysis*, Vol. 17, No. 3, 239-257. doi:10.1080/07430170120093373.

DFG & Leopoldina (2014) *Scientific Freedom and Scientific Responsibility*. Available in english and german at https://www.leopoldina.org/en/publications/detailview/publication/wissenschaftsfreiheit-und-wissenschaftsverantwortung-2014/.

De Luca, C., Colangelo, A.M., Alberghina, L. & Papa, M. (2018) Neuro-Immune Hemostasis: Homeostasis and Diseases in the Central Nervous System. *Frontiers in Cellular Neuroscience*, Vol. 12, Article 459, 8 pp. doi: 10.3389/fncel.2018.004591.

Diaz-Beltran, L., Cano, C., Wall, D.P. & Esteban, F.J. (2013) Systems Biology as a Comparative Approach to Understand Complex Gene Expression in Neurological Diseases. *Behavioral Science*s, Vol. 3, 253–272. doi:10.3390/bs3020253.

Filipp, F.V. (2017) Precision Medicine Driven by Cancer Systems Biology. *Cancer and Metastasis Reviews*, Vol. 36, 91–108. doi:10.1007/s10555-017-9662-4.

Hood, L.E., Omenn, G.S., Moritz, R.L., Aebersold, R., Yamamoto, K.R., Amos, M., Hunter-Cevera, J., Locascio, L. & Workshop Participants (2012) New and Improved Proteomics Technologies for Understanding Complex Biological Systems: Addressing a Grand Challenge in the Life Sciences. *Proteomics*, Vol. 12, No. 18, 2773–2783.

Jackson, R.J., Ramsay, A.J., Christensen, C.D., Beaton, S., Hall, D.F. & Ramsshaw, I.A. (2001) Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox. *Journal of Virology*, Vol. 75, No. 3, 1205-1210.

Kagan, E. (2001) Bioregulators as Instruments of Terror. *Clinics in Laboratory Medicine*, Vol. 21, No. 3, 607-618.

Kumar, A., Pathak, R.K., Gupta, S.M., Gaur, V.S. & Pandey, D. (2015) Systems Biology for Smart Crops and Agricultural Innovation: Filling the Gaps between Genotype and Phenotype for Complex Traits Linked with Robust Agricultural Productivity and Sustainability. *OMICS A Journal of Integrative Biology*, Vol. 19, No. 10, 581-601.

McDermott, J., Samudrala, R., Bumgarner, R.E., Montgomery, K. & Ireton, R. (Eds.) (2009) Preface (v). *Computational Systems Biology, Methods in Molecular Biology* series. New York, Humana Press.

National Research Council (2004) *Biotechnology Research in an Age of Terrorism.* Washington, D.C.: The National Academies Press. Available at http://www.nap.edu.

National Research Council (2006), *Globalization, Biosecurity and the Future of the Life Sciences.* Washington, D.C.: The National Academies Press. Available at http://www.nap.edu.

Naylor, S. & Chen, J.Y. (2010) Unraveling Human Complexity and Disease with Systems Biology and Personalized Medicine. *Personalized Medicine*, Vol. 7, No. 3, 275–289. doi:10.2217/pme.10.16.

Nixdorff, K. (2018) Chapter 9. Advances in the Targeted Delivery of Biochemical Agents, 259-291. *Preventing Chemical Weapons: Arms Control and Disarmament as the Sciences Converge.* M. Crowley, M. R. Dando & L. Shang (Ed.). London: Royal Society of Chemistry.

Wheelis, M. (2002) Biotechnology and Biochemical Weapons. *The Nonproliferation Review*, Vol. 9, 48-53.

Wu, C.-C. & Chen, B.S. (2016) Coordination of Defensive and Offensive Molecular Mechanisms in the Innate and Adaptive Host–Pathogen Interaction Networks. *PLoS ONE*, Vol. 11, No. 2, Article e0149303, 20 pp.

Ylönen, H. (2001) Rodent Plagues, Immunocontraception and the Mousepox Virus. *Trends in Ecology & Evolution*, Vol.16, No.8, 418-420.

Addressing Biotechnological Developments in the BWC Framework: Experiences and Options

UNA JAKOB

PEACE RESEARCH INSTITUTE FRANKFURT (PRIF)

### [#27-EXT.-ABSTRACT]

EXTENDED ABSTRACT

Around the same time that genetic engineering became a real option in the biological sciences in 1972, the Biological Weapons Convention (BWC) was concluded in Geneva. It entered into force in 1975, the same year the “Asilomar Conference” produced the first guidelines for the biosafety and governance of genetic engineering. These political and technological developments did not simply coincide; rather, biological disarmament and scientific and technological (S&T) developments have been intertwined from the outset. The BWC prohibits all biological agents and toxins “whatever their origin or method of production” (Article I (1)), anticipating that further technological advances might fall into that scope. It also stipulates that a review after five years shall “take into account any new scientific and technological developments relevant to the Convention” (Article XII). This task was replicated at all subsequent review conferences, most recently in 2016. All Final Declarations reaffirmed the comprehensive scope of Article I, but there was no systematic review or monitoring of S&T developments. The institutional options to address such developments in the BWC framework remain limited to date. At the same time, the rapid developments in the life sciences create an ever-increasing number of (potential or actual) challenges for biological weapons disarmament. These include for example a broader geographical spread of institutions and researchers, a wider and faster dissemination of knowledge, development of enabling and other technologies that make relevant research easier, cheaper and hence more accessible, and last but not least a deepening knowledge of (micro)biological functions. All of these developments have benign, useful and important roles, and listing them as challenges might seem counterintuitive. However, from a security perspective they all include a potential for misuse and malign application that needs to be monitored and contained in order to mitigate concerns about possible biological weapons proliferation, without unduly limiting scientific freedom. In recognition of these challenges, BWC states parties in 2011 agreed to include S&T review in the new intersessional work programme as one of the standing agenda items. The topic was hence addressed at the annual BWC meetings of

experts and states parties between 2012 and 2015. In the current intersessional process, S&T is again covered by one of the meetings of experts (MX 2) annually between 2018 and 2020. While this increased awareness of this issue among many stakeholders, it did not (yet) produce any more tangible results. States parties and non-governmental experts have developed numerous proposals on how to deal with S&T developments more effectively in the BWC context, including through establishing a science advisory body. Taking into account examples from other treaty regimes such as the Chemical Weapons Convention, the Comprehensive Test Ban Treaty or the Convention on Biological Diversity, the presentation will discuss these proposals and offer some reflections on the available options.

Recent Developments in Biological and Chemical Arms Control

Mirko Himmel

Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg

[#28-abstract]

Abstract

Biological and chemical weapons of mass destruction are banned by two international arms control treaties: the Biological and the Chemical Weapons Convention (BWC, CWC). Recent events, namely the frequent use of chemical weapons in Syria since 2012 and an assassination attempt in Great Britain in 2018 give rise to concerns that under certain conditions the re-emergence of chemical weapons cannot be prevented. In a politically tense atmosphere, a severe loss of trust can be recognised among CWC States Parties. Important questions such as the investigation of the alleged use of chemical weapons cannot any longer be solved in a constructive manner. The political situation within in the BWC regime is different, but not much better. There is still no agreed verification mechanism for this important arms control treaty. Compliance monitoring is relying in part on in-transparent methods. Science and technology are evolving fast, but a structured review of relevant developments is lacking. Within this context, political progress is slow and BWC States Parties experience difficulties to agree on necessary steps fostering the biological weapons ban. The adoption of new production concepts in the chemical industries, dual use aspects of new genetic engineering techniques as well as the convergence between biology and chemistry are some of the future challenges for biological and chemical arms control.

Disarmament, Arms Control and Non-Proliferation – Developments, Challenges, Solutions

OLIVER MEIER

GERMAN INSTITUTE FOR INTERNATIONAL AND SECURITY AFFAIRS (SWP), BERLIN

[#29-ABSTRACT]

ABSTRACT

Three types of disarmament, arms control and non-proliferation agreements have evolved. These regimes to regulate military relevant capabilities, technologies and capacities are faced with different trends. There have been major setbacks on classical arms control as a stability-oriented approach aims to reduce the risks of war, and prevent arms races. Non-proliferation regimes want to minimize the risks that sensitive technologies are misused for hostile purposes. These agreements still hold but there are serious problems, including non-compliance. Humanitarian arms control and disarmament wants to reduce the level of suffering caused by weapons during and after conflicts and focuses on how weapons are used. There has been some progress on humanitarian arms control.

There are three core conditions for the success of arms control, non-proliferation and disarmament agreements. These accords have to be able reduce the security dilemma, must be supported by and implemented faithfully by a vast majority of governments (particularly great powers) and they must be able to adequately absorb technological developments. These conditions can no longer be taken for granted.

One problem is that great powers and particularly Russia and the United States have turned against arms control. At the same time, no new arms control champions have emerged and the emergence of new technologies raises doubts about the effectiveness of arms control regimes.

To tackle these challenges, middle powers like Germany, should attempt to seize four opportunities. First, they should try to secure the acquis and build on arms control successes. Second, they should use the normative power of agreements to pave the way towards binding and verifiable treaties. Third, they should take advantage of new types of governance, in particular to strengthen controls of proliferation-sensitive technologies. Finally, they should work in groups of like-minded states to strengthen arms control, nonproliferation and disarmament agreements.

Determination of Analog Structures as Instrument for the Risk Assessment of Hazardous Chemicals

Volkmar Vill, Gesine Rempp and Mirko Himmel

Institute of Organic Chemistry, University of Hamburg

[#30-Abstract]

Abstract

The evaluation of chemical hazards is object of numerous national and international regulations. The misuse of highly toxic substances for hostile purposes is prohibited by the Chemical Weapons Convention (CWC), an international arms control treaty. Known chemical warfare agents (CWA) and precursor chemicals for their production are listed in the schedules of chemicals in the annexes to the CWC. Additionally, group definitions for chemicals are used in order to cover numerous derivatives of CWA. Lists of individual substances are often recorded as static lists in databases, while structure definitions must be interpreted “on the fly” by experts and translated manually into derivatives of a given parent structure. This process is tedious and prone to mistakes. For chemical arms control, it would be desirable to translate chemical information submerged in the structure definitions into a computer-interpretable form. The database tool SciDex has been developed in the working group of Volkmar Vill. This tool is capable of performing an assessment of chemical hazardous substances. Translating legal texts into computer-based assessment algorithms allows mapping of relevant regulations which apply to a given chemical compound, even to new ones. Furthermore, specific structural analogies can be used to predict approximations of individual physicochemical properties of compounds not listed in a database through comparison of close structural derivatives with known properties. The computer algorithm is capable of identifying chemical substances which have, due to their structure, properties quite similar to those mentioned in the CWC schedules. SciDex is a dynamic database tool which can be used efficiently for preventive chemical arms control and trade monitoring purposes.

Biological Weapons – Sources for (Mass-) Disruption?

HARES SARWARY AND GUNNAR JEREMIAS

CARL FRIEDRICH VON WEIZSÄCKER-CENTRE FOR SCIENCE AND PEACE RESEARCH (ZNF), UNIVERSITY OF HAMBURG

## [#31-ABSTRACT]

ABSTRACT

Biological Weapons are identified as weapons of mass destruction within the arms control discourse, as there were of course (state-organized) attempts to produce biological weapons that possess the ability of mass causalities and there is the possibility that there will be similar attempts in the future. Despite that, the few cases of an intentional release of biological agents in the past show that one can rarely observe actual mass casualties. Within the discourse concerning the Biological Weapons Convention, one can however identify the concern, that biological weapons, even with lower destructive potential, can still have a lasting effect in the form of so-called "mass disruptions".

Often the term disruption seems to focus a disruption of critical infrastructures. However, there seem to exist additionally layers to the concept, which can be seen in mentions of the special appeal of biological weapons for terroristic purposes and effects, which are talked about in terms of "social disruptions". This aspect of a disruption phenomenon addresses effects on a level of interactions and (socio-) psychological impacts, which go beyond the impact on critical infrastructures.

We want to outline ideas on the question of how to divide and organize types of disruption and which affected areas are presumed. We want to open the discussion on how "mass disruption" may not be assessable as a quantitative threshold for defining an effect as such, but a qualitative describable phenomenon which contains imaginations and concerns about vulnerabilities and the importance of areas of societies.

TRACK IV: NEW TECHNOLOGIES AND ARMS CONTROL

TRACK CHAIR:

JÜRGEN ALTMANN

EXPERIMENTAL PHYSICS III, TU DORTMUND UNIVERSITY

INTRODUCTION

Since research and development of new military technology were done systematically they have brought about new weapons systems that often have endangered global peace and military stability. Arms control has limited some of the most urgent problems, in particular with nuclear weapons, but could not change the general course of the qualitative arms race. Today arms-control treaties – not only for nuclear weapons – are in danger. Space weapons, limitation of which has been on the table for more than 30 years, are re-appearing. Hypervelocity missiles threaten to undermine limits on ballistic and cruise missiles. Armed drones, attacking under remote control, are being deployed by dozens of countries. Autonomous weapons, where the computer would select and attack targets without human intervention, are on the horizon. Cyber forces prepare not only defence, but also offence, with effects in the physical world, and co-ordinated with military action therein. Markedly shortened decision times threaten to increase crisis instability, raising the spectre of accidental war. Ever smaller weapons and production in small, inconspicuous installations render verification of bans and limits increasingly difficult.

To discuss dangers from new military technologies and possibilities of preventive arms control in various areas, as well as overarching policy issues, SCIENCE · PEACE · SECURITY invited contributions from the respective fields of natural as well as social science.

New Military Technologies and International Security/ Peace

JÜRGEN ALTMANN

EXPERIMENTAL PHYSICS III, TU DORTMUND UNIVERSITY

[#32-EXT.-ABSTRACT]

EXTENDED ABSTRACT

Advances in science and technology, translated into new kinds of weapons, have always influenced the issue of war and peace, but have gotten immensely higher importance after 1945. Many new technologies, used for military purposes, have increased threats, accelerated the pace of warfare and in consequence reduced decision times, endangering international security and peace. One example from the Cold War is the addition, in the 1960s, of ballistic missiles to bombers as strategic nuclear-weapon carriers which reduced the flight times from many hours to 10-35 minutes, with correspondingly shortened early-warning and reaction times. Another is the introduction of multiple independently targetable reentry vehicles (MIRVs) on missiles in the 1970s which raised the specter of a disarming first strike. Even though concerned scientists had warned against such developments, these qualitative advances could not be prevented, but at least quantitative arms control could be agreed upon (Goldblat, 2002). Success in qualitative arms control was possible in the field of ballistic-missile defence: after considerable efforts by scientists (in the Pugwash Conferences) to convince political leaders (Evangelista, 1999), anti-ballistic missile systems were severely limited by the ABM Treaty (1972), removing motives for compensating offensive build-ups. Depending on political developments nationally as well as globally, military uses of specific technologies could be stopped and weapons destroyed, as with the Biological Weapons Convention (1972) and the Chemical Weapons Convention (1993). In order to be comprehensive and preclude undermining by technological advance, several arms-control treaties contain preventive elements, prohibiting not only use and deployment of certain kinds of weapons, but also the earlier stages of testing and development – additional cases are the nuclear test bans of 1963 and 1996.

However, in most cases military-technological advances went unimpeded. This holds less for qualitatively new kinds of weapons, more for improvements of existing weapons and all sorts of components and systems for their higher effectiveness, including reconnaissance, tactics, strategies and logistics. In the 1980s microelectronics and information and communication technologies (ICTs) allowed markedly higher targeting precision. In the 1990s the notion of the Revolution in Military Affairs and net-centric warfare came to the forefront. The remote-control armed uninhabited vehicles that have been on the rise since the 2000s can be counted as a new kind of weapon.

Fundamental change in weapon systems can be expected from several present trends, with technologies that can be called revolutionary and that act synergistically. A general theme is nanotechnology that comprises many different fields (Altmann, 2006, 2017). Concrete issues include: Autonomous weapon systems where selection and attack of targets would be done by computer without human control, enabled by advances in sensors, ICTs and artificial intelligence; manipulation in cyberspace; additive manufacturing ("3-D printing"); new possibilities of manipulating life processes, in particular genome editing (this may enable targeted application of biological agents and reduce military reservations against them); body manipulation that could produce brain-machine interfaces and enhanced soldiers. Several of the new technologies will be more generally available, including to non-state actors. In case of software-controlled, general-purpose production technologies, preparing nefarious uses could need no more than a change of the process-description file.

Arms races in such technologies are by and large not yet real, still limited to the planning, research and development stages, but they could expand to deployed military hardware soon, with proliferation to many countries. The military situation would destabilise, endangering international security and peace. Also, there are dangers to arms control and international humanitarian law. Civil society could be affected by new kinds of weapons used by terrorists. Needed is military-technology assessment and then preventive arms control (Altmann, 2006: ch. 5, 2008). Preventive arms control limits or prohibits potential new military uses of technologies before they would be deployed, working at the stages of use, acquisition, testing and/or development. Preventive elements are contained in more treaties than the ones mentioned above; the ban of laser blinding weapons is an interesting special case (Protocol, 1995).

Preventive limits of revolutionary technologies encounter difficulties. Many technological developments are driven by the civilian sphere (e.g. "autonomous" cars), several technologies will come with dual-use potential. With civilian interests in the civilian application of such technologies, limiting them will meet resistance. However, in many cases the military requirements go beyond what is being developed for civilian markets, so that specific military development is still needed, military systems will differ from civilian ones and could be limited without marked consequences for civilian products. More problematic is the desire for improved combat strength that moves modern armed forces toward fast introduction of new technologies. In particular, the quest for maintaining or achieving military-technological superiority acts as a driver. Necessary is the insight that national security can only be ensured sustainably by organising international security. With this insight and ensuing political will preventive limitations of the most dangerous military uses should be possible for the near- and mid-term future. In most areas verification of compliance seems possible using established co-operative methods such as data exchange, on-site inspections, sensor systems and overflights, or improved forms thereof.

But the smaller, cheaper, more numerous and more widely available technologies or dangerous systems will become, the more intrusive the verification of compliance with limitations will need to get. In the long run anytime, anywhere inspections in military as well as civilian places could become necessary in theory which would be hard to accept in practice not only by armed forces, but also by private industry and ordinary citizens. Will arms control encounter its limits in such a case? Will prevention of arms races and extreme destabilisation require organising international security in a different manner, by an international system where states for their security no longer rely on the threat of their armed forces, but on an international legal system with a (limited) monopoly of legitimate violence against lawbreakers?

Before such questions will become relevant, one has to look at the present international situation that is characterised by uncertainty and increasing dangers. US-Russian arms control is deteriorating – the ABM Treaty was abrogated in 2001/2002, Russia has stopped participating in the CFE Treaty in 2015, the INF Treaty has ended in 2019, and whether the New START will be prolonged in 2021 is unclear. China's military spending is rising; it is still considerably below the US budget, but China – not participating in nuclear arms control – is increasingly seen as a competent potential adversary by the USA. Intermingled with this triangle of military threats and counter-threats is another triangle consisting of China, India and Pakistan where no agreed arms limitations exist.

It seems that bilateral limitations are no longer a feasible solution. In principle, the global situation could be defused by comprehensive arms control among the USA, Russia and China. However, the outlook for this is dim at present. Each of the three countries puts much emphasis on new military technologies. Their introduction would increase mutual threats and destabilise the situation. As in the Cold War, it is the task of concerned scientists and engineers to inform decision makers and the public about such dangers and to help to reverse the present trend.

REFERENCES

Altmann, Jürgen. (2006). Military Nanotechnology: Potential Applications and Preventive Arms Control. Abingdon/New York: Routledge.

Altmann, Jürgen. (2008). Präventive Rüstungskontrolle, Die Friedens-Warte, 83, 2-3, 105-126.

Altmann, Jürgen. (2017). Preventing Hostile and Malevolent Use of Nanotechnology – Military Nanotechnology After 15 Years of the US National Nanotechnology Initiative. In M. Martellini, A. Malizia (eds.). Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges: Threats and Counter Efforts. Cham: Springer International.

Altmann, Jürgen & Sauer, Frank. (2017). Autonomous Weapon Systems and Strategic Stability. Survival 59 (5), 117-142.

Evangelista, Matthew. (1999). Unarmed Forces – The Transnational Movement to End the Cold War. Ithac NY/London: Cornell University Press. Ch. 6.

Goldblat, Jozef. (2002). Arms Control – The New Guide to Negotiations and Agreements. London etc.: PRIO/SIPRI/Sage.

Protocol on Blinding Laser Weapons (Protocol IV to the 1980 Convention). (13 October 1995). Retrieved from https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=70D9427BB965B7CEC12563FB0061CFB2&action=openDocument&SessionID=C097633C1DD50D4150B74453E6BD62A210202C6D.

Cooperative Transparency – Modernization of Open Skies Sensors in Tense Times

HARTWIG SPITZER

INSTITUTE OF EXPERIMENTAL PHYSICS, UNIVERSITY OF HAMBURG

[#33-LONG-PAPER]

ABSTRACT

Imagine you fly over the territory of a potentially unfriendly neighboring state, you take photographs of it, and no one shoots you down. In fact, the state actually provides you with the infrastructure to carry out your flight. This is regular practice during Open Skies flights. The 34 state parties of the Treaty on Open Skies have opened their full territory from 'Vancouver to Vladivostok' to cooperative observation flights. The Treaty supports mutual transparency of major military assets which are visible in the open. Both the observing and the observed party get copies of the images taken, a basis of avoiding misperceptions. The images have a high degree of undisputed authenticity. The Open Skies Treaty continues to function fairly well in spite of tense East West relations.

Originally film cameras at 30 cm resolution were used. The transition to digital cameras has triggered an ongoing modernization process. Russia and Germany have acquired new dedicated Open Skies aircraft. The United States has established a budget for the acquisition of two new long-range aircraft. This paper will focus on treaty implementation, new aircraft and different configurations of digital aerial cameras acquired by the Russian Federation, the US, Germany and Romania.

1. INTRODUCTION[1]

The Treaty on Open Skies has been, from its beginning, a multi-facetted, although little noticed, microcosm and mirror of changing East-West security relations and regional status conflicts in Europe. In particular, after entry into force in January 2002 the tensions between the Russian Federation on the one hand and Western states on the other were accentuated by a step-by-step deterioration of the East-West arms control architecture: Withdrawal of the United States of America (US) from the Anti-Ballistic Missile Treaty in 2002, failure of NATO states to ratify the Adapted Treaty on Conventional Forces in Europe of 1999 (ACFE), suspension of implementation of the Treaty on Conventional Forces in Europe (CFE) by the Russian Federation in December 2007, the failure of attempts to modernize the Vienna Documents on confidence and security building measures after 2011, and the withdrawal of the US from the INF Treaty and the Russian confirmation of the end of the treaty in 2019. In parallel, various military and political interventions have fuelled mistrust and alienation between the Russian Federation and Western States: The interventions led by the US and France, respectively, in Iraq (2003) and Libya (2011), the recognition of Kosovo by several western states in 2008 and the annexation of Crimea by the Russian Federation in March 2014 as well as the subsequent war in Eastern Ukraine between Ukrainian and separatist forces, the latter ones supported by the Russian Federation. The eastward expansion of NATO since 1999 and the ongoing cooperation of NATO with Georgia and Ukraine have raised concerns in Moscow.

In parallel, an ongoing dispute between Greece and Turkey about an accession application by Cyprus to the treaty paralyzed the Open Skies Consultative Commission – the body which takes decisions on treaty implementation – from January 2011 to July 2012 (Spitzer, 2011). Most recently, a veto from Georgia to accept Russian overflights prevented the flight activity of all states in 2018 (Spitzer, 2018). Nevertheless, flights have resumed as normal this year.

Surprisingly, Open Skies implementation survived such challenges and setbacks so far for several reasons:

- The major players, the Russian Federation and the US, as well as other parties continue to see the treaty as being in their national security interest. They value the degree of transparency it creates.
- The built-in structure of cooperative implementation and reciprocity in data access makes it attractive to all parties.
- The treaty architecture contains several elements of flexibility: Parties can choose flight paths according to changing security concerns. The treaty provides a procedural framework for certified modernisation of aircraft and sensors.

[1] The author has followed the development of Open Skies from the very beginning. He initiated and led a research project on contributions of multispectral imaging in support of arms control monitoring. Based on this work he was invited to support the German Foreign Ministry in preparing the first Open Skies Review Conference in 2005. Subsequently he has participated as an observer in the work of the Informal Group on Sensors (IWGS) of the Open Skies Consultative Commission (OSCC).

This paper will report on recent steps in modernizing aircraft and imaging sensors. It will evaluate the contribution of Open Skies cooperative aerial observation to arms control verification and transparency. To begin with, the treaty substance, impediments to full treaty implementation and compliance conflicts are discussed.

Open Skies works mostly in the quiet. It is rarely noticed by the media with the recent exception of some Russian news services and US defence and security journals, and very occasional features in mainstream newspapers. As far as known to the author only a few scientific papers have been published on Open Skies sensors after entry in to force, see e.g. (Dunay et al., 2004), (Petrie, 2007), (Spitzer, 2009), (Orych, 2015). A comprehensive overview of publications on Open Skies from 1989 to 2004 can be found in (Dunay et al., 2004)

2. DEVELOPMENT AND SUBSTANCE OF THE TREATY

2.1. THE FIRST THREE YEARS UNTIL SIGNATURE

The first three years from the initial proposal of the treaty in May 1989 to its signature in March 1992 saw dramatic changes in the political orientation of states in Europe, which had belonged to the Soviet-led Warsaw Treaty Organization. Likewise, there were major shifts in the Euro-Atlantic security relations.

US President H. Bush had initially proposed an Open Skies agreement to the Soviet leadership in order to test General Secretary Gorbachev on his policy claim of Glasnost (openness) and in order to regain initiative in the arms control arena. In contrast to the bilateral Open Skies proposal of President Eisenhower of 1955, the anticipated agreement was intended to include allied states of both sides[2]. The proposal was quickly picked up by member states of NATO, but also by Hungary[3]. A NATO communiqué of December 1989 contained essential elements of the architecture of the treaty that would emerge from its negotiations (NATO, 1989):

- Full territorial access for cooperative observation flights with fixed wing unarmed aircraft,
- Annual flight quota which are to be derived from the size of participating countries,
- Establishment of a multi-lateral treaty among the parties.

It took two major conferences in Ottawa (February 1990) and Budapest (May 1990) as well as an intense negotiation period from September 1991 to March 1992 in Vienna until parties could agree on the treaty. Key elements are:

[2] For details of Eisenhower´s proposal see e.g. Dunay et al., 2004, pp.17-20 and references quoted therein.

[3] Hungary and Canada performed a first Open Skies demonstration flight as early as in January 1990.

- Limits of the ground resolution of certified imaging sensors (30 cm for film cameras and video sensors, 50 cm for thermal infrared cameras and 300 cm for synthetic aperture radar),
- Availability of image copies to both the observing and the observed states[4],
- Entitlement of active quota for flights in other countries, combined with the obligation to accept the same number of flights over one´s own territory (passive quota).
- Treaty issues are discussed and decided in the Open Skies Consultative Commission (OSCC) which meets monthly in Vienna and in Review Conferences every five years.

The Russian Federation with Belarus and the US have annual active and passive quota of 42 flights, each[5]. Canada, France, Germany, Italy, the United Kingdom, Ukraine and Turkey have quota of 12 flights each, other countries have less[6]. A detailed account of the negotiation phase and its outcome can be found in (Dunay et al., 2004), (Hartmann, Heydrich, 2000) and (Jones, 2014).

The Treaty was signed by 26 states in March 1992. In the meantime, the German Democratic Republic had acceded the Federal Republic of Germany and the Soviet Union had been dissolved. Four successor states of the Soviet Union joined the treaty: Belarus, Georgia, the Russian Federation and Ukraine[7].

In the arms control arena the successful conclusion and implementation of the CFE Treaty of November 1990 eliminated the force dispositions for massive conventional surprise attacks in Europe. The treaty was originally meant to include an aerial verification system. This was dropped because of lack of negotiation time. In a way the role of aerial monitoring was taken over by Open Skies.

However, Open Skies has a much wider territorial scope. Whereas on-site inspections under CFE are restricted to Europe from the Atlantic to the Urals, Open Skies flights can also cover the vast territories of North America (US and Canada) as well as the Russian Federation east of the Urals[8]. Thus, the treaty has a transcontinental dimension and a role in the US-Russian nuclear relationship. Both the US and Russia can use flights to monitor nuclear weapon and missile defence sites in complementation of their satellite reconnaissance assets.

2.2. TRIAL IMPLEMENTATION AND ENTRY INTO FORCE

Entry into force was much delayed by lack of consensus on the treaty in the Russian Federation. The obstacles came from several quarters. Strong opposition to ratification existed in the

[4] Other parties can acquire copies at nominal cost.

[5] The Russian Federation and Belarus have formed a group of parties with joint quota.

[6] See Dunay et al. 2004, page 45 for a table of flight quota.

[7] Kyrgyzstan signed the treaty in 1998 but never ratified it.

[8] On-site inspections under the Vienna Document on Confidence and Security Building Measures cover Europe from the Atlantic to the Urals including the three Caucasus states (Armenia, Azerbaijan and Georgia) plus the territories of the five Central Asian Republics. The latter ones are not parties of the Open Skies Treaty.

Russian military which feared espionage. More importantly, there was an institutional dead lock between the Russian parliament and President Boris Yeltsin. The treaty was eventually ratified in April 2001, well after Yeltsin had resigned. The treaty was now seen as advantageous to Russia in obtaining information with minimal expenditures (see Dunay et al., 2004, 62).

The ten-year phase before entry into force was well used. Parties were eager to train their personnel and to test inspection procedures. Over 400 bilateral trial flights were performed upon mutual agreement. Some of the test flights yielded relevant information about Russian military equipment which had been relocated east of the Urals. Germany hosted two trial certifications of five foreign aircraft each in 2000 and 2001. This created the basis of practical experience for the successful certification of aircraft and sensors of ten countries after entry into force of the treaty (1 January 2002)[9]. In addition, C130 aircraft with a joint sensor pod of a group of ten further countries (the so-called Pod Group) were successfully certified. For an account of the trial implementation phase and the mission practice after entry into force, see (Dunay et al., 2004).

2.3. ACCESSION OF OTHER PARTIES AND FLIGHT ACTIVITY

Eight countries acceded the treaty after entry into force. These included the three Baltic States, Bosnia-Hercegovina, Croatia, Finland, Slovenia and Sweden. Today the treaty comprises 34 states including all NATO member states apart from Albania and Montenegro and a few non-aligned states (namely Bosnia-Hercegovina, Finland, Georgia, Sweden and Ukraine)[10].

Although each country is entitled to fly over any other country within the limits of the quota system, the actual flight activity has developed in a less balanced way. NATO member states have agreed not to overfly each other. NATO states are concentrating their flights on the Russian Federation and Belarus, exploiting most of the passive quota of those countries (42). In return, Russia performs 42 flights annually over NATO states including seven flights over the United States (in 2017). A smaller number of flights were performed in 2017 by non-aligned states: Ukraine (12), Sweden (6), Finland (2). Over the years the total number of active flight missions has been about one hundred annually. Several flights are performed as shared missions of two or three parties in order to reduce the cost per country[11].

Overall the flight activity reflects the politico-military tensions and security concerns between NATO states and the Russian Federation. It addresses such concerns by creating transparency within limits.

[9] The certified camera configurations are designed for operation at different flight altitudes. Some countries operate camera configurations which allow observation below relatively low lying clouds: Canada and France (1210 m), Germany (1550 m, in preparation), Russian Federation (1130 m), Sweden (1830 m), Turkey (1790 m), USA (2150 m).

[10] The Czech Republic and Slovakia became parties after the dissolution of Czechoslovakia on 1 January 1993 as successor states.

[11] A full account of flight activity in 2008 can be found in (Spitzer, 2009).

3. DISPUTES HAMPERING FULL TREATY IMPLEMENTATION

The treaty opens the full territory of parties to observation flights with the exception of a 10 km zone along the border of non-parties. Since entry into force several impediments to full territorial accessibility have come up, two of them as a consequence of unsolved status conflicts. The impediments occurred in the following time sequence[12].

3.1. 2002-2016: NO ACCESS TO SOME US ISLANDS

The Treaty covers both the continental United States as well as US island territories. Access to the Hawaiian Islands was opened in 2007. The Russian Federation has repeatedly asked for flight access also to several smaller islands in the Pacific and the Atlantic[13]. Only in 2016, the US submitted the necessary declarations for the remaining islands including Guam in the Pacific, which hosts a major military base. The first Russian flight over Puerto Rico and the US Virgin Islands was performed from 28 May to 3 June 2019 (OSCC, 2019). The impediment can be considered as resolved.

3.2. SINCE 2010: NO FLIGHTS IN THE RUSSIAN 10 KM BORDER ZONE OF ABKHAZIA AND SOUTH OSSETIA

In consequence of the August 2008 war between Georgian, Russian and separatist forces, the Russian Federation had recognized the entities of Abkhazia and South Ossetia as independent states[14]. Georgia and all other Open Skies parties apart from Russia consider Abkhazia and South Ossetia still as part of Georgia’s national territory – in spite of the de facto separation. Since May 2010 the Russian Federation has rejected flight plans of other parties which would have entered the 10 km zone along the border of Abkhazia. This rejection has been heavily criticized in the Open Skies Consultative Commission and by national capitals[15]. It is a classical dilemma of an unsolved status conflict. The practical effect on overhead image acquisition capability is small, because panorama cameras when flown high enough can view distances well over 10 km[16].

[12] In addition there have been disputes over flight altitude restrictions which mandated high flight levels, e.g. over the Moscow area, over Chechnya, in Norway and Canada. Some of the cases are caused by different national standards and procedures for air traffic control.

[13] See e.g. OSCC (2015) for details.

[14] The entities of Abkhazia and South Ossetia had broken away from Georgia in two bloody secession wars (1991-94). The conflict had a complicated history concerning ethnic composition of the population and political affiliation. Both entities had an autonomous status in the USSR. For details see e.g. (Richter, 2019, pp.16-17) and sources quoted in (Spitzer, 2018). Today Abkhazia and South Ossetia are recognized by five UN member states only: Venezuela, Nicaragua, Nauru, the Russian Federation and Syria.

[15] E.g. the United States have determined in the 2018 Arms Control Report that Russia was in violation of the treaty by ”refusing access of observation in a ten kilometer corridor along its border with the Georgian regions of South Ossetia and Abkhazia”. (State, 2018)

[16] It should be also noted that parties refrained from extending their flights over Georgia to the breakaway territories. The government of Georgia would not have been in a position to guarantee the safety of such flights.

3.3. SINCE APRIL 2012: GEORGIA REFUSES TO ACCEPT OVERFLIGHTS BY RUSSIA

On 4 April 2012, the head of the delegation of Georgia to the OSCC submitted a letter declaring that Georgia will no longer allow any observation flight that includes participation of the Russian Federation over the territory of Georgia (OSCC, 2012). The letter referred to the rejection of an US-Romanian flight plan of May 2010 which would have entered the 10 km zone along the Russian border of Abkhazia. Georgia sees this rejection as a violation of the Open Skies Treaty and of international law.

3.4. SINCE MARCH 2014: NO FLIGHTS OVER CRIMEA

The annexation of Crimea by the Russian Federation in March 2014 is seen by other parties as a violation of international law. In May 2014, the Russian Federation invited other parties to overfly Crimea as part of missions over Russia. Other parties have refrained from doing so because it would imply recognition of the annexation. Thus, the major Russian naval base in Sevastopol is no longer observed by Open Skies flights. Again, a regional status conflict is preventing full treaty implementation.

3.5. SINCE JUNE 2014: FLIGHT LENGTH RESTRICTIONS OVER THE OBLAST OF KALININGRAD

On 10 June 2014, the Russian Federation notified all parties on a flight length restriction of 500 km over the oblast of Kaliningrad. (Open Skies, 2014) The oblast comprises an area of 15.125 square kilometres with a maximum East-West extension of about 170 km and a maximum North-South extension of about 100 km[17]. In detail, Russia designated the airport of Krabrovo in the Kaliningrad oblast as an airfield that can be used for Open Skies flights with a maximum distance of 500 km. In addition, flights out of the Open Skies point of entry in Kubinka near Moscow have to observe a component part of maximum 500 km when flying over the oblast. Previously flights out of Kubinka had included longer observation distances over the oblast. Several parties protested in the Open Skies Consultative Commission[18]. They emphasized that the agreed maximum flight distance for flights out of Kubinka is 5500 km. According to the treaty each state party shall ensure effective observation of its entire territory. Maximum flight distances from Open Skies airfields have to be set and notified correspondingly.

The matter was disputed heavily since 2014 without reaching consensus. Observing parties have respected the limit in flight missions over Russia under protest. Russia has claimed, last time in the OSCC session of 20 May 2019, *"…that the maximum flight distance of 500 km*

[17] The oblast is a Russian exclave on the Baltic Sea surrounded by Poland and Lithuania. The formerly German territory was integrated in April 1946 into the Russian Soviet Federative Socialist Republic (SFSR), the predecessor of the present Russian Federation.

[18] The United States have determined in the 2018 Arms Control Report that Russia was in violation of the treaty by "imposing and enforcing a sublimit of 500 kilometers over the Kaliningrad Oblast for all flights originating out of Kubinka Open Skies Airfield". (State, 2018)

enables an effective observation of the entire territory of the Kaliningrad region, obtaining images of up to 98 per cent of its territory from a single observation flight with the possibility of observing any of its points"[19].

In June 2017 the US administration formally accused Russia of violating the treaty by limiting the flight length over the oblast. In retaliation the US imposed limits on Russian flights over the Hawaiian Islands and closed some airfields for Russian overnight stops, still leaving the full US territory accessible to Russian observation. Russia responded by closing three Open Skies airfields for US flights[20].

The oblast is at the center of security concerns both of Russia and of NATO states, in particular the Baltic States and Poland. It hosts important military bases, a port of the Russian Baltic fleet as well as early warning radar stations and short range nuclear capable missiles. Of particular concern are the Iskander manoeuvrable missiles[21]. The system has been modified for launching also cruise missiles. According to (FAZ, 2019) Russia has expanded and modernized the storage capacities for nuclear weapons in the Kaliningrad region. Both the manoeuvrable rocket and the cruise missile version of the Iskander have a significant military capability due to their targeting accuracy and their manoeuvrability which makes detection and hits by missile defence harder.

4. Modernization of aircraft and sensors

4.1. New Open Skies aircraft

The above described impediments to full treaty implementation are real, but they are only part of the story. The core of the story is the fact that the major players, the US administration and the Russian leadership, as well as the governments of other parties are holding on to the Treaty for the time being in spite of compliance disputes. Major investments in modernization of Open Skies hardware have been made.

Russia was first, already in 2006, to provide a budget for two new long-range Open Skies aircraft of type Tu 214. The first of those aircraft was displayed in August 2011 at an air show

[19] In the view of the author a full observation of the area in one 500 km flight is only possible under rare conditions: Operating a panorama camera from 10 km altitude under a nearly cloud free sky. However, it should be possible to photograph most military sites of known location in one flight of 500 km under favourable cloud conditions.

[20] The restrictions were communicated by the US administration as an incentive for the Russian Federation to return to full treaty compliance. For details of the US measures see (State, 2018).

[21] In reaction to the deployment of US missile defence units in Poland, Russia deployed Iskander missiles in the oblast. The Iskander missile family is reported as comprising road-mobile manoeuvrable missiles with accurate strike potential down to a circular error probable of 5-7 meters. The Iskander can be tipped with several conventional warheads including a cluster munition warhead, a fuel-air explosive enhanced blast warhead, an earth penetrator for bunker busting and an electro-magnetic pulse device as well as with nuclear warheads (from Wikipedia.com, which quotes numerous sources, access 8 August 2019).

in Moscow (see figure 1). Open Skies has the attention of the top Russian leadership; President Putin took a tour of the aircraft. Both aircraft and the digital image sensors on board of type OSDCAM 4060 were certified for use in Open Skies (through the agreed inspection processes for equipment to be used under the treaty) in Kubinka in September 2018[22]. The cost of the modernization program was reported as 220 million USD at the 2010 Review Conference of the Treaty (Open Skies Review Conference, 2010).

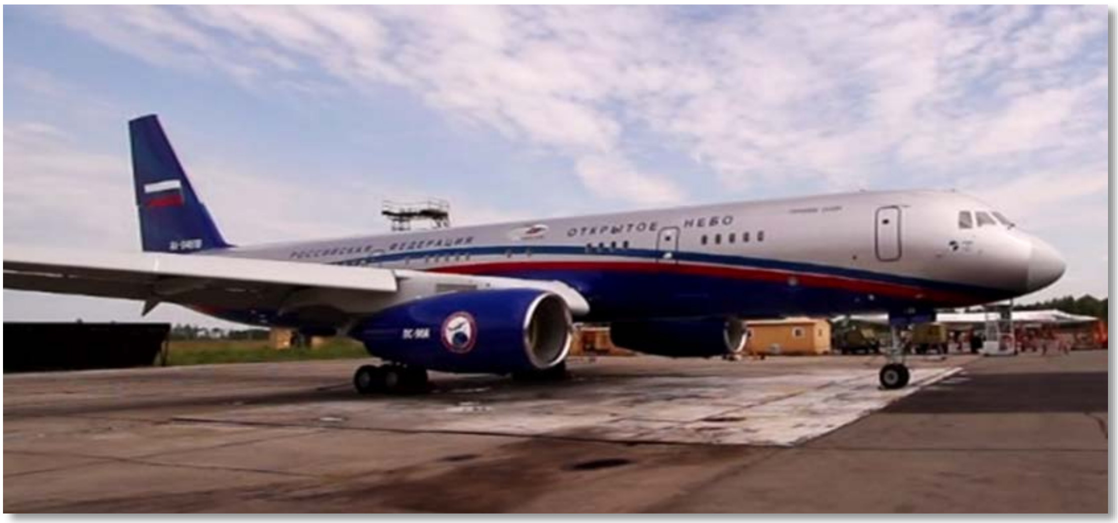


Figure 1: A Russian Open Skies aircraft of type Tu 214 ON on display at the Moscow Air Show, August 2011 (courtesy: US Air Force)

Germany had modified a Russian made Tu 154 jet liner for Open Skies use in the years 1993-1995. The aircraft performed successful trial missions, but was lost in a mid-air collision over the Southern Atlantic in September 1997. It took eighteen years and a lot of lobbying before the German Parliament approved a budget for a new Open Skies aircraft in November 2015[23].

It was decided to acquire a little-flown corporate airliner of type Airbus A319 CJ. The aircraft model A319 CJ has four extra fuel tanks in the freight compartment to allow for long distance direct transit flights of over 6000 km. Thus, Germany will be in a position to perform observation flights far beyond the Urals. The aircraft was adapted for its future role by Lufthansa Technik

[22] The certification procedure was performed 2-11 September 2018. All attending parties apart from the US signed the certification document on 11 September. The US signature was submitted on 26 September in a session of the OSCC without giving reasons for the delay.

[23] The decisive initiative came from several parliamentarians who questioned the government on providing a German Open Skies capability in 2012. One of the parliamentarians, a retired colonel of the Bundeswehr, succeeded in placing the objective in the coalition agreement of the Christian Democratic and Social Democratic Parties in November 2013. The deterioration of conventional arms control and the events of 2014 in Ukraine helped to enhance awareness and acceptance. For more details see (Müller, 2016).

in Hamburg and by several subcontractors. It was handed over to the *Bundeswehr* on 21 June 2019. Figure 2 shows the aircraft at the Lufthansa base in Hamburg.

The aircraft will be available for up to 12 active German missions annually as well as for leasing by partner nations[24]. The target date for certification is fall 2020. Before this happens, extensive test flights have to be performed, in order to establish the flight altitude corridors in which the digital sensors yield the treaty mandated resolution. The cost of acquisition and retrofitting of the aircraft was around 120 million Euro, including cost for training flight crews.

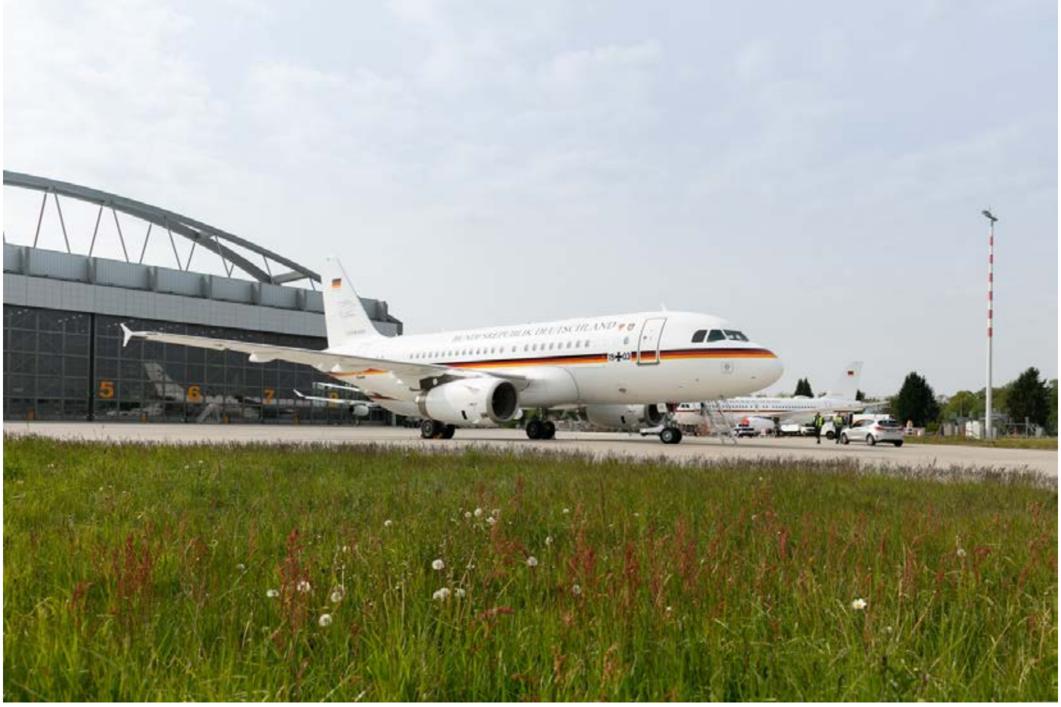


Figure 2: The new German Open Skies aircraft of type A 319 CJ (source: Lufthansa Technik)

The two existing Open Skies aircraft of the *United States* (modified Boeing 707 models) were built in the 1960's. Several recent missions had to be terminated early due to technical failures. The former Secretary of Defense, Mattis, decided to aim for parity of US Open Skies assets with Russia. In consequence a budget of 222 million USD was requested from US Congress and approved in the National Defense Authorization Act (NDAA) for Fiscal Year 2019. The bidding process for two long-range aircraft is under way.

Several parties use existing aircraft: Canada, France, Hungary, Romania, Sweden, Turkey and Ukraine as well as Russia (five medium range An-30 and one Tu 154). The aircraft of the Czech Republic and the UK have been put out of service. The Pod group was dissolved end of 2013. The sensor pod with film cameras is only flown on C130 aircraft of Canada and France. Bulgaria stopped flying their An-30 aircraft for Open Skies missions in 2019. Most other countries

[24] The aircraft has four working stations for sensor operators, 16 seats for inspectors of the observed party and for mission personnel of partner nations, as well as 25 extra seats.

exploit their active flight quota by renting Open Skies aircraft from Hungary, Romania, Sweden and Ukraine or are sharing missions.

4.2. OPEN SKIES SENSORS: TRANSITION TO THE DIGITAL AGE

Under the rules of the treaty, Open Skies sensors have to be commercially available to all parties. When the treaty was negotiated between 1990 and 1992 the commercial market of aerial cameras was dominated by film cameras, mostly with panchromatic (black and white) film. The treaty allows for framing cameras and (wide angle) panchromatic cameras with resolution no better than 30 cm[25].

The transition to commercial digital aerial cameras was initiated by the presentation of a large format mapping camera by the company Z/I Imaging (Oberkochen, Germany) in 2000. Today three digital camera formats are being used commercially: small format or consumer cameras with about 1-30 Megapixel (MP), medium format cameras weighing a few kgs with about 40-150 MP and large format cameras with up to 450 MP.

The Open Skies Treaty authorizes the OSCC to decide on technological updates of existing sensor categories without having to go through a formal amendment (re-ratification process). How to store and transmit information digitally has been addressed in Open Skies already in 1994, primarily in connection with the readout of video sensors, which are a treaty sensor category (with resolution no better than 30 cm). Intensive work to introduce digital aerial cameras started in 2006 in the Informal Group of Sensors of the OSCC.

It took many tests and demonstrations of certification procedures until the OSCC could decide on the introduction of digital cameras in the treaty category of video sensors. Availability on the commercial market was checked in 2008. Cameras with four spectral channels for blue (B), green (G), red (R) and near-infrared light (NIR, with wavelength between 0,69 and 1,1 micrometres) can be used, also a panchromatic channel. Today, certification of sensors is based on a sequence of five steps: (i) lengthy flight tests of the certifying party in order to establish the flight altitudes at treaty resolution for the various camera configurations; (ii) submission of extensive documentation on sensors and processing software, as well as on the outcome of test flights, (iii) demonstration of certification procedures to state parties (the precertification event), (iv) intermediate meeting in order to resolve remaining questions, (v) the actual certification event which demonstrates and confirms the flight altitudes for treaty mandated resolution.

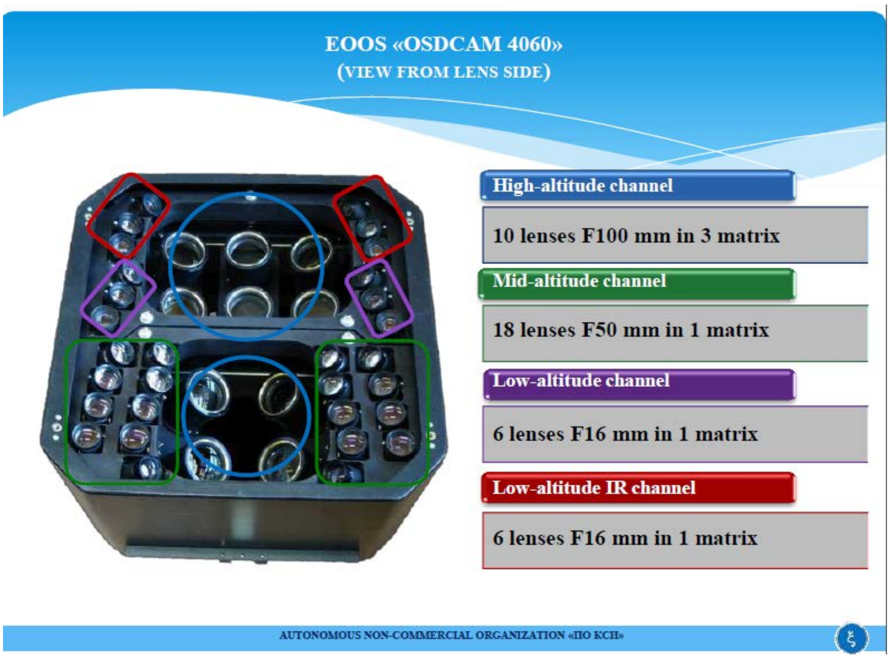
Further work was needed in order to agree on a verified data processing chain. This comprises (a) processing of raw image data to composite images in an agreed Open Skies image data format, (b) duplication of image data, (c) duplication verification, (e) erasure of raw data after processing, and (f) erasure verification.

[25] The resolution is determined on bar targets of black and white bars. The resolution definition which was adopted by the OSCC implies that 30 cm resolution of a film camera under Open Skies corresponds roughly to the ground resolution which is usually quoted for digital cameras: i.e. the size of a ground area which is imaged by a picture element (pixel) of a digital camera. For details see (Dunay et al., 2004, 43 and 74).

How is cheating prevented? Inspectors of the observed state are on-board during data taking. They check that the certified flight altitude for 30 cm resolution is observed. At the end of a mission the digital storage devices are sealed for transport into the media processing station. Image processing, duplication and erasure of raw data is performed in a controlled way in presence of inspectors and experts of both sides. Checks of data and erasure fidelity are being made. The software has to be documented for all parties.

As a result, the image duplicates which are handed over to the observing and the observed party have a very high degree of authenticity[26]. For details see (Orych, 2015). Thus, Open Skies images can be used in bilateral disputes as a source.

4.3. A SYSTEM WITH FORTY LENSES: THE RUSSIAN OSDCAM 4060



EOOS «OSDCAM 4060»
(VIEW FROM LENS SIDE)

High-altitude channel

10 lenses F100 mm in 3 matrix

Mid-altitude channel

18 lenses F50 mm in 1 matrix

Low-altitude channel

6 lenses F16 mm in 1 matrix

Low-altitude IR channel

6 lenses F16 mm in 1 matrix

AUTONOMOUS NON-COMMERCIAL ORGANIZATION «ПО КСИ»

Figure 3: The Russian Open Skies camera system OSDCAM 4060 (source: www.poksi.ru/OSDCAM_44060-Eng.pdf, access 12. August 2019)

Russia was the first party to present a digital camera system for certification in 2013. The system had been developed by a small Russian company KSI in Moscow using sensor chips and lenses available on the commercial market of consumer cameras. The system consists of forty small cameras which are configured in four subsets which have the same focal length each: Six cameras for data taking at low altitudes (1050-1130 m), 18 for medium altitudes (3230-

[26] Providers of commercial satellite imagery have confirmed that the degree of authenticity of Open Skies imagery is unmatched in the satellite world. Transmission and processing of commercial satellite image data is done only by one party without outside checks and without disclosing their internal proprietary methodologies. (VERTIC, 2017)

3500 m) and ten for high altitudes (6490-6790 m). All cameras operate as RGB cameras[27]. The ground swath covered ranges from 2740-2940 m at low altitudes to (7750-8077 m) at medium altitudes and 11.680-12.430 m at high altitudes[28]. There is also a camera subset which operates in the NIR at altitudes of 1390-1440 m.

Each subset produces a strip image which widens at larger observation angles. The strip images can be composed of a composite image. Figure 3 shows the lens configuration of the system.

The camera system was first flown in an Open Skies mission in July 2014 after an eight-month delay by the US administration in signing the certification document[29].

4.4. THE DIGITAL SENSORS SYSTEM DVIS OF THE UNITED STATES

The US had been a vocal proponent of going digital in the IWGS and at Open Skies Review Conferences since 2005. The slogan of the US chairman of the IWGS was “faster, cheaper, better”. Creating a budget for acquisition of digital sensors turned out to be tedious due to bureaucratic drag and competing priorities for defense acquisitions. A decisive step was taken in March 2012 by the Presidential Policy Directive 15. The directive tasked the Department of Defense to establish a budget for acquisition of digital sensors for the two existing US Open Skies aircraft.

The budget was approved by Congress in steps (2013 and in subsequent years). The request for proposals was released in September 2015. It contained quite challenging ground coverage specifications which were derived from the ground coverage of the existing film cameras (one vertical and two oblique framing cameras and one panoramic camera)[30]. The contract was awarded in February 2016 to the veteran-owned company KIHOMAC (KIHOMAC, 2016) with a volume of 37 million USD.

The designers of KIHOMAC took an approach which has some similarity to the Russian approach: Using arrays of multiple cameras to obtain ground coverage of about 99 degrees from three different altitude levels. They decided to combine medium format cameras of type CM-

[27] Aerial RGB cameras have – similar to consumer cameras – an array of filters which are transparent for red, green or blue light, over the matrix of light sensitive sensor elements.

[28] The camera system is certified for use on three aircraft types: An-30, Tu 154 and Tu 214. The ranges of flight altitudes for 30 cm resolution and the related ground coverage, which are quoted in the text, comprise the performance on all three aircraft types. The certified values for An-30 and Tu 154 aircraft are given in (OSCC, 2017).

[29] This delay was caused by interventions of agencies within the US administration which were suspicions of the information gathering potential of the new camera. In the end the forces won which successfully argued that 30 cm from a digital device is equivalent to 30 cm from an analogue device (film) in Open Skies. However, the RGB capability and the digital accessibility of the images provide an added value which all parties can exploit after going digital.

[30] The ground coverage of the US film cameras vary from ca. 3000 m from a vertical framing camera flown at an altitude of ca. 2000 m to 12.500-23.200 m for a panoramic camera flown at 10.800 m according to (OSCC, 2017).

MK produced in Canada by the US owned company Teledyne Optech with 84 MP (10720 x 8064 pixels at 6 micrometers size each). The camera is employed in three spectral variants: (a) as RGB camera, (b) as pan-chromatic camera and (c) as camera operating in the NIR. The high-altitude configuration consists of five panchromatic and five RGB sensors covering a ground swath of 18,9 km from an altitude corridor of 7600-8500 m. The medium altitude configuration uses five RGB cameras covering a ground swath of 14,3 km from altitudes 5800-6400 m. The low altitude configuration has four individual sensors filtered to Red, Green, Blue and NIR and a ground swath of 3100 m from altitudes 1200-1500 m. Image processing will take several days – longer than the present film development[31].

Delays in tests of the system after delivery have been caused by the complexity of the design. Certification is expected in fall 2020 or spring 2021.

4.5. THE DIGITAL SENSORS ON THE GERMAN OPEN SKIES AIRCRAFT

Germany – similar to the US and Russia – acquired a system of electro-optical sensors which take images in three altitude corridors. In contrast to Russia and the US the German system will have both RGB and NIR cameras at all three altitudes[32]. In addition, Germany is the first party to operate a thermal infrared camera system[33].

The RGB and NIR cameras employ the model PhaseOne iXU-RS 1000 from the Danish company PhaseOne with lenses of different focal length from 23 to 90 mm. The camera has 100 MP (11608 x 8708 pixels of size 4,6 micrometer).

The low altitude configuration comprises one vertically mounted RGB and one NIR camera. It is expected to cover a ground swath of 3500 m across track from an altitude of 1550 m. The medium altitude configuration consists of two slightly tilted (by 5 degrees) RGB and NIR cameras each, providing a resolution of 30-35 cm over a swath of 5660 m from an altitude of 3580 m. The high-altitude configuration comprises three RGB and NIR cameras, each providing a

[31] Development of photographic film from Open Skies flights can be usually done overnight. The data from the multiple cameras for medium and high altitudes of the US system have to be stitched together in order to yield three images each, one for vertical view and two for oblique view. This operation is time consuming.

[32] Near-infrared cameras support the monitoring of the health of vegetation and the discrimination of different types of vegetation (e.g. the discrimination of conifers from deciduous trees). This can be used, for example, to detect and analyse camouflage on vehicles, when such camouflage is made of cut vegetation which is dead or dying. Near infrared imaging has been also used for environmental reconnaissance, for example, by estimating the size of expected crops.

[33] Thermal infrared radiation is emitted by all object's day and night due to their surface temperature. Thermal sensors were included in the treaty sensor set to support data taking at night and during winter in northern regions when illumination by sunlight is short and faint. The resolution limit of 50 cm was seen in 1992 as a compromise between the resolution of optical cameras and the performance of then available commercial infrared sensors at flight altitudes of about 1000 m (Hartmann, Heydrich, 2000, 62). An object can be recognized on a thermal IR image by shape if its temperature is different from the temperature of the surrounding area.

resolution of 30-35 cm over 90% of the full swath (10 090 m) from an altitude of 5870 m (IGI, 2019).

The thermal system consists of two tilted uncooled microbolometer cameras with 1024x768 pixels each of size 17 micrometer[34]. The images of the dual camera will be processed into one continuous image with a resolution of 90-130 cm over a ground swath of 1900 m when operated at an altitude of 1550 m.

The sensors are mounted on gyro-stabilized mounts, one for the sensors of each altitude and one for the thermal sensors. Two of the mounts are placed in a front freight department of the aircraft, two of them in the rear, each pointing at windows of 28 mm thickness which are transparent for visible and NIR light, or thermal radiation, respectively. Thus, Germany will have the most comprehensive imaging capability concerning spectral performance, by providing images from RGB, NIR and thermal radiation[35]. The US system will be superior in ground coverage from medium and high altitudes.

4.6. ROMANIA: A FAST LATE COMER

Romania is operating AN-30 medium range turboprop aircraft equipped with one mapping film camera Wild Aviophot RC-20. In 2018 it was decided to provide a modest budget for acquisition of digital sensors. Romania asked for offers of a compact system of cameras on one gyro-stabilized mount, which can provide images at treaty resolution from three altitudes. Romania placed the order with the small German company GGS (GGS, 2019).

GGS delivered and installed medium format cameras from PhaseOne in spring 2019. The low altitude configuration consists of one RGB and one NIR camera each of type iXM-RS100 (11.608 x 8.708 pixels of 4,6 micrometer size), providing 30 cm resolution over a swath of 3480 m from an altitude of 1500 m. The medium altitude configuration comprises one vertically mounted RGB camera and one NIR camera each of type iXM-RS-150 (14.204x10.652 pixels of size 3,76 micrometer), which provide 30 cm resolution over a ground swath of 4260 m, when flown at 3190 m altitude. Two obliquely oriented RGB cameras cover side strips up to ca. 6000 m on each side at resolution between 30 and 82 cm. The high-altitude configuration comprises one PhaseOne RGB and NIR camera, each, of model iXM-RS150. The ground swath covered is 4620 m from an altitude of 5590 m.

Thus, Romania is expected to operate a robust system, which works at three altitude levels both in RGB and NIR.

[34] Microbolometers are thermoelectric sensors operating a wavelength in the region of 7,5-14 micrometer. Incoming thermal radiation heats a sensor element. The heat signal is subsequently transformed into an electric signal.

[35] The thermal camera system can only be certified once the OSCC has agreed on a revised certification procedure for cameras of present-day technology. A previous decision on certification procedures for line scanner technology is no longer in force.

5. OUTCOME: CONTRIBUTIONS TO TRANSPARENCY AND ARMS CONTROL VERIFICATION

5.1. CREATING TRANSPARENCY

The role and the outcome of Open Skies implementation are manifold, depending on the national interests and concerns of parties. Originally, as stated in the Preamble, it had a rather general scope of intentions and objectives:

> *"…Welcoming the historic events in Europe which have transformed the security situation from Vancouver to Vladivostok, wishing to contribute to the further development and strengthening of peace stability and co-operative security in that area by the creation of an Open Skies regime for aerial observation, recognizing the potential contribution which an aerial observation regime of this type could make to security and stability in other regions as well, noting the possibility of employing such a regime to improve openness and transparency, to facilitate the monitoring of compliance with existing or future arms control agreements and to strengthen the capacity for conflict prevention and crisis management in the framework of the Conference on Security and Co-operation in Europe and in other relevant international institutions…"*

The treaty articles were more specific on the character of the aerial observation: Unlimited territorial access and cooperative execution of flights. The achievable transparency was purposely restricted in a twofold way:

- The verified resolution limit of 30 cm enables the detection of major military land vehicles and infrastructure, but excludes detailed reconnaissance, like recognizing the antenna of a tank.
- The flights contain only a limited surprise element. The time period between disclosure of the flight plan of the observing party and the beginning of the actual observation flight is about 24 hours, leaving enough time to cover sensitive equipment.

In addition, unfavourable weather conditions like very low-lying clouds can prevent observation.

Still, everything in the open remains visible if cloud levels can be under flown. This includes land vehicles, aircraft, ships and submarines in ports, missile sites, as well as all kinds of static military and civilian infrastructure.

How does Open Skies observation compare with satellite monitoring? (a) The resolution of Open Skies images for RGB or NIR light of 30 cm is comparable but not superior to the images of the most advanced commercial satellites Worldview 3 and 4 of Digital Globe, USA. Still, smaller countries prefer the access to Open Skies observation over commercial satellite imagery because of operational flexibility and cost. 30-50 military sites can be photographed in one flight mission at a cost below the acquisition cost of 30-50 satellite images[36]. (b) The resolution of Open Skies thermal infrared images is far better than the resolution which can be obtained from commercial satellites cruising in 700 km orbits. For instance, the LANDSAT satellites offer a resolution of only 60 m in the thermal infrared region (wavelength 7,5-14 micron). (c) A decisive advantage of Open Skies images is, as argued above, their verified provenance and their high degree of authenticity.

5.2. CONTRIBUTIONS TO ARMS CONTROL VERIFICATION

Open Skies contributes to the verification of several arms control treaties:

- Open Skies images have been used to prepare and to complement on-site inspections under the CFE treaty. After the Russian suspension of CFE implementation Open Skies flights can be used to monitor the sites of conventional forces in Russia.
- Open Skies flights have been used to photograph chemical weapon storage and destruction sites.
- Open Skies flights are being used to monitor nuclear weapon and missile sites. A protocol to the New START Treaty includes Open Skies assets as monitoring tools.

5.3. COOPERATION WITH THE OSCE

All Open Skies State parties are participating in the OSCE. The relation of the treaty and its parties to the OSCE can be discussed on four levels: (i) Services provided by the OSCE secretariat, (ii) Shared national and OSCE resources, (ii) Cooperation in conflict prevention as specified in the treaty, (iv) Options for further cooperation.

- *Services provided by the OSCE secretariat.* Beginning with the main negotiation phase of September 1991 to March 1992 the secretariat of the OSCE (then CSCE, Conference on Security and Cooperation in Europe) has provided paid services to the Open Skies state parties. This includes meeting rooms in the Vienna Hofburg, administrative support and website management of an Open Skies delegate’s website. The Open Skies website is handled within the OSCE delweb-website which is accessible to delegates who are nominated by Open Skies states, resp. by participating states of the OSCE.
- *Shared national and OSCE resources*. Politically the Open Skies state parties and the bodies of OSCE operate independently. There exist shared information channels. The ambassadors and military advisors assigned to the OSCE in Vienna represent their country also in the OSCC. They provide consistency of national policies for all three OSCE dimensions and for non-OSCE arms control regimes and security building measures. Open Skies state parties make use of the OSCE Communications network, e.g. notably for Open Skies notifications. Delegates of all 57 OSCE participating states have access

[36] Procuring high resolution satellite images in a short time frame can be particularly expensive. The cost per scene can be up to several thousand USD. Germany is renting the Swedish Open Skies aircraft at a cost of ca. 50 000 Euro per flight (without salaries of the German team). This sum is below the cost of 30-50 high resolution satellite images. (German Verification Center, 2019)

via the delweb to the text of OSCC decisions and to statements made in the OSCC which are documented in written form in the Journal of the OSCC. Access to documentation of Open Skies implementation is limited to representatives of Open Skies state parties.

- *Cooperation in conflict prevention and crisis management.* The preamble of the treaty calls for strengthening the capacity for conflict prevention and crisis management in the framework of the CSCE (now OSCE). A procedural architecture for eventual implementation of this option has been specified in Annex L, Sec III, 1. of the treaty (OSCE, 1992, 95):
- 'The Open Skies Consultative Commission shall consider requests from the bodies of the Conference on Security and Co-operation in Europe authorized to deal with respect to conflict prevention and crisis management and from other relevant international organizations to facilitate the organization and conduct of extraordinary observation flights over the territory of a State Party with its consent.'

  This procedure has never been negotiated and executed. But it is worth being explored.[37]
- *Recommendation:* The author suggests exploring need and feasibility of such flights, both in the OSCC and jointly with the head of the Conflict Prevention Center (CPC) of OSCE. Questions to be explored include:
- What kind of non-treaty missions are states parties willing to support with Open Skies assets?
- Are parties prepared to give the CPC a coordinating role in planning flights and data taking as well as in distribution and analysis of images taken?
- Who bears the cost of such flights and data processing of images? A demonstration flight for testing proposed procedures would be helpful. It should be noted that Open Skies parties have considerable experience in shared missions and joint test flights.
- *Options for further cooperation*. Could Open Skies images or insights from such images be made accessible to bodies of the OSCE, like the CPC? In general, not. Open Skies images are government-official (confidential) among the Open Skies state parties and not accessible beyond. However, parties can use their insights and concerns from analysis of Open Skies images in informal bilateral or multilateral contacts in Vienna.

6. CONCLUSION

The Open Skies Treaty has withstood the test of time in spite of implementation deficits. The value assigned to the treaty in the literature depends a lot on the perspective. The US expert

[37] A representative of Sweden has pointed out at the Open Skies Review Conference of 2010 that the option had been already proposed within the OSCE. The OSCE document "Stabilizing Measures for Localized Crisis Situations" proposes an aerial observation regime aimed at checking compliance with agreed stabilizing measures and building confidence and the possibility of using the procedures and measures of Open Skies. (Open Skies Review Conference, 2010 a).

Michael Krepon emphasized the symbolic relevance of opening the full territory to aerial observation:

"The point of the treaty has always been about symbolism rather than technical data collection". (Krepon, 2018).

An expert brief from the US Council on Foreign Relations argues:

> *"The Treaty does provide a valuable benefit: It serves as a tool to measure the health of US-Russian relations. Unlike arms treaties and agreements, Open Skies focuses on access and transparency, which are important ingredients for any good relationship between nations. The treaty provides preapproved implementation standards and guidelines for specific operational elements, such as flight routes, altitudes, and timing. These are quantifiable and measurable."* (Reynolds, 2017)

The treaty has survived on the one hand because the US and the Russian Federation are backing it, most visibly through their investment in new aircraft. On the other hand, being a multilateral treaty there exist a range of diverse motivations and interests of parties to adhere to the treaty. States in neighbourhood of the Russian Federation, which lack satellite capabilities of their own, are clearly interested in the technical image data collection. These states include the Baltic States, Finland, Norway, Poland, Romania, Sweden, Turkey and the Ukraine. Interestingly, whereas Ukraine did not undertake observation flights in Russia before 2014, it does so since 2015 as shared flights with other parties. The military forces in the oblast of Kaliningrad are of particular concern for the Baltic States and Poland. Canada is an arctic neighbour of the Russian Federation.

France, Germany, Italy and the UK value Open Skies images as complement to their satellite reconnaissance capabilities but also for the confidence building effect. All parties acknowledge the value of cooperation of their mission personnel on-board and on the ground.

The treaty has a sound architecture and includes options for modernization. The elements of cooperation inspire those who work with the treaty. The built-in checks prevent cheating and guarantee the production of trustworthy images with a high degree of authenticity. However, the military relationship between the Russian Federation on the one hand and many (though not all) of the other parties on the other is characterized by mistrust and antagonism. This is despite cooperation in other fields like civil use of space assets, basic research and commerce. In the military field both sides, the Russian Federation and the US as well as France and the UK, are hostages of the other's nuclear potential. It is a metastable situation. Open Skies can contribute to stabilization in some way, but it is endangered should further escalation occur.

REFERENCES

DVIS (2017). Digital Visual Imaging System, Presentation of the United States of America at the session of the Informal Working Group on Sensors of the OSCC, Vienna 27-29 November 2017, copy in possession of the author

Dunay, P., Krasznai, M., Spitzer, H., Wiemker, R., Wynne, W. (2004). *Open Skies, A cooperative approach to transparency and confidence building,* Geneva, UNIDIR, pp. 318, accessible from http://unidir.org/files/publications/pdfs/open-skies-a-cooperative-approach-to-military-transparency-and-confidence-building-319.pdf, last access 15 August 2019

FAZ (2019). Abschreckung ohne Wettrüsten. Von Russland können regional begrenzte Kriege ausgehen, Frankfurter Allgemeine Zeitung, 10. August 2019

German Verification Center (2019). German Verification Center, private communication to the author. 9 September 2019

GGS (2019). www.ggs-speyer.de and private communication of a representative of GGS to the author

Hartmann, R., Heydrich, W. (2000). *Der Vertrag über den Offenen Himmel,* Baden-Baden, Nomos, pp. 694

IGI (2019). Integrated Geospatial Innovations, DigiCAM-OS, https://www.igi-systems.com/igi-digicam-os.html and private communication to the author

Jones, P. (2014). *Open Skies: Transparency, confidence-building, and the end of Cold war*, Stanford, Stanford University Press, pp.244

KIHOMAC (2016). KIHOMAC wins the full and open competition for a complete visual sensor replacement on OC 135 Open Skies aircraft, February 26, 2016, https://kihomac.com/kihomac-wins-the-full-open-competition-for-complete-visual-sensor-replacement-on-oc-135-open-skies-aircraft/

Krepon, M. (2018). Is Nothing Better than Something? Trashing These Treaties Makes No Sense. www.defenseone.com, October 2, 2018.

Müller, Björn (2016). New “Open Skies” aircraft for the German Armed Forces, 3 March 2016. https://www.offiziere.ch/?p=26700, last access 15 August 2019

NATO (1989). Open Skies Basic Elements. Annex to the Communiqué of the North Atlantic Council meeting 14-15 December 1989, Brussels, NATO Office of Information and Press

Open Skies Review Conference (2010). Briefing Tu 214, OSCC.RC/46/10, 22 June 2010, Vienna, and oral statement of a representative of Russia during the Conference

Open Skies Review Conference (2010a). Contribution of Sweden “Procedures to request Non-Treaty Missions”, OSCC.RC./14/10, 22 June 2010, Vienna

Open Skies (2014). Internal notification of the Russian Federation to all state parties, OS/RB/14/1018/F26/O dated 10 June 2014

Orych, Agata (2015). Entering the Digital Era of the Open Skies Treaty, Geodesy and Cartography, Vol. 64, No. 1, 2015

OSCC (2012). Letter of the Head of the Delegation of Georgia to the OSCC directed to the Chairperson of the Open Skies Consultative Commission, OSCC.DEL/12/12, 4 April 2012

OSCC (2015). Food for thought of the Russian Delegation on the implementation by the States Parties of provisions of the Treaty on Open Skies related to ensuring effective observation of their entire territories, OSCC.DEL/2/13, 30 January 2015

OSCC (2017). Certified Aircraft Sensor Configuration in Use, Document OSCC.DD/2/16/Rev. 1, 28 February 2017

OSCC (2019). Statements by the delegation of the Russian Federation and by the delegation of the United States of America to the Open Skies Consultative Commission, OSCC79.JOUR/268, 17 June 2019, Annex 1 and 3

OSCE (1992). The Treaty on Open Skies, https://www.osce.org/library/14127?download=true, Last access 9 September 2019

Petrie, G., Spitzer, H. (2007). Open Skies: Aerial Observation to Help Prevent Conflicts Between Countries, Geoinformatics, Vol. 10, No. 5, pp. 24-29, download from http://www.petriefied.info/pubs.html → Publication Nr. 116, last access 15 August 2019

Reynolds, George M. (2017). Taking Stock of the Treaty on Open Skies, Council on Foreign Relations, Member Login, Expert Brief, November 03, 2017, New York, accessible via https://www.cfr.org/expert-brief/taking-stock-treaty-open-skies

Richter, Wolfgang (2019). Erneuerung der konventionellen Rüstungskontrolle in Europa, Vom Gleichgewicht der Blöcke zur regionalen Stabilität in der Krise, SWP-Studie 2019/S 17, Juli 2019, pp. 44, download from https://www.swp-berlin.org/fileadmin/contents/products/studien/2019S17_rrw.pdf, last access 2 September 2019

Spitzer, Hartwig (2009). News from Open Skies: A co-operative treaty maintaining military transparency, VERTIC Brief no. 8, Feb. 2009, 16 p., accessible via www.vertic.org, → publications

Spitzer, Hartwig (2011). Open Skies in Turbulence: A Well-Functioning Treaty is Endangered by Outside Developments, Security and Human Rights, Vol. 22, No. 4, Winter 2011, accessible via https://www.znf.uni-hamburg.de/studium/friedensbildung-peacebuilding.html, → Menu → Publikationen → Hartwig Spitzer, last access 2 September 2019

Spitzer, Hartwig (2018). The Open Skies Treaty as a transparency regime. Extended version of a presentation at the International Conference "In Times of Eroding Cooperative Security – How to Save Conventional Arms Control", Loccum 13-15 June 2018, in print 2019 in Loccumer Protokolle, Evangelische Akademie, Loccum, Germany, Download from https://www.znf.uni-hamburg.de/studium/friedensbildung-peacebuilding.html, → Menu →Publikationen → Hartwig Spitzer, last access 2 September 2019

State (2018). US State Department, Bureau of Arms Control, Verification and Compliance, 2018 Report on Adherence to and Compliance With Arms Control, Nonproliferation, and Disarmament Agreements and Commitments, https://www.state.gov/2018-report-on-adherence-to-and-compliance-with-arms-control-nonproliferation-and-disarmament-agreements-and-commitments/

VERTIC (2017). Private communication of a representative of the microsatellite operator Surrey Satellites Ltd. at a seminar held by the Verification Research, Training and Information Centre, London, September 2017

Additive Manufacturing and the Military: Applications and Implications

GRANT CHRISTOPHER
VERTIC

[#34-LONG-PAPER]

ABSTRACT

This article describes military applications of additive manufacturing (AM): what is happening today, what is possible in the future, and what are the implications of these developments for international security. Additive manufacturing is still developing rapidly with what was formerly hype and promise now being turned into deployment and use. Current use cases, for the military, include production of spare parts in the field and shorter development cycles for new systems. We do not yet understand military applications that will arise from the convergence of AM with other emerging technologies such as artificial intelligence. The broader impact on international security is still unclear. The success of using additive manufacturing is highly dependent on the complexity of the object to be produced, the material used, and the process used to produce it. Strategies to control use of this technology can mirror current export controls for advanced machine tools or focus more permissive controls for digital build files for each individual printer or on the control of the digital files themselves.

1. INTRODUCTION

The implications of additive manufacturing (AM) for the military are not yet understood. The hype of a technology that has been described as capable of transforming where things are made, what they are made of, and by whom, (Economist, 2011) must be tempered by reality.

In AM, parts are built using a computer-programmable machine tool from smaller pieces, similar to a robot that is programmed to build a Lego model. Unlike Lego, which is restricted by the available plastic bricks and stuck together using friction, in AM a computer-controlled melting processes are used to construct a predesigned shape using wires and powder composed from an ever-widening base of materials.

AM is desired for several benefits: it can be used to shorten system development cycles (Goodwin, 2015), introduce cost savings by consolidating components (Kellner, 2015), allow printing in the field (Asclipiadis, 2014), and reduce the mass for components used in aerospace and space (Froes, Boyer, & Dutta, 2019). It will enable faster repairs of damaged systems, enable production of embedded electronics, such as conformal antennae (Esfahani et al., 2018), and conserve valuable material when manufacturing. The agility and flexibility to rapidly design new systems will allow those states with mastery of AM to be better placed to answer unexpected strategic challenges (Schrand, 2016). It can be used to produce individual parts, such as an individual fuel nozzle that fits onto an aircraft (Roschli et al., 2019; Underwood, 2015), or whole systems such as a conventional warhead or missile (Relativity, 2019).

For military applications, relevant printing techniques can be divided into the extrusion methods that melt a material such as thermoplastic wire, directed energy techniques that fully melt a metal, ceramic or high-performance plastic powder or wire, and binder jetting techniques that adhere metal, ceramic or high-performance plastic powder that is then sintered. Materials available include nickel superalloys, titanium, maraging steel and high-performance plastics such as PEEK.

Powder metal printing, the most precise and complex AM process, deposits layers that are 60 micrometres thick, but final part will not maintain this resolution, which will be closer to a tenth of a millimetre. Powder metal printing occurs in an inert atmosphere, which limits the build volume to half a cubic metre. Large area printing is possible, for instance using Oak Ridge National Laboratory's thermoplastic extrusion technique, known as Big Area Additive Manufacturing (BAAM) (Roschli et al., 2019) which can be used to print moulds for aircraft wings. Large area metal printing is also possible: Sciaky's Electron Beam Additive Manufacturing (EBAM) has been used to print titanium propellant tanks for NASA (Kenyon, 2015). The variety of materials available to print is staggering. They range from ultra-hard steels such as maraging steel 300 to specialised metals such as Inconel or Zircaloy.

Yet, AM is a difficult and complex process. Serious discussion of AM must temper the hype with a realistic assessment of what the technology is capable of. AM is not 'plug and play'. For instance, new metal powder printing machines require a six-month commissioning period and individual calibration before entering production (Volpe, Christopher, Kühn, Loehrke, & Shoaf, 2018). Quality control of parts and the slowness of the printing process itself is a serious issue: ISO and ASTM have only just begun publishing industry standards as acknowledged by the United States Department of Defense in their 2016 roadmap for AM (DoD, 2016). In the current generation of metal powder printers, it takes several days to print a 20-centimetre part. Failures that occur in the first few hours will not be discovered until the end of the printing process. This high barrier to entry will limit AM's adoption by state and non-state actors that fail to acquire the tacit knowledge required for this complex manufacturing process.

The development of AM also poses risks by potentially enabling horizontal proliferation, for both state and non-state actors, via the availability of the technology and the increased risk of cyber espionage (Fey, 2017) and easy access to crude conventional weapons (Nelson, 2015). The shortening of supply chains and the ability to rapidly design new components will also impact military planning and as development continues has the potential to be game-changing for military logistics (Schrand, 2016).

This paper will assess AM with regards to convergence with key technologies that enable relevant capabilities with context for their impact on international security. This is followed by a description of how adversaries may adopt and benefit from AM and finally, the outline of possible means to reduce these risks.

2. THE IMPACT OF AM

The development of AM is occurring in parallel with significant technological advances in other sectors, such as Artificial Intelligence (AI), increased computing speed and cloud computing. We, therefore, discuss developments and advances in AM in this context.

2.1. AM, HIGH-PERFORMANCE COMPUTING AND AI

High-performance computing allows the use of more detailed computer models when prototyping. The driver of the fast development cycle in AM is not just the process itself but the combination of AM with computer modelling (Goodwin, 2015). Increased computing power permits the use of more accurate models of performance under operational conditions. Development cycles can be drastically shortened using an iterative process of modelling, producing prototypes and feeding the test results from the prototype back into the design. The AM process, which builds a product from the ground up, may also allow the verification of a part as it is constructed further contributing to shortening development cycles (DoE, 2019).

Machine learning, itself enabled by increases in computing power, can also be used to model failure modes of AM parts in real time (Jackson, 2018). Although it may take some achieve this capability, first steps are being taken, as demonstrated with the collaboration between the United States Navy's Office of Naval Research and AM tech company Senvol to improve the printing process using machine learning ("Senvol Developing Machine Learning Software of US Navy for Additive Manufacturing," 2018). The expected improvement this will provide in reliability will encourage adoption of AM and encourage the risk-averse security sector to use AM to produce critical components.

The implications are that new systems can be developed in such short periods that they can impact military operations in months, rather than years. They can be deployed during a single extended operation or campaign if a tactical vulnerability is identified that can be countered with a new system designed in-part using AM (Schrand, 2016).

2.2. AM AND THE IOT

The Internet of Things (IoT) is the set of devices that can communicate over the internet or a private secure network. Connecting AM machines to the IoT enables two significant capabilities for AM-produced parts. First, distributed ledger technologies, or blockchains, can be used to both grant permissions for permitted users and validate that the contents of digital build files for AM machines that are on a secure IoT node (Hoffman & Volpe, 2018). Assurances by the blockchain that digital build files are free from industrial sabotage will provides an additional layer of security beyond encryption. Such techniques can be adopted to limit the proliferation of any part produced using AM or any other computer-aided manufacturing technique.

Second, sensors connected to the IoT can be used to monitor the performance of components in-situ (G. Christopher, 2018). When instrumented with sensors, a part's operating conditions can be communicated to a secure data cloud to provide performance data. Machine learning can then be used to model when a part is likely to fail, leading to predictive maintenance. This is, of course, all possible without AM. The innovation provided by AM is the possibility to produce parts with embedded sensors, thus increasing the reach of the IoT. Systems with embedded sensors will be more reliable so will reduce costs over time, they will improve safety by decreasing the likelihood of catastrophic accidents and will increase the confidence in AM. Instrumented sensors will also have tactical military applications. If embedded in battlefield equipment and uniforms sensors can be used to monitor battlefield conditions to relay information about the tactical environment.

Integrated sensors could open up new possibilities for verification and monitoring of arms control agreements. AM cannot solve purely political problems about the introduction of sensors into a facility, but for organisations that conduct inspections and remote monitoring incorporating sensors into facility production equipment, as a plant is being designed, or by replacing older components, could be an attractive prospect.

2.3. AM AND 3D SCANNING

When supply chains fail, or individual parts are available only via an expensive batch process, AM can be used to reverse engineer a component by 3D scanning the part to produce a digital model, such as the impeller printed by Siemens for the Krško nuclear power plant in Slovenia (Siemens, 2017). AM can also be used to produce machine tools and ‘widgets’ that previously only were available via more costly, slower production methods (NNSA, 2016). This is used to keep down costs and also extend the lifetimes of older systems (Johnston, Smith, & Irwin, 2018).

2.4. AM AND SHORTENED SUPPLY CHAINS

The ultimate shortened supply chain for the military is the ability to print in the field. The United States Army Rapid Equipment Force (REF) has been using 3D printing in the field since 2012 (Asclipiadis, 2014). This can be used to perform maintenance and routine tasks as well as providing militaries with flexibility for problem solving in the field (Schrand, 2016). AM is also being included in plans for combat readiness by reducing the requirement to maintain a full inventory of replacement parts (JL, 2018).

3. HOW AM COULD DESTABILISE INTERNATIONAL SECURITY

With AM, manufacturing becomes local and immediate. Moreover, AM will be able to iterate multiple generations of a system before a conventionally manufactured system is even deployed.

This points to several possible effects. First, in a future conflict, a state that is able to maintain an asymmetric advantage in design agility and flexibility will better placed to counter any unanticipated strategic or tactical disadvantage (Schrand, 2016). By contrast, conflict between AM-capable states could result in a dynamic where systems and counter-systems are rapidly developed.

Second, If AM can deploy full systems that are cheap and easily replaced, states that are overly-reliant on small numbers of expensive systems could be overwhelmed without a commensurate rapid manufacturing capability. Modern militaries are composed of expensive, difficult to replace systems. All but the most well-resourced states in a prolonged conflict will lose systems to attrition that cannot be replaced. For instance, states that rely on ballistic missile defence, (BMD), rapid production of missiles could saturate and overwhelm the designed systems before they can be upgraded (Walsh, 2017).

Third, limiting the spread of new technologies is nearly impossible. Any new proven new capability that AM provides will eventually spread to potential adversary states. As AM has developed, the introduction of electronic printing, which will allow the integration of sensors, is one such AM-enabled technique that will provide new capabilities that are not replicable via other manufacturing techniques.

These risks, as described, may not be as great as they first appear. Bar some extreme cases, such as Relativity's in-development entirely 3D printed rocket (Relativity, 2019), AM is being used on a component-by-component basis, where it provides some efficiency or new capability, rather than being used to print entire systems.

In the OECD countries, there are clear applications and use cases of AM that are being developed for use by militaries (DoD, 2016). Potential adversaries have no doubt observed gains and promising areas of AM and will seek to emulate such successes in their own weapons programmes.

AM could enable proliferation of advanced technologies to both state and non-state actors. In particular, in states that fear isolation due to sanctions, such as North Korea and Iran, AM could be pursued as a means to evade sanctions and achieve autarky (Johnston et al., 2018). AM hardware and raw materials are largely free from export controls so should be less difficult than conventional hardware for states to acquire. AM also wastes less material than subtractive techniques so it will be attractive for programmes with limited quantities of material. This could be used in any case where AM can substitute for conventional manufacturing, which at present ranges from production of liquid-fuel propulsion systems to turbines and small unmanned systems.

States and non-state actors with cyber espionage capabilities will seek to acquire designs and intellectual property associated with advanced systems in either a targeted or opportunistic manner. Destroyed or damaged systems that are acquired, via encounters or by accident, will become easier to reverse engineer using 3D scanning and printing technologies (Johnston et al., 2018).

4. ADDRESSING THE CHALLENGE

Fey (Fey, 2017) describes five broad areas to address risks posed by AM: (1) strengthening cybersecurity, (2) safeguards in hardware, (3) export controls, (4) awareness and (5) industry self-regulation.

Deterring cyber-theft of intellectual property by advanced state-backed cyber-espionage programmes is a broader problem that applies to all computer aided manufacturing. The most valuable intellectual property for AM is not the geometry of the part but the instructions to the machine for how to build it. Yet, while AM remains difficult, stealing digital design files and associated hardware parameters will only provide very advanced users with the ability to successfully manufacture the part.

Export controls are a more difficult prospect. Additive manufacturing is being developed globally, including in non-OECD countries (G. E. Christopher, 2018). The leaders in developing AM include North America, Western Europe Japan, South Korea, China and Russia. In addition to traditional manufacturing hubs, International service providers are present all over the globe including in areas of weak export control enforcement. Attempts to control the spread of the technology will require the use of multilateral regimes and a willingness, that has not yet been expressed, for adequate controls to be put in place. States must balance their interests in developing new technology sectors with the associated risks with the spread of the technology. Reluctance to control the technology is rooted in a desire to maintain any commercial advantage which will also lessen the effectiveness of self-regulation by industry. As military applications emerge the appetite to control the technology may increase commensurately.

Guiding the rise of AM to ensure maximum benefits are reaped – while addressing security risks – is a difficult challenge for policy makers. But AM has not yet reached its full potential so we do not know how it will most impact international security. Based on our current understanding, AM will not be transformative on strategy and nor will it render export controls obsolete, but will likely have a significant impact in the specific areas of design, mobile repairs and integrated sensors.

REFERENCES

Asclipiadis, A. (2014). Rapid Equipping Force uses 3-D printing on the frontline. URL: https://www.army.mil/article/129635/Rapid_Equipping_Force_uses_3_D_printing_on_the_frontline/

Christopher, G. (2018). *Additive Manufacturing: The Future for Safeguards.* Paper presented at the IAEA Symposium on International Safeguards, Vienna.

Christopher, G. E. (2018). *3D Printing: A Challenge to Nuclear Export Controls*. Retrieved from Ridgeway Information: https://irp-cdn.multiscreensite.com/90a0a242/files/uploaded/GC_3D_Printing_Nuclear_PASCC.pdf

DoD. (2016). *Department of Defense Additive Manufacturing Roadmap*. Retrieved from America Makes: https://www.americamakes.us/wp-content/uploads/sites/2/2017/05/Final-Report-DoDRoadmapping-FINAL120216.pdf

DoE. (2019). 4 Major opportunities for additive manufacturing in nuclear energy. URL: https://www.energy.gov/ne/articles/4-major-opportunities-additive-manufacturing-nuclear-energy

Economist. (2011). Print me a Stradivarius. *The Economist, 398*(8720), 11.

Esfahani, M. R. N., Shuttleworth, M. P., Harris, R. A., Kay, R. W., Doychinov, V., Robertson, I. D., Desmulliez, M. P. Y. (2018, 16-18 July 2018). *Hybrid Additive Manufacture of Conformal Antennas.* Paper presented at the 2018 IEEE MTT-S International Microwave Workshop Series on Advanced Materials and Processes for RF and THz Applications (IMWS-AMP).

Fey, M. (2017). *3D Printing and International Security: Risks and Challenges of an Emerging Technology*. Retrieved from http://nbn-resolving.de/urn:nbn:de:0168-ssoar-51867-8

Froes, F., Boyer, R., & Dutta, B. (2019). 1 - Introduction to aerospace materials requirements and the role of additive manufacturing. In F. Froes & R. Boyer (Eds.), *Additive Manufacturing for the Aerospace Industry* (pp. 1-6): Elsevier.

Goodwin, B. (2015). *Additive Manufacturing and High-Performance Computing: a Disruptive Latent Technology.* Paper presented at the APS March Meeting 2015, San Antonio, TX, USA.

Hoffman, W., & Volpe, T. A. (2018). Internet of nuclear things: Managing the proliferation risks of 3-D printing technology. *Bulletin of the Atomic Scientists, 74*(2), 102-113. doi:10.1080/00963402.2018.1436811

Jackson, B. (2018, 16 February). Real-Time Metal 3d Printer Monitoring At El Paso Awarded In $900k ARL Grant. URL: https://3dprintingindustry.com/news/real-time-metal-3d-printer-monitoring-el-paso-awarded-900k-arl-grant-129057/

JL. (2018). Revolutionizing an entire supply chain: additive manufacturing and the US Army. URL: https://digital.hbs.edu/platform-rctom/submission/revolutionizing-an-entire-supply-chain-additive-manufacturing-and-the-us-army/

Johnston, T., Smith, T. D., & Irwin, J. L. (2018). *Addditive Manufacturing in 2040: Powerful Enabler, Disruptive Threat* (PE-283-RC). Retrieved from RAND: https://www.rand.org/pubs/perspectives/PE283.html

Kellner, T. (2015). The FAA Cleared the First 3D Printed Part to Fly in a Commercial Jet Engine from GE. URL: http://www.gereports.com/post/116402870270/the-faa-cleared-the-first-3d-printed-part-to-fly/

Kenyon, H. (2015, 30 August). 3-D Manufacturing's Holy Grail. URL: https://www.sci-aky.com/images/pdfs/3D-Manufacturing-Holy-Grail-by-Aerospace-America.pdf

Nelson, A. J. (2015). The Truth About 3-D Printing And Nuclear Proliferation. URL: https://warontherocks.com/2015/12/the-truth-about-3-d-printing-and-nuclear-proliferation/

NNSA. (2016). KCNSC reaches milestone in digital manufacturing. URL: https://www.energy.gov/nnsa/articles/kcnsc-reaches-milestone-digital-manufacturing

Relativity. (2019). Relativity - Mission. URL: https://www.relativityspace.com/

Roschli, A., Gaul, K. T., Boulger, A. M., Post, B. K., Chesser, P. C., Love, L. J., Borish, M. (2019). Designing for Big Area Additive Manufacturing. *Additive Manufacturing, 25*, 275-285. doi:https://doi.org/10.1016/j.addma.2018.11.006

Schrand, A. M. (2016). Additive Manufacturing: From Form to Function. *Strategic Studies Quarterly, 10*(3), 74-90.

Senvol Developing Machine Learning Software of US Navy for Additive Manufacturing. (2018, 13 March). URL: http://senvol.com/2018/03/13/senvol-developing-machine-learning-software-u-s-navy-additive-manufacturing/

Siemens. (2017, 9 March 2017). Siemens sets milestone with first 3D-printed part operating in nuclear power plant. URL: http://www.siemens.com/press/pool/de/pressemitteilungen/2017/powergenerationservices/PR2017030221PSEN.pdf

Underwood, J. (2015, 15 June 2015). GE Aviation readies first 3-D printed jet engine nozzle at Alabama plant. URL: http://www.madeinalabama.com/2015/06/ge-aviation-readies-first-3-d-printed-jet-engine-nozzle/

Volpe, T., Christopher, G., Kühn, U., Loehrke, B., & Shoaf, S. (2018). *Additive Manufacturing and Nuclear Nonproliferation: Shared Perspectives on Security Implications and Governance Options*. Retrieved from https://www.stanleyfoundation.org/publications/pdb/AddManfPDB1018.pdf

Walsh, D. (2017, 24 July). Additive Manufacturing: The Next Great Challenge to Missile Defence. URL: https://www.nuclearreactions.rusi.org/single-post/2017/07/24/Additive-Manufacturing-The-Next-Great-Challenge-to-Missile-Defence

Seeing the Drone from the Swarm – Social and Technical Barriers to Drone Swarm Proliferation

LINDSAY RAND

CENTER FOR INTERNATIONAL AND SECURITY STUDIES AT MARYLAND, UNIVERSITY OF MARYLAND

[#35-LONG-PAPER]

ABSTRACT

As swarm technologies continue to garner attention among international security experts, misdiagnosis of the feasible rate and style of swarm proliferation has led to overly-assumptive, and subsequently inefficient, policy responses. The current body of literature on drone swarms identifies various aspects of international security that armed drone swarms could augment if implemented. In these analyses, impact magnitudes and policy action scopes hinge on the assumption of an unrealistically fast rate of proliferation. This distortion appears to be largely driven by the fact that swarms are derivatives of drones, and drones have proliferated rapidly on the global scale. However, swarm systems differ from individual drones because they require an increased level of autonomy in order to function. In conflating the two technologies when predicting proliferation potential, current analyses often ignore the impact that technical and social barriers unique to swarm development will have on the rate of swarm proliferation, and thus over-dramatize the predicted proliferation rate and overall applicability of swarms. This paper presents a more conservative estimate of swarm proliferation rate that takes into account technical and social barriers, and that allows for more concrete policy responses to target specific aspects of drone swarm proliferation through triaging the most imminent security risks.

1. INTRODUCTION

Although the security world has yet to grapple with and become accustomed to the use of armed drones in defense activities, the recent application of drones as “drone swarms” further raises the stakes and intricacies of establishing an international order and rules system for armed drones, as well as developing national military postures toward the use of such technologies. With respect to their military application, armed drones have sparked concern among international security scholars and practitioners due to the insufficiency with which they are covered in current arms and export control agreements (Altmann, 2013) and the lack of transparency in their use for inter-military operations; many states, including the U.S., maintain a posture of 'strategic ambiguity' in drone operation (Ewers et. al., 2017). These issues have yet to be resolved at the international level and tension points have been exacerbated by the sheer rate at which drones have proliferated (Buchanan and Keohane, 2015). Because drone swarms are composed of drones, they elicit similar concerns that drones do, however, as they are augmented by increased autonomy, they also infuse new concerns that were typically peripheral and prospective in drone policymaking (Kallenborn and Bleek, 2019). In light of the fact that drone swarms promise to exacerbate tensions rising from a lack of comprehensive drone policy, as well as introduce new concerns arising from increased autonomy, there have been a number of commentaries arguing that drone swarms will profoundly change military combat (Hambling, 2015; Scharre, 2014; Scharre, 2018). However, analyses that claim swarms to be indicators of a new wave of military combat tend to assume or imply that swarms will proliferate as rapidly as drones have and may eventually become quotidian functions of military activities.

Scholars and practitioners have already highlighted a number of concerning implications that could arise from implementation of armed drone swarms, including: ethical and operational issues arising from military technologies operating with an increased level of autonomy, disruption of current defense strategies due to the increased offensive capability allowed for by drone swarms, elevated risks for proliferation or use of chemical, biological, radiological and nuclear (CBRN) warfare systems in tandem with drone swarm development, and the general potential that swarms will have to disrupt strategic stability. Although autonomy has long been viewed as a forthcoming threat in the drone policy sphere (Sparrow, 2007; Sharkey, 2012; Asaro, 2012), the impetus to actually engage in meaningful debates and discussions that would conclusively determine some sort of international consensus on an acceptable level of autonomy has been undercut by the fact that drones can ostensibly maintain a meaningful level of human interaction, to some degree, for nearly every strategic action. However, since swarms are inherently reliant on automation in order to perform even basic functions, and unlike drones cannot perform at least some strategic actions under the direct control of a human operator, their introduction in the military technology sphere necessitates greater dialogue on autonomy. Beyond the legal and moral dimensions of autonomy, there is also concern over the sheer physical power that swarms composed of large numbers of drones will have. Scientists and engineers have indicated that the development of technological methods to protect against swarms will be difficult and expensive (Scharre, 2015, "Counter-Swarm"; Tucker, 2018). Scholars have also examined swarms in the context of CBRN warfare technologies and have identified the various ways in which drone swarms could be used to complement or substitute for CBRN technologies, or to challenge CBRN technologies when used in opposition (Kallenborn and Bleek, 2019). Finally, both with respect to CBRN and conventional weapons, scholars have argued that swarms have the potential to decrease strategic stability in a number of domains and thus may increase the risk of conflict escalation (Kallenborn and Bleek, 2019; Altmann and Sauer, 2017).

However, the current literature on drone swarms is lacking in depth of analysis on how swarm proliferation will occur. The scholars that have written more intensively about drone swarms have only vaguely alluded to the proliferation process, and in cases where proliferation is explicitly discussed, most have simply argued for the high likelihood of largescale drone swarm proliferation based on the fact that drones themselves are widely available (Ewers et. al., 2017). Beyond these brief considerations, very little has been written about the social and technical barriers that those hoping to develop drone swarms will face. This omission has prevented consideration of the ways in which relevant barriers will shape the availability and application of swarm technology, and how such an analysis could be used to prepare more targeted arms control or international agreement opportunities to limit the use and detrimental impact of armed drone swarms.

This paper will survey the validity of the concerns raised in current research based on a closer consideration of the technical and social foundation of drone swarm technology. The background and threat identification sections of this paper will discuss the technological differences between armed drones and drone swarms, and then survey the body of literature on the threats introduced by armed drone swarm implementation. However, because current analyses overlook the realistic barriers that swarm technology development is likely to face, there is limited discussion on the realistic imminence of these threats and what form early use will take. Thus, this paper will expand upon the current body of literature by analyzing the technical and social barriers that will constrain the proliferation potential of drone swarms and posit potential resulting options for policymakers based on the re-framing of drone swarm threat immediacy. Under this analysis, this paper argues that social and technical factors should be used to temper the current predictions with regard to how rapidly drone swarms will be employed and what capabilities early swarms will have. Finally, this paper demonstrates how a more nuanced proliferation consideration can ultimately allow for the ability to triage the risks introduced by drone swarms and to develop more concrete policies to address high-priority risks.

2. Background

2.1. Distinguishing Between Swarms and Drones

The individual physical components of swarms are derived nearly entirely from current drone technology, which has already been implemented for quite some time in the defense realm. Among defense and security scholars, drones are typically referred to as either unmanned aerial vehicles (UAVS), unmanned ground vehicles (UGVs), or unmanned underwater vehicles (UUVs), depending on where they are operating. Drone technologies have triggered apprehension since their initial implementation. Concern over drone technology has been rooted both in its tactical application, such as drone killing, and surveillance application. Drones used for tactical purposes and that carry weapons are typically referred to as armed drones. This paper will focus on armed drones and armed drone swarms (swarms composed of armed drones), though significant literature can be found on drone use for alternative purposes.

Armed drone use has been criticized at the moral, legal, technical, and strategic levels. With regard to tactical use, scholars such as Frank Sauer and Niklas Schornig argue that drone killing is morally, legally, and politically problematic (Sauer and Schornig, 2012). At a more macro level, scholars have also argued that drone application has led to an increased likelihood of conflict by lowering the cost to the initiator and thus incentivizing first use (Sauer and

Schornig, 2012). Beyond the disruption caused by drones themselves, scholars have also identified ways in which drones could disrupt linked technical systems. This could be through direct technical interference, such as through the command, control, communication, and intelligence (C3I) network, or through heightening political tension and increasing disagreement among potential adversaries (Zhao, 2018).

Swarm implementation not only carries the same concerns as drone implementation, but also introduces new concerns through the physical enhancement of increased drone numbers and (potentially but not necessarily) variability and through the digital enhancement of increased autonomy. Drone swarms are systems of multiple drones that work together, while not operating identically, to complete a shared, group objective (Scharre, 2015, "Unleash the Swarm"; Scharre, 2018). Paul Scharre defines swarms as, "large numbers of dispersed individuals or small groups coordinating together and fighting as a coherent whole," (Scharre, 2014). While the physical technology basis for swarms is similar to drones, swarms must be augmented by digital technology innovation. Swarms operate by relying on some type of communication and processing network that allows for individual drones to perform basic operations independently, as well as communicate with other drones in the swarm and a command base, without necessarily having to revert back to a central command for every individual action. The extent of regulation and oversight exerted by the central intelligent control of the swarm designates whether the swarm has a central command (high central control), or exhibits distributed, emergent behavior (limited central control). Because of this immense communication coordination network, most subject matter experts agree that in order to allow for the unique operation of each individual drone, working coherently with the entire swarm *in real time* and responding to unplanned environment changes, drones in a swarm must be granted a requisite amount of autonomy (e.g. Chandhar, Danev, & Larsson, 2016). Thus, swarm application introduces two unique issues that extend beyond those already prevalent for single-drone military activities: the physical problem of having multiple drones operating simultaneously, and thus increasing the tactical threat and difficulty to defend against, and the legal and moral complications regarding increased autonomy, and thus less meaningful human control, in accomplishing military objectives.

2.2. APPLICATION SURVEY

Due to their physical and digital enhancements, a wide range of swarm applications have been identified across both the civilian and military domains. In "The Upside and Downside of Swarming Drones," Irving Lachow specifies three main military use categories for swarms: attack, defense, and support functions (including intelligence, surveillance, and reconnaissance). The benefits of using swarms in these applications largely derive from the swarm's ability to disperse multiple agents over a large area, ensure an increased level of survivability, and increase the difficulty of developing countermeasures (Lachow, 2017). Military scholars argue that because of these features, integration of swarms into warfare allows for greater efficacy, lethality, and survivability, as well as the opportunity for parallel warfare (Williams, 2018; Arquilla and Ronfeldt, 2000; Scharre, 2014; Hurst, 2017). However, beyond the military domain, a wide range of civilian applications have also been identified, making swarms a dual-use technology. Interestingly, very crude swarms have already been used in the entertainment industry as alternatives to fireworks, with a 300-drone pre-programmed swarm having been employed in Lady Gaga's Super Bowl halftime show. Other potential applications that have been suggested for future use include agricultural processes, such as water and pesticide dispersal, search and rescue operations, package distribution, and industrial management (Hambling, 2017).

As the breadth and utility of these applications continue to grow in prominence, so has funding and research progress towards actual swarm implementation. Beyond private industry research and development for civilian purposes, many countries are developing military-based swarm programs. Most recently, the United Kingdom government issued a series of funding allocations for drone swarm projects, including projects on mini drones and the 'Many Drones Make Light Work' project (U.K. Ministry of Defence, 2019). In the U.S., drone swarm prototype systems have been publicly tested since as early as 2016, with the testing of a Perdix drone swarm (U.S. Department of Defense, 2017). China has also been aggressively pursuing drone swarm technologies and is suspected of having more extensively tested drone swarms and developed advanced autonomy and artificial capabilities to specifically enhance swarm operation (Romaniuk and Burgers, 2018). Although not necessarily under the Chinese military, but in coordination with them, the China Electronics Technology Group Corporation (CETC) has tested drone swarms composed of 67, 119, and 200 UAVs (Kania, 2019). Other countries that are actively pursuing military swarms include South Korea, Russia, Turkey, and Israel (Kallenborn & Bleek, 2019; Hambling, 2018).

3. THREAT IDENTIFICATION

While swarms offer many benign, beneficial uses in both the civilian and military domains, their implementation also presents new challenges to the international community. Scholars have recently begun to think more critically of the impact that military use of drone swarms could have as the technology begins to grow more developed and implementation seems more imminent. Threats have been identified through consideration of the impact that swarms will have on other technology systems, the feasibility of wide-spread horizontal proliferation, the potential for escalation due to swarm malfunction or uncontrolled swarm interactions, and the ever-pressing moral and legal dilemmas resulting from increased autonomy.

3.1. IMPACT ON EXISTING SYSTEMS

One key area of swarm policy research that has evolved focuses on the impact that swarms will have on existing technology systems and the strategic stability that has been established for these legacy systems. As swarms have fallen under the more general security studies category of "emerging technologies," scholars in the security field have applied a methodological approach in thinking about swarm implication that is similar to what they have used in thinking about other emerging technologies (Bidwell and MacDonald, 2018). Within the focus area of emerging technologies, which has recently experienced a resurgence in interest and resource allocation (Ford, 2017), a general approach of identifying impact potential has developed. Primarily, impact potential is measured by whether or not a technology incentivizes first-use where it was not previously incentivized, either of the technology itself or of the technical system it is disrupting, or whether the emerging technology alters the survivability of an established technology system (Bidwell and MacDonald, 2018). For example, under this analysis, the fact that tactical swarm applications could lead a country to believe that it can circumvent a missile defense system more easily, and thus provides greater incentivization for first use would indicate a high impact potential. At the same time, swarms could also disrupt the perceived survivability of nuclear weapons by inhibiting the usability of a missile defense system. With respect to armed drone swarms, scholars such as Zachary Kallenborn and Philipp Bleek have highlighted the potential applications that drones could have in the dispersal of chemical, biological, radionuclide, nuclear, or explosive weapons (Kallenborn and Bleek, 2019). However, impact potential in the military realm can also be determined based on a number of other factors, such as whether a technology makes an existing system obsolete or intensifies an arms race (Altmann, 2005). The emphasis on impact potential in this line of research also often affords emerging technologies deemed capable of having a disruptive impact on the name of "disruptive technologies."

It should be noted that up until now such research has neglected consideration of the technical feasibility of constructing a swarm system capable of successfully accomplishing such goals, and even less consideration has been given to the potential for swarms to match the development of anti-swarm technologies. Anti-swarm technologies are currently assessed to be at a relatively nascent stage of research and development. But it has been argued that if a soft, non-kinetic) anti-swarm defense method is found it could deny use for a specific area fairly effectively, even if kinetic counter-swarm technologies, such as air-defense artillery, are less effective (Frantzman, 2019; Scharre, 2015, "Counter-Swarms"; Shmuel, 2018). Scharre has identified a number of options that could be considered in developing anti-swarm technologies, including: low cost-per-shot weapons, such as lasers or electromagnetic rail guns, or even machine guns; another swarm; high-powered microwaves; swarm communication jammers; strategic traps to get guide the swarm into a disadvantageous position; or even software infiltration capabilities to allow for hijacking the swarm. Despite this diverse assortment of potential defenses, Scharre does concede that research and development on anti-swarm efforts are still in early stages of consideration, as is evidenced by the fact that the U.S. military budget for counter-swarm measures is spread across such a wide variety of potential options (Scharre, 2015, "Counter-Swarms").

3.2. EASE OF HORIZONTAL PROLIFERATION

In addition to the threats posed by swarms augmenting highly-developed military capabilities, such as CBRN systems, scholars have also identified the threat of rudimentary, conventionally armed drone swarms, exacerbated by the ease of access to the core drone technologies. Although there certainly are high-level drone technologies that require a large amount of capital and scientific expertise to acquire or develop, there are also types of drones that are able to be constructed or purchased with minimal knowledge and financial resources (Woodhams, 2018; Ewers et. al., 2017). Furthermore, countries that do have the adequate technical background and financial resources are able to buy nearly exact derivatives of other countries' drone technologies, as was the case with the Netherlands and Belgium acquisition of a variation on a U.S.-made drone (Woodhams, 2018). Thus, because of the sheer ease in acquiring the basic drones required for swarms, many scholars have posited that drone swarms will proliferate rapidly (Madrigal, 2018; Homayounnejad, 2018). Additionally, analyses asserting wide horizontal proliferation have led to fears of terrorist acquisition of drone swarms, especially as drones have already been identified as a key technology for non-state actors (Tonnessen, 2017; Tucker, 2017; Hurst, 2019). In this respect, scholars argue that such horizontal proliferation could allow for non-state actors or other rogue actors with minimal resources to have an asymmetric impact in security domains (Hurst, 2019).

3.3. Unintended Escalation, Flash Wars, or Flash Attacks

Another threat pertains to the probability that a swarm would malfunction due to a technological accident, a hijacking, or in a response to an adversary's system/swarm and lead to unintended escalation: such types of accidents are referred to as unintended escalation, "flash wars," or "flash attacks" (Scharre, 2014; Scharre, 2018; Altmann and Sauer, 2017). Concern over this threat is also echoed by researchers studying emerging technologies, such as James Acton who claim that newer technologies have undergone less testing, and may malfunction in the real-world, resulting in inadvertent escalation (Acton, 2018). Early technical research exploring swarm applications identified the difficulty of fully verifying that swarm technologies will operate properly without malfunction (Vanderbilt et al. 2004). For example, a malfunction could include the swarm losing connectivity to its human controller, and thus having to operate on an entirely autonomous basis. Additionally, because swarm technology efficacy is difficult to verify, malware could be programmed in intentionally, and may go undetected. Scholars have also cautioned that artificial intelligence (AI) integration into drone swarms could lead to swarms operating more autonomously than what was initially intended. Scharre writes, "Increased autonomy in the use of force raises the dangerous specter of "flash wars" initiated by autonomous systems interacting on the battlefield in ways that may be unpredictable," (Scharre, 2014; Scharre, 2018). Finally, drone swarms could be hacked or experience a cyber-attack that makes them operate in a manner different from what the operating party intended; this could allow for an adversary or a third party to intervene in a strategic operation or military exercise (Wesson and Humphreys, 2013). In *Military Robots and Drones*, Robert Springer suggests that "autonomous combat systems offer the possibility to create a consummate double agent or sleeper, appearing to function normally until a critical moment, when a malfunction or loss of operator control can yield a devastating result," (Springer, 2013).

3.4. Increased Autonomy

The final threat that has received a significant amount of attention, and which has been previously alluded to multiple times in this article already, is the increased autonomy required for drone swarms. The concerns regarding autonomously functioning military technologies are multifold. With regard to defense oversight and organizational structure, there is concern over the level of accountability that can be ascertained with an autonomous system and the difficulty of tracing the decision-making process for an autonomous system in order to determine a problem or assign culpability (Scharre, 2014; Scharre, 2018). With respect to the technology itself, there are concerns over whether or not there would be bias in the coding, and how such biases and prejudices may impact the life or death decisions made by the autonomous system (Knight, 2017). Finally, legal, moral, and ethical concerns also arise from autonomy; significant consideration has been given at the international level to determine whether or not combat with autonomous robots is unethical, violates basic human rights, or is illegal under the Laws of War (Sparrow, 2007; Sharkey, 2012; Asaro, 2012; Singer, 2009; Wilson, 2014).

4. Socio-Technical Considerations to Constrain Proliferation Predictions

As this analysis has shown, swarm implementation introduces a number of potential risks; however, despite the fact that efforts have been taken to mitigate identified risks, such efforts become misdirected and ineffective when the realistic proliferation drivers and mechanisms are not taken into account. Although the sheer assortment of beneficial uses of swarms, both for civilian and military purposes, may convince some scholars and policymakers that proliferation is inevitable, there are significant social and technical hurdles that nations looking to incorporate swarm tactics into their militaries will have to surmount before implementation. The key social hurdle identified here is the necessary use of autonomy, distinguishing armed swarm use from armed drone use. The key technical hurdle identified here is the requirement of advanced systems engineering and communication technologies necessary for the development of each specific type of swarm. The significance of these hurdles is heightened by the fact that swarm development will have to be task driven, and thus swarms developed in the civilian sphere will not be easily transferrable to the military sphere, minimizing the risks that swarms normalized in the civilian realm will pave the way towards military swarm use. Once these hurdles are considered in more depth, the future of swarm technology application appears much more limited, and thus ultimately allows for more clear and targeted policy approaches based on the proliferation pathways that are identified as most likely. This section will assess the relevance of social pressures and technical constraints in obstructing wide-scale proliferation and use of different types of armed drone swarms, allowing for more narrow and targeted policy recommendations to be given in the following section.

4.1. Social Construction of Technology

Whether or not the threats introduced by military application will alter the reception of drone swarms, and thus the number of missions that drone swarms are applied to in the international security field, varies depending on if the question is approached using either the social construction of technology framework or the technological determinism framework. Under the social construction of technology framework, social acceptance and use of a technology impacts the development trajectory of the technology, and thus significant social apprehension will place a limiting pressure on the number and types of applications for the given technology. Based on the number of social concerns regarding autonomy, strategic stability implications, unintended escalation, and horizontal proliferation, the social construction of technology theoretical framework would argue that the development of drone swarms could be impeded as a result of the social concerns. The social construction of technology framework contrasts the easily, and often unconsciously, assumed technological determinism framework asserting that a technology will develop and proliferate as long as there are enough perceived benefits and uses of the technology (Pinch and Bijker, 1984; Sovacool, 2006). However, it is worth noting that in the case of armed drone swarms, whether or not social pressure is influential is most likely dependent not only on the presence of a robust dialogue on concerns in the civilian sphere, but also on this dialogue of concerns being at least partly understood and acknowledged by the military community.

As the prior threat analysis indicated, there would likely be significant social investment and concern during the initial implementation of armed drone swarms as autonomy presents a paradigmatic shift in multiple facets of the current security framework. A key driver of this social resistance is the increased autonomy, and decreased human accountability, which becomes especially startling in tactical/combat uses of drone swarms, as it could lead to autonomous machines making life or death decisions, more frequently referred to as lethal autonomous weapon systems (LAWS). For this reason, autonomous robots, be they swarms or single drones, are receiving a lot of criticism for the magnitude of change they would introduce into military activities. This has also led many scholars to investigate the different levels of interaction that human controllers could have with the swarms in order to assure a certain level of meaningful human control and to identify where along that spectrum are thresholds to legal and ethical strategic operation (Kolling et. al., 2015; Hussein, 2018). Beyond the legal and ethical considerations, which have already gained traction in the civilian and academic spheres, the social impact of decreased human interaction and decision-making in the military sphere is especially apparent using Eliot Cohen's parameters for whether a technology signifies a military revolution: "Will it change the appearance of combat?" and "Will it change the structure of armies?" (Cohen, 1996). If these two questions are taken as being indicators of technologies that produce military revolutions, then Scharre's analysis of swarm impact on military organization positively indicates that swarms constitute a military revolution. Scharre writes, "scaling multi-vehicle control up to large swarms will require even more fundamental shifts in the command-and-control paradigm," (Scharre, 2014). Thus, social barriers to swarm adoption, and the underlying consent to largely autonomous systems, have significant foundations both in the military and civilian dialogues.

Furthermore, current literature focused on the evolution of drone swarms and how future systems should be designed for the most ideal prototypes suggests that the social construction of technology will be especially relevant to the development of drone swarms themselves. One scholar, Kathleen Giles, has argued at multiple forums (NATO and the Naval Postgraduate School) that drone swarms are most efficiently and effectively developed when their design and construction is centered around a mission objective (a top-down approach) (Giles, 2016). This contrasts earlier assumptions that currently available technologies and subcomponents of drone swarms, for example individual drone types, can be fused together by altering the management system (a bottom-up approach), and thus the belief that pre-existing swarm components can be refabricated to fit a new purpose (Giles and Giammarco, 2017). Specifically, Giles argues that "to produce mission-effective systems, system architects must consider the doctrine, design, and planned assessment methodologies when developing a swarm UAS," (Giles, 2016). Giles' argument is rooted in her assessment that systems engineering is one of the most prohibitive steps of drone swarm application. Even if a group of scientists are presented with all of the proper components for a type of swarm, it would take a high-level system engineering team *with a mission in mind* to actually develop an efficient and effective swarm system (Giles, 2016). Thus, because a high-level plan based off of a desired end product is required for the development of each lower-level technology in a swarm, the technology determinism argument that technologies will be developed irrespective of social conditions deterring certain types of end products is even less likely to be relevant in the case of drone swarms. This could change as stronger software capabilities evolve and are able to be adapted more seamlessly to variable hardware components, but a requisite amount of development and testing would still have to occur before the social construction of technology framework, as presented here, becomes irrelevant.

These two points taken together make the argument that because drone swarms will not evolve easily and will need to be purposefully developed with specific functions in mind, and given that there are social reasons for both the civilian and military personnel to give pause before blindly pursuing such developments, adequate social pressure could shape the development trajectory of drone swarms . However, this social pressure, and thus the limitation it would create in the furthering of drone swarm technology development, will only gain traction if it receives adequate attention at the policymaker, military, and public levels. This is especially important given the fact that social concerns specific to the public may seem to be at odds with the perceived needs of the military. However, even absent the acceptance of civilian concerns in military developments, consideration of the strategic threats identified earlier in this article and Cohen's military revolution argument indicate that there are significant military-based social hurdles as well.

4.2. SYSTEMS ENGINEERING AS TACIT KNOWLEDGE

Beyond affording greater weight to the social construction of technology framework for drone swarm development, the heavy systems engineering requirement for swarms also acts as a technical tacit knowledge barrier. Based on Giles' assessment that the overarching plan for the swarm construction is the primary indicator of an efficient and effective swarm, a significant amount of systems engineering expertise will be required in order to incorporate the multiple types of drones and drone technologies into one cohesive swarm. Furthermore, the work capacity of each trained systems engineer, and the applicability of each technology produced, is limited based on Giles' argument that swarm technologies are not easily transferrable, at least for tactical swarms (Giles, 2016). In other words, having enough systems engineering capability to produce one type of swarm does not guarantee a wide variety of transferrable uses; each swarm and application will require a significant amount of systems engineering (with the caveat that some swarms may have more intensive or more facile evolutionary steps depending on function, realm of use, and prior drone swarm technologies they are innovated from). This will force swarm developers under constrained resources to have to prioritize what types of swarms they deem most necessary. This type of filter for proliferation, and the ability to address it, has been referred to under the context of intangible technology control, which takes into account the difference between controlling the flow of specific technologies compared to controlling the flow of knowledge and skill (Stewart, 2016). Although information knowledge might be able to flow relatively easier than physical materials, because swarm technology software will be so characteristic of the specific hardware, simple software transfers or espionage recovery will not easily or quickly be able to be applied to the technologies on hand. Additionally, the utility of such information transfers could be made more difficult by including software features making the swarm system highly dependent on hardware components that are extremely difficult to access or that require intensive user knowledge.

5. POLICY IMPLICATIONS

As was promised at the outset of this paper, it is through affording greater consideration to the social and technical barriers identified for swarm development that more targeted policy approaches can be identified to mitigate the highest priority risks introduced by drone swarms. Based on the assessment of social barriers presented in this analysis, social pressures may play an appreciable role in preventing the proliferation of swarms, and heightened focus should be given to swarm types that are deemed to be particularly disruptive. Furthermore, based on the technical barrier of the intensive systems engineering requirement and the limitation on the transferability of one swarm's technologies to another, the sheer rate of proliferation across different applications is unlikely to occur as rapidly as the current body of literature would suggest. Thus, efforts focused on restricting specific types of applications in the civilian sphere may be more useful than previously assumed, such as those that are more directly transferrable and easier to adapt to military purposes. Because Giles' argument makes a strong case for social factors having a large influence on swarm implementation, and thus bolsters the strength of the social construction of technology theory, the international community should establish norms and treaties early on that restrict the swarm behaviors that pose significant threats. Early establishment of such norms and treaties could ensure that the technologies for restricted types of swarms are not developed before the treaties and norms can be established. However, in order to ensure that such dialogue and recommendations gain traction beyond the policymaker and academic fields (and expand into the military fields), arguments need to emphasize the impact that drone swarms will have on the military community as well.

Additionally, even though swarms are considered dual-use, because they must be repurposed for each individual use, development in the civilian sphere by private companies for civilian purposes does not necessarily translate to a rapid proliferation of swarms in the military domain. This is substantiated by Verbruggen's research on LAWS and the impact of civilian innovation on military development. Specifically, Verbruggen identifies the obstacles blocking easy flow of innovation from the civilian sphere to the military sphere, including the degree of modification required for military purposes (which in the case of armed drones would be significant), and the cost for modification (Verbruggen, 2019). However, it is worth noting that the swarms relevant to Giles' and Verbruggen's arguments are predominately heterogenous swarms, or more complex swarm systems, thus it would be worth identifying the different risk pathways posed by heterogenous swarm systems with variable individual drone components and more basic homogenous swarm systems with each drone component operating similarly, the latter of which may be less restrained by social barriers. Because use of homogenous swarm systems composed of drones with simple military modifications is most likely, scholarship should focus on identifying likely swarms to be developed with these characteristics and the impact of these specific swarm types.

Based on the threats identified and the assumption of a slower rate of proliferation than previously anticipated, at least for complex, heterogenous swarm systems, the areas for arms control agreements should be ranked based on disruption level in order to establish what types of limitations must be prioritized. Since there is significant evidence that swarms could decrease the strategic stability of other technology systems, arms control agreement negotiations should begin with restricting swarm use near nuclear weapon or missile defense facilities. This may ultimately lead to the conclusion that swarms must be banned entirely, if effective verification and regulation mechanisms are not found to limit them from accessing specific areas. Also of immediate importance is the determination of areas or systems that could be impacted by low-complexity swarms, as those are the swarms that will likely proliferate more rapidly and broadly; this would include systems where swarms could be applied in sheer magnitude without necessarily having complex functions for individual drones in the swarm (for example, overwhelming a missile defense system).

Additionally, since there is significant societal concern regarding the implementation of autonomous systems, technical and policy experts must continue discussions to determine acceptable levels of autonomy, and potential metrics to monitor and verify such levels. Early agreements could focus on limiting specific types of hardware or software technologies that give rise to autonomy, or conversely the types of technologies and behaviors that autonomy is allowed to be applied to (such as activation of weapons). Beyond diplomatic efforts, the international community must also continue to engage the broader public to ensure that a significant social pressure would be perceived by militaries that consider adopting swarm technologies.

Finally, to address the threat of flash wars or unintended escalation, communication channels and response plans should be established to determine courses of action once a swarm has been hijacked or is experiencing a technical malfunction. Such communication and response postures could be established through war-game scenarios or through coalition-building. Immediate transparency would have to be prioritized, especially in an instance of severe crisis between two major powers. Additionally, during routine dialogues, countries could set norms on what types of responses would be acceptable in instances of escalation that may be the result of an accident or hijacking, and which types would be disproportionate or asymmetrical. This is especially likely given the high possibility for error in complex swarm operations, especially if a country or proliferator fails to adequately verify the efficacy of the swarm or perceives little benefit in undergoing verification.

With respect to horizontal proliferation, as Giles argues that systems engineering is a foundational technique required for drone swarms, and as systems engineering has historically been treated as a tacit knowledge in military technology development (Gormley, 2008), there are still certain avenues to bolster technical barriers. However, as was shown in the previous section, the macro-level component of systems engineering, including the intent of the engineers and architects, is probably easier to address with arms controls and treaties than the micro-level component of the engineer themselves. In other words, it is easier to eliminate an objective through restricting use than through restricting certain types of technical expertise altogether, especially when the systems produced are dual-use and have arguably good applications (Stewart, 2016). Treaties and arms control agreements targeting the system-design stage would most likely resemble norm-setting on acceptable use or could take the form of a monitoring regime to more strictly compel cooperative behavior. This has more-or-less been the approach towards anti-satellite technologies in space, and also is tangentially reminiscent of policies that guide countries towards specific types of nuclear reactors. That said, certainly access to high-trained systems engineers could be a prohibitive barrier for low-technology countries and non-state actors in acquiring drone swarms. Thus, such consideration can help address and correct the fear that any nation with access to drone technologies will be able to develop drone swarms. This barrier could conceivably be bolstered by widely-administered anti-swarm technologies (with the obvious omission of swarm technologies themselves being used as anti-swarm technologies), which would at least increase the complexity in developing a survivable and usable swarm and thus raise the requirement for systems engineering capability. Another option to bolster this barrier is to minimize the potential gain from intelligence gathering by making all relevant information on armed drone swarm technologies highly specific to unique hardware components. By inserting these software-to-hardware dependencies, the acquisition of either software-based intelligence would not necessarily allow for easy swarm development if the highly specific hardware components are unknown or not accessible. Again, consideration should be given to the most prioritized areas, which have the highest risk of impact if affected, in which to apply anti-swarm technologies, if such technologies are developed, or intelligence acquisition blocks.

6. CONCLUSION

This paper has shown that swarm implementation is different from drone implementation in the military domain, and thus poses new threats. At their technical roots, swarms ultimately require some degree of autonomy to operate. The debate over autonomy in drones has led to consideration, if not constraint, over the allowed level of autonomy for UAVs, UUVs, and UGVs, however, this would not be possible in the case of swarms. Additionally, swarms pose threats to the strategic stability of established technology systems, introduce concerns regarding horizontal proliferation, and threaten the possibility of unintended escalation or flash wars/attacks.

However, appreciation for the difference between swarms and drones can also serve to provide greater nuance on the predicted proliferation potency of swarms. Despite proclamations that swarms will be “unavoidable” and “pervasive,” based on parallels drawn to drone proliferation, social and technical barriers challenge the likelihood of a rapid proliferation. While the benefits that swarms could offer both the military and civilian sphere do make it likely that swarms will be implemented at some point, the socio-technical issues identified in this analysis suggest the applications will be narrower and more limited than what is believed. Under this new restrained view of swarm proliferation, more targeted policy actions have been identified. Policymakers should rank the highest priority threats of swarms and target actions to mitigate high-priority risks. Particular emphasis should be given to defending, either through regulation or technical defense mechanisms, areas in which swarm use would result in decreased strategic stability. Additionally, protocol should be set up for response to swarm incidents, as such incidents could be accidental, and escalation should be avoided at all costs. Finally, bolstering technical barriers could help to ensure that non-state actors and terrorist groups are unable to acquire swarms.

REFERENCES

Acton, James. (2018). “Inadvertent Escalation and the Entanglement of Nuclear Command-and-Control Capabilities.” Belfer Center – Policy Brief. Retrieved from https://www.belfercenter.org/publication/inadvertent-escalation-and-entanglement-nuclear-command-and-control-capabilities.

Altmann, Jürgen. (2005). “Nanotechnology and preventive arms control.” Forschung DSF No. 3, Osnabrück: Deutsche Stiftung Friedensforschung, 2005. Retrieved from https://bundesstiftung-friedenforschung.de/wp-content/uploads/2017/08/berichtaltmann.pdf.

Altmann, Jürgen. (2013). “Arms control for armed uninhabited vehicles: an ethical issue.” *Ethics and Information Technology*, vol. 15, 137-152. Retrieved from https://link.springer.com/content/pdf/10.1007%2Fs10676-013-9314-5.pdf.

Altmann, Jürgen & Sauer, Frank. (2017). “Autonomous Weapon Systems and Strategic Stability.” *Survival: Global Politics and Strategy*, vol. 59, no. 5, 117-142. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/00396338.2017.1375263?needAccess=true.

Arquilla, John & Ronfeldt, David. (2000). *Swarming and the Future of Conflict*. RAND CORP. Santa Monica, CA. Retrieved from https://www.rand.org/pubs/documented_briefings/DB311.html.

Asaro, Peter. (2012). “On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making.” *International Review of the Red Cross*, vol. 94, no. 886, 687-709. Retrieved from http://e-brief.icrc.org/wp-content/uploads/2016/09/22.-On-banning-autonomous-weapon-systems.pdf.

Bidwell, Christopher & MacDonald, Bruce. (2018). “Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security.” Federation of American Scientists. Retrieved from https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf.

Buchanan, Allen & Keohane, Robert. (2015). “Toward a Drone Accountability Regime.” *Ethics and International Affairs,* vol. 29, no. 1, 15-37. Retrieved from https://www.cambridge.org/core/journals/ethics-and-international-affairs/article/toward-a-drone-accountability-regime/81BCAB304843656FC28810A29ACB4886.

Chandhar, Prabhu, Danev, D. & Larsson, E. (2016). “Massive MIMO as enabler for communications with drone swarms.” *Institute of Electrical and Electronics Engineers*, 347-354. Retrieved from https://ieeexplore.ieee.org/abstract/document/7502655.

Cohen, Eliot. (1996). “A Revolution in Warfare.” *Foreign Affairs,* vol. 75, no. 2, 37-54. Retrieved from http://www.comw.org/rma/fulltext/9603cohen.pdf.

Ewers, Elisa, Fish, Lauren, Horowitz, Michael, Sander, Alexander, and Scharre, Paul. (2017). “Drone Proliferation: Policy Choices for the Trump Administration.” Center for New American Security – Papers for the President. Retrieved from http://drones.cnas.org/wp-content/uploads/2017/06/CNASReport-DroneProliferation-Final.pdf.

Ford, Celeste. (2017). “Eight Grants to Address Emerging Threats in Nuclear Security.” Carnegie Corporation of New York, International Peace and Security Program – Press Release. September 25, 2017. Retrieved from https://www.carnegie.org/news/articles/eight-grants-address-emerging-threats-nuclear-security/.

Frantzman, Seth. (2019). “Are air defense systems ready to confront drone swarms?” *Defense News*, September 26, 2019. Retrieved from https://www.defensenews.com/global/mideast-africa/2019/09/26/are-air-defense-systems-ready-to-confront-drone-swarms/.

Giles, Kathleen. (2016). “A Framework for Integrating the Development of Swarm Unmanned Aerial System Doctrine and Design.” NATO Science and Technology Office Public Release, 1-14. Retrieved from https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SET-222/MP-SET-222-14.pdf.

Giles, Kathleen & Giammarco, K. (2017). “Mission-based Architecture for Swarm Composability.” *Complex Adaptive Systems Conference: Engineering Cyber Physical Systems,* vol. 114, 57-64. Retrieved from https://www.sciencedirect.com/science/article/pii/S1877050917317994.

Gormley, Dennis. (2008). *Missile contagion: cruise missile proliferation and the threat to international security*. Praeger Security International.

Hambling, David. (2015). *Swarm Troopers: How Small Drones Will Conquer the World*. Archangel Ink.

Hambling, David. (2017). “The next era of drones will be defined by ‘swarms’.” *BBC.* April 27, 2017. Retrieved from http://www.bbc.com/future/story/20170425-were-entering-the-next-era-of-drones.

Hambling, David. (2018). “Change in the air: Disruptive Developments in Armed UAV Technology.” United Nations Institute for Disarmament Research. Retrieved from http://www.unidir.org/files/publications/pdfs/-en-726.pdf.

Homayounnejad, Maziar. (2018). “Autonomous Weapon Systems, Drone Swarming and the Explosive Remnants of War.” Kings College London – Dickson Poon Translational Law Institute Research Paper Series. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099768.

Hurst, Jules. (2017). “Robotic Swarms in Offensive Maneuver.” *Joint Forces Quarterly*, vol. 87. Retrieved from https://ndupress.ndu.edu/Publications/Article/1326017/robotic-swarms-in-offensive-maneuver/.

Hurst, Jules. (2019). “Small Unmanned Aerial Systems and Tactical Air Control.” *Air & Space Power Journal*. Retrieved from https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-33_Issue-1/F-Hurst.pdf.

Hussein, Aya, & Abbas, Hussein. (2018). “Mixed Initiative Systems for Human-Swarm Interaction: Opportunities and Challenges.” 2nd Annual Systems Modelling Conference. October 2018. Retrieved from https://arxiv.org/pdf/1808.06211.pdf.

Kallenborn, Zachary & Bleek, Philipp. (2019). “Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons,” *War on the Rocks*, February 14, 2019. Retrieved from https://warontherocks.com/2019/02/drones-of-mass-destruction-drone-swarms-and-the-future-of-nuclear-chemical-and-biological-weapons/.

Kallenborn, Zachary and Bleek, Philipp. (2018) “Swarming destruction: drone swarms and chemical, biological, radiological, and nuclear weapons.” *The Nonproliferation Review,* vol. 25, no. 5-6, 523-543. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/10736700.2018.1546902?af=R&journalCode=rnpr20.

Kania, Elsa. (2019). “Chinese Military Innovation in Artificial Intelligence.” Testimony before the U.S.-China Economic and Security Review Commission Hearing on Trade, Technology, and Military-Civil Fusion. June 7, 2019. Retrieved from https://www.uscc.gov/sites/default/files/transcripts/June%207%2C%202019%20Hearing%20Transcript.pdf.

Knight, Will. (2017). “Forget Killer Robots – Bias is the Real AI Danger.” *MIT Technology Review*, October 3, 2017. Retrieved from https://www.technologyreview.com/s/608986/forget-killer-robotsbias-is-the-real-ai-danger/.

Kolling, A., Walker, P., Chakraborty, N., et al. (2015). "Human Interaction with Swarms: A Survey." *IEEE Transactions on Human-Machine Systems*. Retrieved from https://core.ac.uk/download/pdf/42611179.pdf.

Lachow, Irving. (2017). "The upside and downside of swarming drones." *The Bulletin of the Atomic Scientists* vol. 73, no. 32, 96-101. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/00963402.2017.1290879?needAccess=true.

Madrigal, Alexis. (2018). "Drone Swarms Are Going to Be Terrifying and Hard to Stop." *The Atlantic*, March 7, 2018. Retrieved from https://www.theatlantic.com/technology/archive/2018/03/drone-swarms-are-going-to-be-terrifying/555005/.

Ouagrham-Gormley, Sonia Ben. (2012). "Barriers to Bioweapons: Intangible Obstacles to Proliferation." *International Security*, vol. 36, no. 4, 80-114. Retrieved from https://muse.jhu.edu/article/470588/pdf.

Pinch, Trevor & Bijker, Wiebe. (1984). "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other." *Social Studies of Science*, vol. 14, no. 3, 399-441. Retrieved from https://www.jstor.org/stable/pdf/285355.pdf?casa_token=QVs1oT0J0SoAAAAA:9je2LTZ33kxz-qqF4gQrJGyHP17ibpp_4M3mJy9zMkYqjOI1CIl_74sIcddr8fbhnLz5avoR3BjKL1v-awb5PjfPeKNF2U79us_PYCeh7x6qV5ekC388.

Romaniuk, Scott and Burgers, Tobias. (2018). "China's Swarms of Smart Drones have Enormous Military Potential." *The Diplomat*. February 3, 2018. Retrieved from https://thediplomat.com/2018/02/chinas-swarms-of-smart-drones-have-enormous-military-potential/.

Rouff, C., Vanderbilt, A., Hinchey, M., Truszkowski, W., & Rash, J. (2004). Verification of emergent behaviors in swarm-based systems. *Proceedings. 11th IEEE International Conference and Workshop on the Engineering of Computer-Based Systems*. 2004. Retrieved from https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20040081039.pdf.

Sauer, Frank and Schornig, N. (2012). "Killer drones: The 'silver bullet' of democratic warfare?" *Security Dialogu*e vol. 43, no. 4, 363-380. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/0967010612450207?casa_token=ITxJ29Akjp-cAAAAA:0d7tM2_dNm4ta244mivaiSURLP0hTH7WNOWTeSLxsfF-PbgfJAZOnVrsoovoNrsX55mIzEpxQYCEn.

Scharre, Paul. (2014). "Robotics on the Battlefield Part II: The Coming Swarm." Center for New American Security. Retrieved from https://www.cnas.org/publications/reports/robotics-on-the-battlefield-part-ii-the-coming-swarm.

Scharre, Paul. (2015). "Counter-Swarm: A Guide to Defeating Robotic Swarms." *War on the Rocks*. March 31, 2015. Retrieved from https://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-swarms/.

Scharre, Paul. (2015). "Unleash the Swarm: The Future of Warfare." *War on the Rocks*. March 4, 2015. Retrieved from https://warontherocks.com/2015/03/unleash-the-swarm-the-future-of-warfare/.

Scharre, Paul. (2018). *Army of None: Autonomous Weapons and the Future of War*. W.W. Norton & Company.

Sharkey, Noel. (2012). "The evitability of autonomous robot warfare." *International Review of the Red Cross*, Vol. 94, No. 886, 787-799. Retrieved from http://e-brief.icrc.org/wp-content/uploads/2016/09/23.-The-evitability-of-autonomous-robot-warfare.pdf.

Shmuel, Shmuel. (2018). “The Coming Swarm Might be Dead on Arrival.” *War on the Rocks*, September 10, 2018. Retrieved from https://warontherocks.com/2018/09/the-coming-swarm-might-be-dead-on-arrival/.

Sparrow, Robert. (2007). “Killer Robots.” *Journal of Applied Philosophy*. Vol. 24, No. 1, 62-77. Retrieved from https://wmpeople.wm.edu/asset/index/cvance/sparrow.

Singer, Peter. (2009). “Military Robots and the Laws of War.” *Brookings Institute*. Retrieved from https://www.brookings.edu/articles/military-robots-and-the-laws-of-war/.

Sovacool, Benjamin. (2006). “Reactors, Weapons, X-Rays, and Solar Panels: Using SCOT, Technological Frame, Epistemic Culture, and Actor Network Theory to Investigate Technology.” *The Journal of Technology Studies*. Retrieved from https://pdfs.semanticscholar.org/3cf5/f8428e11f4d32fa4d445611f2e5230d2e365.pdf.

Springer, Paul. (2013). *Military Robots and Drones*. Santa Barbara, CA: ABC-CLIO.

Stewart, Ian. (2016). “Examining Intangible Controls.” A report prepared by Project Alpha at King’s College London. 2016. Retrieved from https://www.kcl.ac.uk/alpha/assets/examining-itt-part-1.pdf.

Tonnessen, Truls. (2017). “Islamic State and Technology – A Literature Review.” *Perspectives on Terrorism* 11, no. 6. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/659/html.

Tucker, Patrick. (2017). “Counter-Terror Chief: Expect Terrorist Drone Swarms ‘Soon’.” *Defense One*. February 27, 2017. Retrieved from https://www.defenseone.com/technology/2017/02/counter-terror-chief-expect-terrorist-drone-swarms-soon/135736/.

Tucker, Patrick. (2018). “Pentagon Wants More Money for Lasers to Defend Against Missiles, Drone Swarms,” *Defense One*. November 13, 2018. Retrieved from https://www.defenseone.com/technology/2018/11/pentagon-wants-more-money-lasers-defend-against-missiles-drone-swarms/152796/.

UK MoD. “£2.5m injection for drone swarms.” (2019). United Kingdom Ministry of Defence – Press Release. March 28, 2019. Retrieved from https://www.gov.uk/government/news/25m-injection-for-drone-swarms.

US DoD. “Department of Defense Announces Successful Micro-Drone Demonstration.” (2017). United States Department of Defense – Press Release. January 9, 2017. Retrieved from https://www.defense.gov/Newsroom/Releases/Release/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/.

Vanderbilt, C., Hinchey, M., & Truszkowski, W. (2004). “Verification of Emergent Behaviors in Swarm-based Systems.” *Institute of Electrical and Electronics Engineers* – Conference Proceedings. Retrieved from https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20040081039.pdf.

Verbruggen, Maaike. (2019). “The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems.” *Global Policy*, vol. 10, no. 3. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12663.

Wesson, Kyle and Todd Humphreys. (2013). “Hacking Drones.” *Scientific American* 309 no. 5.

Williams, Sean. (2018). “Swarm Weapons: Demonstrating a Swarm Intelligent Algorithm for Parallel Attack.” *School of Advanced Military Studies* – Graduate Dissertation.

Wilson, Richard. (2014). “Ethical Issues with Use of Drone Aircraft.” *Institute of Electrical and Electronics Engineers*, vol. 978, no. 1. Retrieved from https://csiflabs.cs.ucdavis.edu/~ssdavis/188/Ethical%20Issues%20with%20use%20of%20Drone%20Aircraft.pdf.

Woodhams, George. (2018). “Weapon of choice? The expanding development, transfer, and use of armed UAVs.” United Nations Institute for Disarmament Research. Retrieved from http://www.unidir.org/files/publications/pdfs/weapons-of-choice-the-expanding-development-transfer-and-use-of-armed-uavs-en-723.pdf.

Zhao, Tong. (2018). “Tides of Change: China’s Nuclear Ballistic Missile Submarines and Strategic Stability.” *Carnegie Institute- Tsinghua Center for Global Policy*. Retrieved from https://carnegietsinghua.org/2018/10/24/addressing-future-challenges-pub-77498.

A Developing Arms Race in Outer Space? Deconstructing the Dynamics in the Field of Anti-Satellite Weapons

ARNE SÖNNICHSEN

UNIVERSITY OF DUISBURG-ESSEN

DANIEL LAMBACH

GOETHE UNIVERSITY FRANKFURT & UNIVERSITY OF DUISBURG-ESSEN

[#36-PAPER]

ABSTRACT

Private actors dream of the commercialization of space, scientists dream about discoveries on the Moon, Mars, and in deep space, while security experts worry about space as a theatre of war. Fears about the militarization of space often make techno-determinist and techno-essentialist arguments. According to these narratives, technology drives politics and technological artefacts have inherent and unchangeable characteristics. For example, the recent development of Anti-Satellite (ASAT) capabilities among space powers like China and India is often described as an example of an increasingly febrile security competition. This paper takes a Social Construction of Technology (SCOT) approach to arms races in outer space. Using a case study of Mission Shakti, India's first successful ASAT test in 2019, we find that while Indian officials made some security-related claims about their ASAT project, they were just as likely, if not more, to advance status-seeking arguments. This offers possibilities for de-securitizing outer space.

1. INTRODUCTION

Recent years have witnessed a boom in human activity in space and a surge of development of space-related technologies, with commentators warning of a 'new space race' (Pekkanen, 2019). But this rhetoric is overblown. The structural preconditions are very different from that of the first space race, in which the US and the USSR directed huge resources towards science and research in order to outdo the other in a mostly ungoverned space. However, that does not preclude the possibility of *arms races* in or relating to outer space. As human activity in space grows, so does the need for governance and conflict management. Unfortunately, 'hard security' issues are mostly absent from multilateral deliberations on outer space, leaving each state to forge its own policy with little coordination and trust-building among rivals. As a result, the present system of Outer Space Governance is not suited to preventing or containing arms races. This is all the more problematic since space powers have pushed a securitized view of space (Peoples, 2010, 2011), and increases in national space capabilities are further exacerbating tensions (Handberg, 2018).

We focus on the example of Anti-Satellite Weapons (ASAT) where there are widespread worries of a developing arms race. These development are undoubtedly posing risks for relations among space powers but they are also based on what Bourdieu calls a 'doxa', something that is self-evident and taken for granted within a community (Bourdieu, 1977, 164-169), and on an essentializing view of technology as being imbued with certain inherent characteristics. In contrast, we argue, in line with most of Science & Technology Studies, that the development, purpose and effects of technology are socially situated. Our aim is therefore to deconstruct the assumptions behind current discussions about coming arms races in outer space. This is not to deny the likely risks of escalation or the existence of security dilemmas in this field, but rather to probe how such dynamics emerge in socio-technical assemblages of national security. Focusing on the highly dynamic field of ASAT, we use the recent example of 'Mission Shakti', India's first successful test of a kinetic ASAT system, as a case study of how states develop weapons systems not just for reasons of security but also for status-seeking and domestic politics.

2. Arms Races and Arms Control in Outer Space

There are renewed discussions about war *in* space, not just *involving* space. Recent moves by the United States government to establish a 'Space Force' have to be read as an attempt to collect existing capabilities for military action in space within a new contingent of the US armed forces (Hunter & Bowen, 2018). Russia and China also have dedicated branches of the armed forces with responsibilities for outer space. Discussions about 'spacepower' (derived from classic conceptions of 'seapower') have been going on for some time (Bowen, 2019) as are notions that space assets need to be protected from aggression (Wolter, 2006). In spite of these antecedents, recent moves seem to signal shifts in discourse and perception that are more open to the possibility of warfare in space than seemed previously likely (Pavelec, 2012). However, it is not clear whether the buildup of military assets is driven by genuine security concerns or whether it should be interpreted as more of a symbolic move underpinning a nation's claims for great power status. The famed 'nuclear club' is now complemented by the 'space club' (Paikowsky, 2017) – a trend that is relevant not just for First World states (Harding, 2013).

ASAT technology has been envisioned since the early days of spaceflight (Bulkeley & Spinardi, 1986). The earliest systems were developed by the US and the USSR with the first successful Soviet test in 1970. ASAT capabilities have since been developed by other space powers (for a comprehensive overview, see Weeden & Samson, 2018). In January 2007, China successfully shot down a defunct weather satellite. This set off a series of tests by other nations including the United States and Russia. Most recently, in March 2019, India has conducted a successful test of its ASAT system ('Mission Shakti'), using a ground-launched interceptor missile.

Other nations such as Iran, Pakistan, and North Korea are not known to possess ASAT capability, although Weeden and Samson note that such capabilities could theoretically be developed out of existing ballistic missile programs (Weeden & Samson, 2018). It is, therefore, appropriate to speak of an ASAT arms race, although this is entangled with wider dynamics in the field of ballistic missiles.

3. MISSION SHAKTI

The literature on arms races and the security dilemma argues that such processes are driven by a mixture of security concerns and uncertainty about other states' intentions (Khan & Khan, 2019; Tang, 2009). However, an analysis of the ASAT arms race shows that states are not only motivated by security fears. Relevant social groups also attach other meanings to ASAT, specifically its symbolic value (in line with the argument by Musgrave & Nexon, 2018). This becomes evident in the recent example of 'Mission Shakti', the first successful test of an Indian ASAT missile. On 27 March 2019, a ground-launched interceptor missile destroyed the Indian earth observation satellite Microsat-R via kinetic impact at an altitude of 283 km in Low Earth Orbit. The ASAT system was spun off from India's ABM program and was developed by the Defence Research and Development Organisation (DRDO), a research branch of the armed forces. There are indications that the program received strong support from the Indian government and might have even been fast-tracked (also Lele, 2019b, 12-13; see the relatively pessimistic assessment of Indian ASAT capabilities in Weeden & Samson, 2018).

Entering into the ASAT arms race fulfils three distinct objectives for the Indian government. First, in line with a security dilemma explanation, there are indications that India was genuinely worried about its strategic disadvantage vis-à-vis China (Lele, 2019b; Tellis, 2019). India and China have a history of conflict and Indian space assets were vulnerable to Chinese ASAT after the latter's 2007 test. Hence, one of Mission Shakti's aims was to 'establish credible space deterrence against China' (Davis, 2019). The BJP, the governing party of Prime Minister Narendra Modi, tweeted 'India now has the capability to shoot down any satellite that may pose a threat to its security in lower orbit' (@BJP4India, 27 March 2019). In contrast, Pakistan, India's chief regional rival, did not seem to feature much in the decision due to its lack of comparable space capabilities, although Pakistani analysts see the test as a move to entrench Indian technological superiority in space (Khan & Khan, 2019). But public reactions by other states were calm. Pakistan and China, the two countries most likely to feel threatened, only warn against the militarization of space and risks of escalation in abstract terms, along with Russia. Criticisms focused mainly on the creation of space debris. NASA Chief Administrator Jim Bridenstine said that creating debris was a 'terrible, terrible thing [and] not compatible with the future of human spaceflight' (Foust, 2019). If there is an ASAT arms race, it is a relatively relaxed one so far.

Second, ASAT is also, maybe even predominantly, about enhancing India's status as a global power. The grand strategy of the Hindu nationalist government is 'driven by the pursuit of national strength and international prestige […] to restore India's civilizational glory and rightfully secure the country a more prominent place in the international system' (Rej & Sagar, 2019, 73), and ASAT is portrayed as symbolic capital in evidence of that fact. It is repeatedly stressed that India is only the fourth country to acquire ASAT capabilities. PM Modi himself claimed that the successful test was proof that India has now 'entered the elite club of space power' (@narendramodi_in, 31 March 2019). Government representatives point out that the effort was completely indigenous and developed solely by Indian scientists, thereby underscoring further the nationalist narrative (@narendramodi 27 March 2019). In addition, India is keen to portray itself as a responsible power, highlighting the very low altitude of the target and the head-on approach of the interceptor missile. The official line was that all debris fragments would decay and burn up in the atmosphere within, at most, 45 days. However, independent analysts conclude that the impact was not exactly head-on, launching some fragments into much higher altitudes, some even above the orbital band of the International Space Station (~410 km) (Akhmetov, Savanevych, & Dikov, 2019; Langbroek, 2019). Bridenstine's comments also point towards an emerging norm against 'unsafe' ASAT tests. Some commentators think that the relatively rapid development of the ASAT system was at least partly driven by a wish to establish ASAT capability before such tests are regulated or even banned (Porras, 2019; Davis, 2019).

Third, the ASAT test also had a domestic politics angle. Some opposition parties frame the mission as a political stunt ahead of the national elections in April 2019. An opposition newspaper criticized Modi for claiming credit for a technology developed by DRDO scientists, whose budget he had previously cut, in a program that was started by his predecessor Manmohan Singh in 2012 (National Herald, 2019). In response, the BJP accused the previous government of dragging its feet on several weapons programs, including the ASAT system, while it was in office (@BJP4India, 27 March 2019). The government also uses the political capital generated by the test to push for institutional reforms in the military, such as the creation of a Defence Space Agency (DSA) to command all space assets formerly attached to India's army, navy and air force, as well as the development of a space doctrine to govern the use of its newly developed assets (Gupta, 2019; Lele, 2019a).

In conclusion, while Mission Shakti might look like another step in a typical arms race, the picture seems to be more complex than that. The security angle is only one in a complex and entangled set of aims and aspirations by key actors in India. The government is also keen to present itself as a modern, responsible member of the space club – a step foreshadowed for quite some time (Aliberti, 2018). The ASAT test, the DSA, and the space doctrine represent a continuation of this strategy.

4. Conclusion

On the face of it, there is great potential for arms races in outer space. Outer space activity has always had military connotations and states continue to treat outer space as a military domain. Control in/over outer space is also becoming more valuable as its commercial value grows (although a weaponization of space might inhibit that same commercial use). International regulation is thin and 'traditional' arms control approaches are hindered by disagreements over what even constitutes a 'weapon' in the outer space context. Moreover, countries are developing non-kinetic counterspace and ASAT capabilities that represent the next stage of technological evolution (Tellis, 2019). All of these factors should give us cause to worry.

However, as this paper has demonstrated, states do not develop space weapons only, and maybe not even mainly, to seek security in space. Generalizing from the Indian case, we conclude that status-seeking is a prominent motive in processes of outer space militarization. Weapons systems are symbolically important in that they underpin narratives of national greatness and international status. Somewhat paradoxically, this opens possibilities to lessen pressures towards the weaponization and militarization of outer space. If states attach the problem of insufficient status to their existing space technology, then there are many possible solutions beyond developing further weapons capabilities. Instead, states may be induced to seek status through the responsible use of space, the commercial exploitation of space resources or through scientific breakthroughs. Current cooperative projects to develop lunar bases or deep space gateways can be seen as opportunities in this direction, as is the development of a normative framework surrounding ASAT testing. These are but a few examples of how outer space can be progressively de-securitized as civilian and commercial activities grow.

REFERENCES

Akhmetov, V., Savanevych, V., & Dikov, E. (2019). Analysis of the Indian ASAT test on 27 March 2019. *arXiv*.

Aliberti, M. (2018). *India in Space: Between Utility and Geopolitics*. Cham: Springer.

ANI (2019, March 28). Russia's statement on #MissionShakti: Russia, intends to continue to make necessary effort to prevent an arms race in outer space. The idea of ??developing a multilateral legally binding instrument for keeping outer space peaceful based on the Russian-Chinese draft treaty... 1/3 [Tweet]. Retrieved from https://twitter.com/ANI/status/1111492898019663872

Bijker, W. E. (1995). Sociohistorical Technology Studies. In S. Jasanoff, G. E. Markle, J. C. Petersen, & T. Pinch (Eds.), *Handbook of Science and Technology Studies* (pp. 229-256). Thousand Oaks: Sage.

BJP4India (2019, March 27a). This is how the Anti Satellite Missile works. India now has the capability to shoot down any satellite that may pose a threat to its security in lower orbit. #MissionShakti [Tweet]. Retrieved from https://twitter.com/BJP4India/status/1110861171916038149

BJP4India (2019, March 27b). Congress led UPA Surgical Strike: Don't do it Air Strike: Don't do it A-SAT Missile: Don't do it Modi Sarkar Surgical Strike: Go For It Air Strike: Go For It A-SAT Missile: Go For It Modi Hai To Mumkin Hai. #MissionShakti [Tweet]. https://twitter.com/BJP4India/status/1110886268408233984Bourdieu, P. (1977). *Outline of a Theory of Practice*. Cambridge: Cambridge University Press.

Bowen, B. E. (2019). From the sea to outer space: The command of space as the foundation of spacepower theory. *Journal of Strategic Studies, 42*(3-4), 532-556. doi:10.1080/01402390.2017.1293531

Brandau, D. (2015). Demarcations in the Void: Early Satellites and the Making of Outer Space. *Historical Social Research, 40*(1), 239–264.

Bulkeley, R., & Spinardi, G. (1986). *Space Weapons: Deterrence or Delusion?* Cambridge: Polity Press.

Chow, B. G. (2017). Stalkers in Space: Defeating the Threat. *Strategic Studies Quarterly, 11*(2), 82-116.

Chow, B. G. (2018). Space Arms Control: A Hybrid Approach. *Strategic Studies Quarterly, 12*(2), 107-132.

Commission to Assess United States National Security Space Management and Organization. (2001). *Report of the Commission to Assess United States National Security Space Management and Organization*. Retrieved from Washington D.C.: Retrieved from http://www.dod.gov/pubs/space20010111.html

Davis, M. (2019, 29 March 2019). Will India's anti-satellite weapon test spark an arms race in space? Retrieved from https://www.aspistrategist.org.au/will-indias-anti-satellite-weapon-test-spark-an-arms-race-in-space/

Foust, J. (2019). NASA warns Indian anti-satellite test increased debris risk to ISS. *SpaceNews*. Retrieved from SpaceNews.com website: https://spacenews.com/nasa-warns-indian-anti-satellite-test-increased-debris-risk-to-iss/

Gupta, S. (2019). After A-SAT testing, PM Modi asks NSA Ajit Doval to prepare draft space doctrine. *Hindustan Times*. Retrieved from Hindustan Times website: https://www.hindustantimes.com/india-news/after-a-sat-testing-pm-modi-asks-doval-to-prepare-draft-space-doctrine-now/story-lHWeecJefZJHyoUmITeHBO.html

Handberg, R. (2018). War and rumours of war, do improvements in space technologies bring space conflict closer? *Defense & Security Analysis, 34*(2), 176-190. doi:10.1080/14751798.2018.1478181

Harding, R. C. (2013). *Space Policy in Developing Countries: The Search for Security and Development on the Final Frontier*. London, New York: Routledge.

Hertzfeld, H. R., Weeden, B., & Johnson, C. D. (2016). Outer Space: Ungoverned or Lacking Effective Governance? New Approaches to Managing Human Activities in Space. *SAIS Review of International Affairs, 36*(2), 15-28.

Hunter, C., & Bowen, B. (2018, 27.08.2018). Donald Trump's Space Force isn't as new or as dangerous as it seems. Retrieved from http://www.thespacereview.com/article/3559/1

Khan, Z., & Khan, A. (2019). Space Security Trilemma in South Asia. *Astropolitics, 17*(1), 4-22. doi:10.1080/14777622.2019.1578931

Klein, H. K., & Kleinman, D. L. (2002). The Social Construction of Technology: Structural Considerations. *Science, Technology, & Human Values, 27*(1), 28-52. doi:10.1177/016224390202700102

Langbroek, M. (2019). Why India's ASAT Test Was Reckless. *The Diplomat*. Retrieved from https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless/

Lele, A. (2019a). India needs its own space force. *SpaceNews*. Retrieved from SpaceNews.com website: https://spacenews.com/op-ed-india-needs-its-own-space-force/

Lele, A. (2019b). Space Security Dilemma: India and China. *Astropolitics, 17*(1), 23-37. doi:10.1080/14777622.2019.1578932

Maogoto, J. N., & Freeland, S. (2007). Space Weaponization and the United Nations Charter Regime on Force: A Thick Legal Fog or a Receding Mist? *The International Lawyer, 41*(4), 1091-1119.

Munters, W., & Wouters, J. (2017). *The Road Not Yet Taken for Defusing Conflicts in Active Debris Removal: A Multilateral Organization*. Retrieved from Leuven:

Musgrave, P., & Nexon, D. H. (2018). Defending Hierarchy from the Moon to the Indian Ocean: Symbolic Capital and Political Dominance in Early Modern China and the Cold War. *International Organization, 72*(3), 591-626. doi:10.1017/s0020818318000139 narendramodi (2019, March 27). #MissionShakti is special for 2 reasons: (1) India is only the 4th country to acquire such a specialised & modern capability. (2) Entire effort is indigenous. India stands tall as a space power! It will make India stronger, even more secure and will further peace and harmony. [Tweet]. https://twitter.com/narendramodi/status/1110801488559759360

narendramodi_in (2019, March 31). With success of #MissionShakti, our scientists have achieved a great feat. Till now only three countries had such a capability. It is due to our scientists that India has entered the elite club of space power: PM @narendramodi #MainBhiChowkidar [Tweet]. Retrieved from https://twitter.com/narendramodi_in/status/1112331783817842689

National Herald. (2019). Modi stakes claims to other's achievements again, this time of DRDO scientists. *National Herald*. Retrieved from https://www.nationalheraldindia.com/opinion/herald-view-modi-stakes-claims-to-others-achievements-again-this-time-of-drdo-scientists

Paikowsky, D. (2017). *The Power of the Space Club*. Cambridge: Cambridge University Press.

Pavelec, S. M. (2012). The Inevitability of the Weaponization of Space: Technological Constructivism Versus Determinism. *Astropolitics, 10*(1), 39-48. doi:10.1080/14777622.2012.647392

Pekkanen, S. M. (2019). Governing the New Space Race. *AJIL Unbound, 113*, 92-97. doi:10.1017/aju.2019.16

Peoples, C. (2010). The growing 'securitization' of outer space. *Space Policy, 26*(4), 205-208.

Peoples, C. (2011). The Securitization of Outer Space: Challenges for Arms Control. *Contemporary Security Policy, 32*(1), 76-98. doi:10.1080/13523260.2011.556846

Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science, 14*(3), 399-441.

Porras, D. (2019). Anti-satellite warfare and the case for an alternative draft treaty for space security. *Bulletin of the Atomic Scientists, 75*(4), 142-147. doi:10.1080/00963402.2019.1628470

Rej, A., & Sagar, R. (2019). The BJP and Indian Grand Strategy. In M. Vaishnav (Ed.), *The BJP in Power: Indian Democracy andReligious Nationalism* (pp. 73-82). Washington D.C.: Carnegie Endowment for International Peace.

Russell, S. (1986). The Social Construction of Artefacts: A Response to Pinch and Bijker. *Social Studies of Science, 16*(2), 331-346.

Tang, S. (2009). The Security Dilemma: A Conceptual Analysis. *Security Studies, 18*(3), 587-623. doi:10.1080/09636410903133050

Tellis, A. J. (2019). India's ASAT Test: An Incomplete Success. Retrieved from https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884

Weeden, B., & Samson, V. (2018). *Global Counterspace Capabilities: An Open Source Assessment*. Retrieved from Broomfield: https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf

Williams, R., & Edge, D. (1996). The social shaping of technology. *Research Policy, 25*(6), 865-899. doi:https://doi.org/10.1016/0048-7333(96)00885-2

Wolter, D. (2006). *Common Security in Outer Space and International Law*. Geneva: United Nations Institute for Disarmament Research.

Meaningful Human Control of Lethal Autonomous Weapon Systems

STEFKA SCHMID, THEA RIEBE AND CHRISTIAN REUTER

SCIENCE AND TECHNOLOGY FOR PEACE AND SECURITY (PEASEC), TECHNISCHE UNIVERSITÄT DARMSTADT

[#37-PAPER]

Abstract

In the discussion of lethal autonomous weapon systems (LAWS) in the expert forum of the Convention on Certain Conventional Weapons (CCW), the interpretation of crucial concepts such as autonomy and human control is decisive for the future direction of international humanitarian law. Starting from the perspective of a synthesis of Actor-Network Theory (ANT) and Value-Sensitive-Design (VSD), we aim to analyse the discourse of LAWS and ask for possibilities to implement *Meaningful Human Control*.

1. INTRODUCTION AND RELATED WORK ON LAWS AND MHC

The debate on the development and deployment of lethal autonomous weapon systems (LAWS)[38] is of increasing importance, with discussions stalling and technological development progressing. This investigation, therefore, sheds light on the work of the Group of Governmental Experts (GGE) of the UN Convention of Certain Conventional Weapons (CCW). The CCW, offering an arena for international cooperation, has dedicated itself to the purpose of finding a common ground with respect to an understanding of LAWS as well as the necessary degree of human control (UNIDIR, 2018). LAWS have been discussed concerning ethical impacts and International Humanitarian Law (IHL), and their impact on the arms race dynamic and the stability of international security as well as on human controlling warfare (Altmann & Sauer, 2017). From an ethical perspective, the concept of *Meaningful Human Control (MHC)* supports a human-centric approach. As autonomous technology is increasingly at the centre of contemporary military innovations, questions of (human) agency and responsibility in warfare have become even more pressing (Hellström, 2013). As stressed by the United Nations Institute for

[38] The term lethal seems to exclude weapons against material and non-lethal weapons – but military parlance can also mean disable or destroy. To include these, the term AWS (Autonomous weapon systems) is often used. However, the CCW-Debate explicitly uses the term LAWS.

Disarmament Research (UNIDIR), the concept of *MHC* may prove useful in the context of development and use of (semi-) autonomous weaponry (UNIDIR, 2014).

Scholars of various disciplines are interested in the question of LAWS and human control. Crootof (2016), focusing on the applicability of international humanitarian law and accountability, reflects on the inherent imprecision of the concept of *MHC*, while stressing the need to interpret the evolving norm as convergent with existing international law. Amoroso and Tamburrini (2019) provide requirements for *MHC* with respect to humanitarian law. While this is important, at least for international legal debates, the legal discourses lack to discuss the design of technical components. This may be due to discursive boundaries of the disciplines. Approaches like Schörnig's (2019) and Bhuta et al. (2016) paying attention to legal, technical, and ethical issues are still rare. To understand the obstacles for human control, it is important to take a closer look at computer science and engineering, especially robotics and the requirements for the lethal or destructive application. Such publications are frequently interested in the development of semi-autonomous drones (Albers et al., 2010; Chao et al., 2010; Scharre, 2018), machine learning techniques, and human-computer interaction. Often focusing on civilian environments, some scholars pay special attention to crisis situations (Adams & Friedland, 2011) or warfare technology (Hocraffer & Nam, 2017). Still, many engineering studies are interested in optimizing automatic or autonomous processes and robotics of AWS (Arkin et al., 2012; Gray et al., 2012).

In contrast, there are studies dedicated to machine ethics, such as Canellas et al. (2016) or Hägele et al. (2017), the latter focusing on risk assessment and not explicitly making use of more abstract concepts. Chmielewski (2018) tries to incorporate non-Western values and stresses the need for an ethical evaluation of the use of LAWS, referring to IEEE's "Ethical Considerations in Artificial Intelligence and Autonomous Systems" (2016). The cognitive engineering approach by Canellas et al. (2016) is one of the few works which have analyzed different understandings of *MHC* and concrete options realized in human-computer interaction. The authors highlight implications for function allocation to autonomous systems vis à vis human operators, derived from definitions of *MHC*.

In this work, we investigate the technological values incorporated into LAWS, which may be competing against each other due to different stakeholders across the CCW arena (Friedman et al., 2009). This is plausible as the various variants of LAWS may be seen as part of a discourse instead of isolated value-laden innovations. Thus, we pose the question: **"How can *MHC* of LAWS by the UN Convention on Certain Conventional Weapons be ensured, under conditions of potentially supportive or ambivalent technological values and underlying discourses?"**

We focus on the Convention on Certain Conventional Weapons (CCW) as the most relevant international body dedicated to the regulation of respective human-machine interaction and main organizational forum of the conceptual debate regarding autonomy and control with respect to lethal weaponry. To answer the question of how MHC may be achieved within this forum, a discourse analytical approach, grasping mindsets and conceptualizations is a plausible choice.

2. VALUE-SENSITIVE DESIGN

We chose to analyse *MHC* with regard to LAWS from a synthesized perspective of actor-network theory (ANT) (Law, 2008) and Value-Sensitive Design (VSD) approach (Friedman, 2009). Following ANT, as a relational, material-semiotic approach, it offers the possibility to pay special attention to interactions between humans and non-humans (Braun et al., 2018; Law, 2008). This is especially plausible when analysing human-machine interaction in the field of autonomous robots, illustrating the ontological symmetry of so-called actants as well as instances of non-human agency (Braun, 2018; Callon, 1984). Second, interested in Latour's work of deconstructing laboratories (Murdoch, 1997) and material objects (Latour, 1990), and describing how a certain innovation came to be socially dominant, we assume LAWS as a socio-technical network to undergo processes of innovation *translation* (Hanseth et al., 2004; Tatnall & Gilding, 1999). Tatnall and Gilding (1999) define ANT "or the 'sociology of translations' […] [as] concerned with […] construction and maintenance of networks made up of both human and non-human actors. […] It explores the ways […] how they compete with other networks, and how they are made durable over time". Shedding light on LAWS' inscribed attributes, we follow the VSD approach by Friedman et al. (2009), acknowledging its merit of shifting analysis from longer time spans of processes of *enrolment*, actor coalitions, origins of *assemblages* (Callon, 1984; Law, 2008; Lee et al., 2014) to already materialized values and their relationships among each other. VSD yields theoretical and methodological implications by assuming more or less abstract values to be reflected in interfaces or software and thus indicate the need for interpretative work (Friedman & Nissenbaum, 1996). Following this approach, we consider the design process to be especially relevant with respect to interaction between human operator and LAWS, an assumption which is already prevalent in debates about the regulation of autonomous weaponry.

3. ACKNOWLEDGEMENTS

This research was funded by the TU Darmstadt FIF-IANUS research project *IT Research of Concern*.

REFERENCES

Adams, Stuart M., & Friedland, Carol J. (2011). A Survey of Unmanned Aerial Vehicle (UAV) Usage for Imagery Collection in Disaster Research and Management. In *Proceedings of the Ninth International Workshop on Remote Sensing for Disaster Response*. https://doi.org/10.1037//0022-0167.35.3.298

Adamson, G., Havens, J. C., & Chatila, R. (2019). Designing a Value-Driven Future for Ethical Autonomous and Intelligent Systems. In *Proceedings of the IEEE* (Vol. 107, pp. 518–525). https://doi.org/10.1109/JPROC.2018.2884923

Albers, Albert, Trautmann, Simon, Howard, Thomas, Nguyen, Trong Anh, Frietsch, Markus, & Sauter, Christian. (2010). Semi-autonomous flying robot for physical interaction with environment. In *2010 IEEE Conference on Robotics, Automation and Mechatronics, RAM 2010*. https://doi.org/10.1109/RAMECH.2010.5513152

Arkin, Ronald C., Lyons, Damian, Shu, Jiang, Nirmal, Prem, & Zafar, Munzir. (2012). Getting it right the first time: predicted performance guarantees from the analysis of emergent behavior in autonomous and semi-autonomous systems. *Proc. SPIE 8387, Unmanned Systems Technology XIV*. https://doi.org/10.1117/12.918128

Braun, Benjamin, Schindler, Sebastian, & Wille, Tobias. (2018). Rethinking agency in International Relations: performativity, performances and actor-networks. *Journal of International Relations and Development*. https://doi.org/10.1057/s41268-018-0147-z

Callon, Michel. (1984). Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. *The Sociological Review*, vol. *32*, , pp. 196–233. https://doi.org/10.1111/j.1467-954X.1984.tb00113.x

Canellas, Marc C., & Haga, Rachel A. (2016). Toward meaningful human control of autonomous weapons systems through function allocation. In *International Symposium on Technology and Society, Proceedings*. https://doi.org/10.1109/ISTAS.2015.7439432

Chao, Haiyang, Cao, Yongcan, & Chen, Yangquan. (2010). Autopilots for small unmanned aerial vehicles: A survey. *International Journal of Control, Automation and Systems*, vol. *8*, iss. 1, pp. 36–44. https://doi.org/10.1007/s12555-010-0105-z

Chmielewski, P. (2018). Ethical Autonomous Weapons?: Practical, Required Functions. *IEEE Technology and Society Magazine*, vol. *37*, iss. 3, pp. 48–55. https://doi.org/10.1109/MTS.2018.2857601

Crootof, Rebecca. (2016). A Meaningful Floor for “Meaningful Human Control.” *Temple International & Comparative Law Journal,* vol. *30*, iss. 1, pp. 53–62.

Friedman, Batya, Kahn, Peter H., & Borning, Alan. (2009). Value Sensitive Design and Information Systems. In *The Handbook of Information and Computer Ethics*. https://doi.org/10.1002/9780470281819.ch4

Friedman, Batya, & Nissenbaum, Helen. (1996). Bias in Computer Systems. *ACM Transactions on Information Systems*, vol. *14*, iss. 3, pp. 330–347. https://doi.org/10.1145/230538.230561

Gray, A., Yiqi Gao, Lin, T., Hedrick, J. K., Tseng, H. E., & Borrelli, F. (2012). Predictive control for agile semi-autonomous ground vehicles using motion primitives. In *2012 American Control Conference (ACC)*. https://doi.org/10.1109/ACC.2012.6315303

Hagele, Georg, & Soffker, Dirk. (2017). A simplified situational environment risk and system reliability assessment for behavior assurance of autonomous and semi-autonomous aerial systems: A simulation study. In *2017 International Conference on Unmanned Aircraft Systems, ICUAS 2017*. https://doi.org/10.1109/ICUAS.2017.7991415

Hanseth, Ole, Aanestad, Margunn, & Berg, Marc. (2004). Guest editors’ introduction: Actor-network theory and information systems. What’s so special? *Information Technology & People*, vol. *17*, iss. 2, pp. 116–123. https://doi.org/10.1108/09593840410542466

Hellström, Thomas. (2013). On the Moral Responsibility of Military Robots. *Ethics and Inf. Technol.*, vol. *15*, iss. 2, pp. 99–107. https://doi.org/10.1007/s10676-012-9301-2

Hocraffer, Amy, & Nam, Chang S. (2017). A meta-analysis of human-system interfaces in unmanned aerial vehicle (UAV) swarm management. *Applied Ergonomics*, vol. *68*, , pp. 66–80. https://doi.org/10.1016/j.apergo.2016.05.011

IEEE. (2016). Reframing Autonomous Weapons Systems. *The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems*. https://doi.org/10.1016/j.jaap.2016.03.014

Latour, Bruno. (1990). Technology is Society Made Durable. *The Sociological Review*, vol. *38*, iss. 1_suppl, pp. 103–131. https://doi.org/10.1111/j.1467-954X.1990.tb03350.x

Law, John. (2008, September). Actor Network Theory and Material Semiotics. *The New Blackwell Companion to Social Theory*. https://doi.org/doi:10.1002/9781444304992.ch7

Lee, Heejin, Harindranath, G., Oh, Sangjo, & Kim, Dong-Jae. (2014). Provision of Mobile Banking Services from an Actor-Network Perspective: Implications for Convergence and Standardization. *Technological Forecasting and Social Change*, vol. *90*, iss. B, pp. 551–561. https://doi.org/10.1016/j.techfore.2014.02.007

Murdoch, Jonathan. (1997). Inhuman/Nonhuman/Human: Actor-Network Theory and the Prospects for a Nondualistic and Symmetrical Perspective on Nature and Society. *Environment and Planning D: Society and Space*, vol. *15*, iss. 6, pp. 731–756. https://doi.org/10.1068/d150731

Schörnig, Niklas. (2019). Unmanned Systems: The Robotic Revolution as a Challenge for Arms Control. In C. Reuter (Ed.), *Information Technology for Peace and Security* (pp. 233–265). Wiesbaden: Springer.

Tatnall, Arthur, & Gilding, Anthony. (1999). Actor-Network Theory and Information Systems Research. In *Proceedings of 10th Australasian Conference on Information Systems* (pp. 955–966).

UNIDIR. (2014). The Weaponization of Increasingly Autonomous Technologies: Considering how Meaningful Human Control might move the discussion forward.

Preventive Arms Control for Small and Very Small Armed Aircraft and Missiles – Technical Potential, Dangers and Preventive Arms Control

MATHIAS PILCH AND JÜRGEN ALTMANN
EXPERIMENTAL PHYSICS 3, TU DORTMUND UNIVERSITY

[#38-PAPER]

ABSTRACT

Small and very small armed uninhabited air vehicles (UAVs) and missiles are actively pursued in military research and development. Despite limited payload, militarily significant damage could be achieved by very high precision, by hitting sensitive spots, and by attacking in swarms. Principally, UAVs and missiles down to 1 mm size and below could be built in the future. A wide-spread deployment can endanger arms control, destabilise the military situation between adversaries, and provide qualitatively new tools for terrorists. From a natural-science and technical viewpoint, in our new project, the current status and trends will be analysed and used to extrapolate developments over a period of 5-10 and 10-20 years. Options for preventive limitations and their verification will be considered systematically, too.

1. INTRODUCTION

Uninhabited vehicles are increasingly being deployed and used by armed forces, with uninhabited air vehicles (UAVs) most advanced. Since 2001 UAVs have been armed and used for attacks by a few states, the number of countries with armed UAVs (in 2017, there have been 28; World of Drones, 2017)) is steadily rising. These UAVs have wing spans of many metres, most traditional missiles are several metres long.[39] The principal possibility of small and very

[39] Except for shoulder-fired air-defence missiles such as the US Stinger with 1.5 m length and 14 cm diameter, (FAS (Federation of American Scientists), 2000).

small armed UAVs and missiles was mentioned early, fuelled by emerging microsystems technology and nanotechnology, but proposals for limits or prohibitions [40] have not been taken up so far. In the meantime first small armed UAVs have arrived – the US has introduced the AV Switchblade, a propeller-driven aircraft of a few times 10 cm wing span with an explosive payload that is directed over several km into a target using a video radio link. [41] Prototypes of much smaller UAVs – so-called Micro Air Vehicles (MAVs) – have been developed, e.g. the flapping-wing Nano Hummingbird in 2011 (unarmed, about 10 minutes endurance (Keennon, Klingebiel & Won, 2012)). In 2008 the US Air Force Research Laboratory presented its future vision in an animated cartoon showing a centimetres-size MAV that could kill a sniper when in direct contact (AFRL (US Air Force Research Laboratory), 2008); (see also the video by (Russell, 2017)). The micro helicopter Black Hornet Nano (Prox Dynamics, Norway), with 12 cm rotor diameter and 18 g mass, has been sold in the thousands (Prox Dynamics, 2018). Images of three cameras are transmitted by radio over up to 1.6 km. In 2016 Prox Dynamics was bought by FLIR, USA. Much smaller, insect-like MAVs are being demonstrated in research. [42] Components can be produced in two dimensions and then folded origami-like permanently or temporarily, alleviating mass production (Dufour, Owen, Mintchev & Floreano, n.d.; Ma et al., 2013; Sreetharan, Whitney, Strauss & Wood, 2012).

Much less sophisticated, improvised armed UAVs have been built and used by non-state actors using commercial and hobby multicopters as well as home-built fixed-wing UAVs, e.g. the attack on Russian air and naval bases in Syria by militants, (Binnie, 2018; New York Times, 2018) or the so-called Islamic State (IS) using them as scouts or for attacks with explosive charges (BBC, 2016).

Propeller, helicopter and flapping-wing UAVs are relatively slow, so the possibility of jet propulsion exists (it seems that the micro-turbines work on which the US Defence Advanced Research Projects Agency (DARPA) had funded in the early 2000s (Altmann, 2001, Section 4.1.5) are still under research (Wikipedia, 2017). A different approach is to make use of animals – experiments have successfully controlled the flight of a giant moth (Bozkurt, Gilmour, Sinha, Stern & Lal, 2009; see also iBionicS, 2018).

Using nanotechnology components throughout, UAVs of small-insect size, that is down to below 1 mm, should be possible – fully artificial or by modifying real insects. They could be transported to the target region by a “mothership”.

[40] Mainly by (Altmann, 2001, 2006): prohibition of missiles and „mobile micro-robots” below 0.2-0.5 m size.

[41] *Switchblade*: range: 10 km backpack with 15 km-45 km options; weight: approximately 2.5 kg including payload, launcher and transport bag; size: fits into rucksack; lethality: precision strike with very low collateral damage, (AeroVironment Inc., 2017).

[42] E.g. flapping wing, mass 80 mg, still powered via tether, (Ma, Chirarattananon, Fuller & Wood, 2013); 100 mg, perching by electrostatic adhesion, (Graule et al., 2016); about 200 mg, moving in water and air (Chen et al., 2017).

In the area of missiles (using air-breathing-jet or rocket propulsion), smaller systems have been developed, too, one intent being the wish to arm smaller UAVs. The Hellfire missile, e.g., fits to the US Predator and Reaper combat UAVs, but is much too large and heavy for smaller UAVs. [43] Smaller missiles can also be carried by a soldier and shot in a bazooka style. With a smaller warhead and destructive radius such missiles need (more) precise guidance. Examples are the BAE Advanced Precision Kill Weapon System (APKWS) with 70 mm diameter and 15 kg mass (Green, 2010), the NAVAIR Spike (57 mm, 2.4 kg) (Lance, 2006) and the Raytheon Pike (40 mm, 0.9 kg) (Raytheon Company, 2019) – the latter can be launched from a standard grenade launcher underslung under a rifle.

Principally, using nanotechnological components for casing, propellant, nozzle, sensors and control computer/electronics, pencil-sized micro missiles should be possible that would need to hit extremely precisely, with e.g. centimetres accuracy (Altmann, 2001, Section 4.2.7). What such missiles could achieve – singly, released from a “mothership” and as a swarm – in terms of speed, range, endurance as well as damage is unclear. Guided small (e.g. rifle) projectiles (e. g. EXACTO (Extreme Accuracy Tasked Ordnance), DARPA (Defense Advanced Research Projects Agency), 2015), could fulfil similar roles as small missiles – the main differences are the time courses of acceleration and speed. Hybrid systems that combine rocket propulsion with propeller, rotor or flapping wings, e.g. for the final approach, are also possible.

Expectations about the military capabilities of swarms were high already in the early 2000s (e. g. Arquilla & Ronfeldt, 2000), recently the interest has increased strongly, there is talk about a robotics revolution with swarms (Scharre, 2014, see also Hambling, 2015). The general idea is to have a number of vehicles that would act as an organic whole even if the single units may have limited computation resources. They could attack a target simultaneously or in a staged fashion from many sides, saturating defences. Various methods of defence against swarms have been mentioned, not only counter-swarms (Scharre, 2015); whether offence or defence would get the upper hand is unclear. The US military has demonstrated adaptive formation flying of 103 Perdix micro drones, released from traditional combat aircraft (US DoD (US Department of Defense), 2017) a Navy demonstration of LOCUST (Low-Cost UAV Swarming Technology) used tube launchers (Smalley, 2015). The DARPA Gremlins program is to develop reusable UAVs that would be released and recovered by a transport aircraft (DARPA (Defense Advanced Research Projects Agency), 2017). A lighter-than-air “aircraft carrier” has also been proposed (Bosma, 2017). Russia is working on UAV swarms as well as China (Hambling, 2016; Tass, 2017). First swarm attacks using “homemade” small UAVs have occurred in Syria (Binnie, 2018; New York Times, 2018). The numbers and sizes of swarm elements can vary greatly. Human control would only be possible of the swarm as a whole, but fully autonomous operation is envisaged, too (e. g. Hurst, 2017).

[43] Hellfire: length: 163–175 cm, diameter: (without fins) 18 cm, mass 45-48 kg, maximum range: 7 km (direct fire), 8 km (indirect fire), minimum range: 0.5-1.5 km (FAS (Federation of American Scientists), 2012).

Concepts for civilian applications of small UAVs abound (e.g. Small UAV Coalition, 2018). Misusing or adapting them for hostile purposes is a possibility to be reckoned with. For small missiles and rockets, on the other hand, there are only very few civilians use additional to the established ones on the horizon.[44]

2. The Project

With funding by the German Foundation for Peace Research (*Deutsche Stiftung Friedensforschung*; DSF) we shall investigate the technical potential of small and very small armed systems in the context of the systematic studies of potential military applications of microsystems technology and nanotechnology; a recent update has found no need to change the assessment or the recommendations (Altmann, 2001; Altmann, 2006, see also Altmann, 2005, 2017). Armed uninhabited systems in general have been subject to a few systematic studies with respect to technological trends, military applications, “strategic/political” consequences as well as preventive arms control (e. g. Altmann, 2013; Krishnan, 2009; Sauer & Schörnig, 2012). The subset of autonomous weapon systems has been covered in parallel to the increasing international discussions, [45] here the problem of compliance with international humanitarian law and fundamental ethical questions have been in the foreground (e.g. Sparrow, 2007; Krishnan, 2009; Asaro, 2012; Stroh, 2016), but increasingly the problem of stability is being discussed (Altmann & Sauer, 2017; Scharre, 2016). Detailed studies of preventive arms control for small and very small armed systems, differentiating them by the medium (air, land, sea, outer space) and by size class, do not exist. This project will provide reliable information on the relevant aspects of small UAVs and small missiles, and will treat preventive-arms-control aspects – including civilian applications and verification – in more detail than the earlier work.

3. Scientific Technical Analysis

The project will investigate the properties to be expected of ever smaller UAVs and missiles, including their use in swarms. [46] The scientific-technical analysis of small UAVs and missiles will treat several basic areas: aerodynamics, scaling laws for various properties (such as payload and total mass and the ratio between both, air drag, energy requirements, destructive potential), materials (including adaptive ones), engines (including micro-turbines), guidance (during flight and terminal homing), sensors, computing hardware, communication by radio (including conformal antennae, and possibly by other principles, maybe laser interrogation,[47] soft-

[44] Established: weather sounding, life-line shooting to a stranded ship, firecrackers, hobby rocketry; potentially new: very small space rockets.

[45] In particular, the informal and formal expert meetings in the context of the Convention on Certain Conventional Weapons CCW (UN (United Nations), 2018).

[46] While the focus is on armed systems, unarmed ones will be covered as well, since modifications for carrying or forming a weapon are possible.

[47] As had been discussed for "smart dust" (Pister, Kahn & Boser, 2001).

ware/algorithms, system integration, production technologies, with a special view on 3-D printing and on 2-D structuring in such a way that 3-D systems are formed by complex folding (origami).

4. Research Questions and Expected Results

The main questions of the project are:

- What is the extent of deployment in relevant countries of small armed UAVs and small missiles and what is being done in research and development?
- What properties and capabilities of small armed UAVs and small missiles are to be expected in the near future (in 5-10 years) as well as the medium-term future (in 10-20 years)?
- Will small armed UAVs and small missiles bring particular dangers (for arms control/international humanitarian law, for international security/military stability, for humans/environment/society), so that preventive limitations are recommended, and if so, how can such limitations be designed and compliance be verified?

These questions are to be answered by interdisciplinary research with a strong science and technology component.

Following the research questions, the project is to pursue three goals, correspondingly, in three partial projects.

4.1. Goal 1 Survey of the status in deployment, development and research of small armed UAVs and small missiles

Based on data bases, scientific and Internet publications, small armed UAVs and small missiles deployed and used worldwide will be listed with their properties, with a look at non-armed systems that could be provided with or used as weapons. Activities by non-state actors will be included. As far as possible from publicly available sources (including conferences, technical reports, grey literature), development and research efforts and goals will be collected and reported. Swarms and countermeasures will be covered as well.

Goal 2 Extrapolation of the properties of future small armed UAVs and small missiles

Based on the research and development efforts identified, on planning documents and forecasts, the properties and capabilities of small armed UAVs and small missiles to be expected in 5-10 years and in 10-20 years will be explored. Technical as well as military-operational aspects will be covered. Limits from the foreseeable technology status (e.g. power supply) as well as from principal laws of nature (e.g. aerodynamics) will be considered. Swarms will be treated with limited effort only, more work will be devoted to countermeasures.

4.2. Goal 3 Small armed UAVs and small missiles in the framework of preventive arms control

Small armed UAVs and small missiles (existing as well as to be expected in future) will be assessed under the standard criteria of preventive arms control (Neuneck & Mölling, 2001, (Altmann, 2005, Section 4.2). The different kinds that will have been found under goal 1 or come out as possible or plausible under goal 2 will be judged with respect to:

- Existing or intended arms-control treaties; international humanitarian law; weapons of mass destruction;
- Military stability between potential adversaries; arms races; proliferation;
- Human health, environment, sustainable development; societal and political systems; the societal infrastructure.

Because it is to be expected that strong dangers under one or more of the criteria will be found, limitation or prevention options will be considered systematically, taking into account the different kinds (e.g. by size, payload, speed, weapon effect), civilian uses, potential criminal/terrorist uses. Verification methods and means will be conceived and evaluated under various aspects, among them: providing sufficient assurance of compliance and sufficient probability of finding relevant violations, minimizing negative effects on civilian uses, limiting military as well as civilian intrusiveness.

5. Conclusion

Small armed UAVs and missiles will likely increase in importance, in military capabilities as well as in numbers of types and of systems, in particular if they act in swarms. For political decisions of countries about what to do in this area – whether to participate in a more or less unrestricted arms race, or to act for preventive limitations – well-founded knowledge about the possible developments and their dangers is needed, as is presentation of potential limitation and verification options.

The project will produce a systematic overview of the present status and the future trends (time horizon 10 years and 20 years, worldwide) of small armed UAVs and missiles, followed by an assessment under preventive-arms-control criteria and a presentation of options for limitation and verification. The results will be made available internationally by scientific publications, conference contributions and dissemination to decision makers and officials.

References

AeroVironment Inc. (2017). Switchblade data sheet. Retrieved January 23, 2018, from https://www.avinc.com/images/uploads/prouct_docs/SB_Datasheet_2017_Web_rv1.1.pdf

AFRL (US Air Force Research Laboratory). (2008). M.A.V. – Micro Air Vehicles. Retrieved January 22, 2018, from http://www.youtube.com/watch?v=_5YkQ9w3PJ4

Altmann, J. (2001). Military Uses of Microsystem Technologies – Dangers and Preventive Arms Control. Münster: agenda.

Altmann, J. (2005). Nanotechnology and Preventive Arms Control. In *Forschung DSF No. 3*, Osnabrück: Deutsche Stiftung Friedensforschung. Retrieved from https://bundesstiftung-friedensforschung.de/wp-content/uploads/ 2017/08/berichtaltmann.pdf

Altmann, J. (2006). Military Nanotechnology – Potential applications and preventive arms control. London, New York: Routledge.

Altmann, J. (2013). Arms Control for Armed Uninhabited Vehicles – An Ethical Issue. In *Ethics and Information Technology* (Vol. 15, *2*, pp. 137–152). doi:10.1007/s10676-013-9314-5

Altmann, J. (2017). Zur ethischen Beurteilung automatisierter und autonomer Waffensysteme. In I.-J. Werkner & K. Ebeling (Eds.), *Handbuch Friedensethik*, Wiesbaden: Springer VS.

Altmann, J. & Sauer, F. (2017). Autonomous Weapon Systems and Strategic Stability. *Survival*, *59*(5), 117–142.

Arquilla, J. & Ronfeldt, D. (2000). Swarming & The Future of Conflict. Santa Monica, CA: RAND: RAND Corporation. Retrieved January 23, 2018, from https://www.rand.org/content/dam/rand/pubs/documented_ briefings/2005/RAND_DB311.pdf

Asaro, P. (2012). On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision making. In *International Review of the Red Cross* (Vol. 94, *886*, pp. 687–709).

BBC. (2016). How Islamic State is using consumer drones. Retrieved January 25, 2018, from http://www.bbc.com/ future/story/20161208-how-is-is-using-consumer-drones

Binnie, J. (2018). Russians reveal details of UAV swarm attacks on Syrian bases. Retrieved January 23, 2018, from http://www.janes.com/article/77013/russians-reveal-details-of-uav-swarm-%20attacks-on-syrian-bases

Bosma, J. (2017). Lighter-Than-Air (LTA) 'Aircraft Carriers' of Persistent, Cheap Micro-Weaponized UAV Swarms for Fleet BMD Overwatch, EW, and Wide-Area ASW/Surveillance. In *23rd AIAA Lighter-Than-Air Systems Technology Conference, AIAA AVIATION Forum*. doi:10.2514/6.2017-4134

Bozkurt, A., Gilmour, R., Sinha, A., Stern, D. & Lal, A. (2009). Insect Machine Interface Base. In *Neuro Cybernetics. IEEE Transactions on Biomedical Engineering* (Vol. 56, *6*, pp. 1727–1733).

Chen, Y., Wang, H., Helbling, E. F., Jafferis, N. T., Zufferey, R., Ong, A. Wood, R. J. (2017). A biologically inspired, flapping-wing, hybrid aerial-aquatic microrobot. *Science Robotics*, *2*(11). doi:10.1126/scirobotics.aao5619

DARPA (Defense Advanced Research Projects Agency). (2015). EXACTO Guided Bullet Demonstrates Repeatable Performance against Moving Targets. Retrieved January 24, 2018, from https:// www. darpa. mil/ news- events/2015-04-27

DARPA (Defense Advanced Research Projects Agency). (2017). Progress Toward an Ability to Recover Unmanned Aerial Vehicles on the Fly. Retrieved January 23, 2018, from https://www.darpa.mil/news-events/2017-03-15

Dufour, L., Owen, K., Mintchev, S. & Floreano, D. (n.d.). A Drone with Insect-Inspired Folding Wings. In *Interna- tional Conference On Intelligent Robots And Systems (Iros 2016)* (pp. 1576–1581). New York: IEEE. Retrieved January 28, 2018, from https://infoscience.epfl.ch/record/221316/files/IROS_2016.pdf

FAS (Federation of American Scientists). (2000). FIM-92A Stinger Weapons System: RMP & Basic. Retrieved January 28, 2018, from https://fas.org/man/dod-101/sys/land/stinger.htm

FAS (Federation of American Scientists). (2012). HELLFIRE Family of Missiles. Retrieved January 23, 2018, from https://fas.org/man/dod-101/sys/land/wsh2012/132.pdf

Graule, M. A., Chirarattananon, P., Fuller, S. B., Jafferis, N. T., Ma, K. Y., Spenko, M. Wood, R. J. (2016). Perching and takeoff of a robotic insect on overhangs using switchable electrostatic adhesion. *Science*, *352*(6288), 978–982. doi:10.1126/science.aaf1092

Green, N. (2010). APKWS II Update. Retrieved July 8, 2019, from https://web.archive.org/web/20161215045906/http://www.dtic.mil/ndia/2010armament/Thursday-LandmarkANickGreen.pdf

Hambling, D. (2015). Swarm Troopers: How small drones will conquer the world. United States: Archangel Ink.

Hambling, D. (2016). If Drone Swarms Are the Future, China May Be Winning. Retrieved January 23, 2018, from http://www.popular-mechanics.com/military/research/a24494%20/chinese-drones-swarms/

Hurst, J. (2017). Robotic Swarms in Offensive Maneuver. In *Joint Forces Quarterly* (Vol. 87, *4*). Retrieved January 23, 2018, from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-87/jfq-%2087_105-111_Hurst.pdf

iBionicS. (2018). Integrated Bionic MicroSystems Laboratory (iBionicS Lab). Retrieved January 25, 2018, from https://ibionics.ece.ncsu.edu/main.html

Keennon, M., Klingebiel, K. & Won, H. (2012). Development of the Nano Hummingbird: A Tailless Flapping Wing Micro Air Vehicle. In *50th AIAA Aerospace Sciences Meeting including the New Horizons Forum and Aerospace Exposition, Aerospace Sciences Meetings*. doi:10.2514/6.2012-588

Krishnan, A. (2009). Killer robots: Legality and Ethicality of Autonomous Weapons. Farnham/Burlington VT: Ashgate.

Lance, D. G. (2006). World's Smallest Guided Missile Hits Target. China Lake, CA: Naval Air Warfare Center Weapons Division Public Affairs Office. Retrieved July 8, 2019, from https ://web.archive.org/web/20170102083321/http://www.navair.navy.mil/index.cfm?fuseaction=home.NAVAIRNewsStory&id=3468

Ma, K. Y., Chirarattananon, P., Fuller, S. B. & Wood, R. J. (2013). Controlled Flight of a Biologically Inspired, Insect-Scale Robot. *Science*, *340*(6132), 603–607. doi:10.1126/science.1231806

Neuneck, G. & Mölling, C. (2001). Methoden, Kriterien und Konzepte für Präventive Rüstungskontrolle. In *Wissenschaft und Frieden, Dossier Nr. 38*.

New York Times. (2018). Russia Says Its Syria Bases Beat Back an Attack by 13 Drones. Retrieved January 25, 2018, from https://www.nytimes.com/2018/01/08/world/middleeast/syria-russia-drones.html

Pister, K., Kahn, J. & Boser, B. (2001). Smart Dust: Autonomous sensing and communication in a cubic millimeter. Retrieved January 28, 2018, from http://robotics.eecs.berkeley.edu/~pister/SmartDust

Prox Dynamics. (2018). PD-100 PRS. Retrieved January 18, 2018, from http://www.proxdynamics.com/products/pd- 100-black-hornet-prs

Raytheon Company. (2019). Pike munition – Miniaturized, Laser-Guided Weapon. Retrieved July 8, 2019, from https://www.raytheon.com/capabilities/products/pike

Russell, S. (2017). Slaughterbots. Retrieved January 25, 2018, from https://www.youtube.com/watch?v=9CO6M2HsoIA

Sauer, F. & Schörnig, N. (2012). Killer Drones – The Silver Bullet of Democratic Warfare? In *Security Dialogue* (Vol. 43, *4*, pp. 363–380).

Scharre, P. (2014). Robotics on the Battlefield Part II: The Coming Swarm. Washington DC: Center for a New American Security. Retrieved January 23, 2018, from https://s3.amazonaws.com/files.cnas.org/documents/ CNAS_TheComingSwarm_Scharre.pdf

Scharre, P. (2015). Counter-Swarm: A guide to defeating robotic swarms. Retrieved January 23, 2018, from https://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-%20swarms/

Scharre, P. (2016). Autonomous Weapons and Operational Risk. In *CNAS Working Papers*, Washington, D. C.: Center for New American Security. Retrieved January 28, 2018, from https://www.cnas.org/publications/reports/ autonomous-weapons-and-operational-risk

Small UAV Coalition. (2018). Benefits. Retrieved January 29, 2018, from http://www.smalluavcoalition.org/benefits/

Smalley, D. (2015). LOCUST: Autonomous, swarming UAVs fly into the future. Arlington, Va.: Office of Naval Research. Retrieved January 18, 2018, from https://www.onr.navy.mil/Media-Center/Press-Releases/2015/LOCUST-low-cost-UAV-swarm-ONR.aspx

Sparrow, R. (2007). Killer Robots. In *Journal of Applied Philosophy* (Vol. 24, *1*, pp. 62–77).

Sreetharan, P. S., Whitney, J. P., Strauss, M. D. & Wood, R. J. (2012). Monolithic fabrication of millimeter-scale machines. *Journal of Micromechanics and Microengineering*, *22*(5, 055027). Retrieved from http://iopscience.iop.org/article/10.1088/0960-1317-/22/5/055027/meta

Stroh, P. (2016). Humanitär-völkerrechtliche Rahmenbedingngen für den Einsatz luftgestützter unbemannter militärischer Kampfsysteme im bewaffneten Konflikt. In *DSF Forschung Nr. 40*, Osnabrück: Deutsche Stiftung Friedensforschung. Retrieved January 28, 2018, from https://bundesstiftung- friedensforschung.de/blog/forschung-dsf-no-40/

Tass. (2017). Russia is developing artificial intelligence for military and civilian drones. Retrieved January 23, 2018, from http://tass.com/defense/945950

Weapons Verification with High-Tech? – Chances of and Obstacles to Making Use of Emerging Technologies in Arms Control

NIKLAS SCHÖRNIG
PEACE RESEARCH INSTITUTE FRANKFURT (PRIF)

[#39-PAPER]

PAPER

It has become almost a dictum that arms control[48] is in a crisis. But whenever the arms control community feels that rock bottom has been reached, things get even worse. The fact that after the US withdrawal from the INF Treaty, which eliminated land-based intermediate- and short-range missiles, the Trump administration is also very likely to not prolong the New START treaty on strategic nuclear weapons (Gramer and Seligman 2019), is a case in point here. While much of the current problems can be related to political differences and a lack of political will,[49] one has to ask how new technologies factor into these problems. Emerging technologies, and especially, but not exclusively information technologies, are changing the military landscape dramatically. Networked warfare has become one of the buzz words of the last decade(s), first within Western democracies (under the label of a Revolution in Military Affairs (RMA) or Transformation; McNaughter 2007) but with other technologically advanced states following soon (Newmyer 2010). In addition, autonomous weapon systems (AWS) based on complex expert systems and AI have become a hotly debated topic, less so within the military community but by think tanks (e.g. Schörnig 2010; Scharre 2018), non-governmental organizations (Human

[48] In this text, arms control is understood as a rather broad concept, including disarmament measures (i.e. the reduction of weapons), stability measures (i.e. limitations- including controlled armament) as well as transparency measures , e.g. confidence and security building measures (CSBMs) or regular information exchange (Müller and Schörnig 2006).

[49] Harald Müller argues that different states of relations between states, ranging from hostility to security community, offer related options for arms control. While opponents, for example, are only likely to agree to limit their armament rather than disarm, states with mostly cooperative relations are willing to accept far-reaching transparency (Müller 1996: 405-408).

Rights Watch 2012; Heinrich Böll Foundation 2018) and a concerned public. Critics of so-called lethal autonomous weapon systems (LAWS) fear that in the not so far future, computer algorithms rather than human operators will decide upon life and death, that these systems will not be able to uphold international law and will lead to a significant acceleration of warfare (e.g. Heinrich Böll Foundation 2018). While advocates of automated weapons reject many of these arguments, most agree, however, that weapon systems which use artificial intelligence enhanced by machine learning, would be too risky to use given the unpredictability and intransparency of the decision making processes of such systems.[50] In sum, new emerging technologies might have a severe impact on threat perceptions, military operations and crisis as well as strategic stability (Altmann and Sauer 2017).

What makes matters worse, is that many of these emerging technologies render well-known and proven techniques of arms control useless. Simplifying a bit, arms control during the Cold War was essentially based on bean-counting planes, missiles, tanks and so forth. Since the rapid advances in computing power and information technologies experienced since the 1990s, however, the capability of a certain weapon system is more and more defined by software and constant information exchange rather than its hardware. Instead of focusing on quantities, arms control has to focus on quality (Schörnig 2015; Fey 2016) or content itself with confidence and security building measures – CSBMs (Altmann 2019). So, rather than just having to deal with the lack of political will limiting arms control options, technological developments are making the prospect of successful arms control agreements even bleaker.

On the other hand, however, new and emerging technologies can help to overcome certain problems classical arms control regimes face. It is a specific problem of arms control that it can fail even if all participating parties have an interest in it, when all sides distrust the others to stick to the agreement. All parties fear that if they comply whereas the other side cheats they will end with a significant disadvantage reducing their security (Waltz 1979). From an arms control perspective, international treaties to limit or reduce weapon systems must always be backed by working and trustworthy verification procedures, which are key to the acceptance of any arms control regime in an anarchic international system.[51] Verification can be understood as the “process of gathering and analyzing information to make a judgement about parties’ compliance or non-compliance with an agreement. It aims to build confidence between the parties, assuring them that their agreement is being implemented effectively and fairly” (UNIDIR 2003: 1). Especially when the relations are tense, the need for reliable (for the verifier) and acceptable (for the verified) verification measures is paramount for the success of arms control. Verification, therefore, usually walks a tight rope. On the one hand, it has to ensure that the verifying party gets enough certainty about the opposing side’s behaviour to accept limitations on its own armament. On the other hand, verification must to be not too intrusive, as intrusive measures can be used for espionage, revealing military secrets to the verifying party

[50] Several personal conversations with military personnel.

[51] In the discipline of international relations, “anarchy” does not mean a lawless situation with anyone fighting anyone else but simply the fact that there is no higher entity above the nation state ensuring a state’s survival. In an anarchic international system states a basically facing a self-help system (Waltz 1979).

which could lead to a military disadvantage or even a surprise attack. So, rather than ensuring 100% certainty, verification has to balance these contradicting claims, provide all parties with sufficient information without being too noisy and drive up the costs of cheating, both in economic as well as political terms, to unacceptable levels. Furthermore, successful verification provides enough early warning time for an appropriate reaction should one partner cheat nevertheless (Wiesner 1986) and, in extreme cases, legitimizes coercive measures (e.g. national or international sanctions) to bring a deviating party back into compliance (Daase and Meier 2013).

In reality, however, verification is easier said than done. While there is a debate about reforming the *Chemical Weapons Convention* verification regime, the *Biological Weapons Convention* still lacks any verification mechanism and is likely to do so for the foreseeable future. The Open Skies Treaty allows inspection flights over all European countries, the US and Canada with especially certified planes to enhance transparency and trust. These planes, however, are often denounced as “spy planes” by the media[52] and even some scientific outlets.[53] And when it comes to autonomous weapons, some experts blame the lack of any reliable verification system for the stalling debates in the UN context (Horowitz 2016).

In sum, verification is a hotly debated issue in many realms of armament. But it is obvious, that certain new technologies like drones, new sensors and AI-based systems offer the potential to improve at least some of the existing regimes or to facilitate future ones.

One case in point is the *Comprehensive Test Ban Treaty* (CTBT) which bans all nuclear test explosions - underground, underwater, in the atmosphere or in outer space.[54] It has been signed by more than 180 states and ratified by more than 160[55] but has not yet come into force as some mandatory states have yet to sign.[56] However, in anticipation of the treaty, the CTBT Organization, the CTBTO, has already been established and has already set up an International Monitoring System (IMS) consisting of 336 stations in 89 countries to detect any nuclear explosion world-wide by infrasound, underwater sound, seismic activities and radionuclide concentration. Already as early as 2010, scientists proposed using machine learning technology “that could provide both incremental and comprehensive value for event detection by increasing the accuracy of the final data product” (Russel et al. 2010). It is intuitively comprehensible that machine learning, which is very well suited for statistically based pattern recognition (more and more often surpassing human abilities), can help to distinguish, for example, between natural and man-made seismic activity, helping to avoid both false positives (leading to wrong

[52] E.g. https://www.cbsnews.com/news/russian-spy-plane-flying-over-sensitive-u-s-military-sites/.

[53] https://warisboring.com/a-russian-spy-plane-is-being-allowed-to-photograph-u-s-military-sites/.

[54] https://www.ctbto.org/fileadmin/content/reference/outreach/objective_and_activities_2007_web.pdf.

[55] https://www.ctbto.org/the-treaty/status-of-signature-and-ratification/.

[56] The so-called Annex 2 states which have yet to sign are: DPRK, India and Pakistan, while China, Egypt, Iran, Israel, and the United States have signed, but not ratified.

accusations and political tension) as well as false negatives, where a potential threat goes undetected. On the other end of the spectrum, machine learning technology has been put to use to help distinguishing between anti-personnel mines (APMs) and flattened tin cans. When earth penetrating radar is used in the process of demining, APMs and flattened cans present very similar radar echoes. So, flattened cans produce false positives, significantly slowing down the process of demining. With the help of self-learning algorithms, the process is eased considerably (Lück 2019). Yet another example is the use of satellite imagery, paired with machine learning to identify missile sites[57] – or other (potentially) military sites of interest. These short examples show in an exemplary way how new technologies can enhance the significance of available data beyond human assessment. States should have an interest in introducing these technologies to enhance verification.

Yet states are rather reluctant to accept new technologies for verification purposes. And here the second aspect of verification – intrusiveness – comes into play. Trusting software to only assess what the regime allows is a tricky issue. How can it be guaranteed, that the new technology is tailored so narrowly to fit a specific verification purpose that no safety concerns are valid? One case in point is the Open Skies (OS) Treaty. The treaty allows "four types of sensors with which observation aircrafts could be equipped, including optical panoramic and framing cameras, video cameras with real-time display, infra-red line-scanning devices, and sideways-looking synthetic aperture radar".[58] The cameras had to be analog for a long time and it was as late as 2014 when Russia was the first country to certify and install digital equipment on one of its OS planes (Spitzer 2014, 2018). While the result was to allow digital equipment in the end, the fear of not being able to cope with the wide range of opportunities new technology is offering, often leads to a very conservative and reluctant approach. The main resulting question therefore is, how this fear can be overcome to reap the rewards new technology is offering for verification purposes. In other words: the second level problem of how to ensure transparency within the instruments which are used to create first level transparency has to be solved. In the case of AI-driven arms control, the obvious approach would be to demand explainability in arms control algorithms. But this might actually lead to a paradox: Measures ensuring explainability in machine learning for arms control purposes might help developing acceptable machine learning AI suitable for autonomous weapons in the end. So much more creativity is needed, to ensure tailored technologies suitable for verification purposes.

One thing is clear, however: Decision makers who lack the political will to foster arms control should not be given the chance to hide behind technological excuses for inaction.

[57] https://spacenews.com/with-commercial-satellite-imagery-computer-learns-to-quickly-find-missile-sites-in-china/.

[58] https://www.nti.org/learn/treaties-and-regimes/treaty-on-open-skies/.

References

Altmann, Jürgen 2019. Militärische Vorbereitungen auf Cyberkrieg – Gefahren und mögliche Begrenzungen. In I.-J. Werkner and N. Schörnig, eds, *Cyberwar – die Digitalisierung der Kriegsführung. Fragen zur Gewalt • Band 6*, Wiesbaden: Spinger VS, forthcoming.

Altmann, Jürgen/Sauer, Frank 2017: Autonomous Weapon Systems and Strategic Stability. *Survival* 59 (5), pp. 117-42.

Daase, Christopher/Meier, Oliver 2013. The changing nature of arms control and the role of coercion. In C. Daase and O. Meier, eds, *Arms Control in the 21st Century*, Milton Park: Routledge, pp. 233-41.

Fey, Marco 2016: Waffen aus dem 3D-Drucker: Additives Fertigen als sicherheitspolitisches Risiko? (HSFK-Report Nr. 9/2016), Frankfurt: HSFK.

Gramer, Robbie/Seligman, Lara 2019. The INF Treaty Is Dead. Is New START Next? https://foreignpolicy.com/2019/02/01/the-inf-treaty-is-dead-is-new-start-next-russia-arms/. Last access: June 28, 2019.

Heinrich Böll Foundation (ed.) 2018.*Autonomy in Weapon Systems. A Report by Daniele Amoroso, Frank Sauer, Noel Sharkey, Lucy Suchman and Guglielmo Tamburrini* Berlin: Heinrich Böll Foundation.

Horowitz, Michael C. 2016. Ban killer robots? How about defining them first? https://thebulletin.org/ban-killer-robots-how-about-defining-them-first9571. Last access: Junary 15, 2018.

Human Rights Watch 2012: Losing Humanity. The Case against Killer Robots, Washington, DC: Human Rights Watch.

Lück, Nico 2019: Künstliche Intelligenz und Rüstungskontrolle. Der Einsatz maschinellen Lernens in Waffensystemen und Verifikationsmaßnahmen. PRIF Report 4/19, Frankfurt: HSFK.

McNaughter, Thomas L. 2007: The Real Meaning of Military Transformation: Rethinking the Revolution *Foreign Affairs* 86 (1), pp. 140-7.

Müller, Harald 1996. Von der Feindschaft zur Sicherheitsgemeinschaft - Eine neue Konzeption der Rüstungskontrolle. In B. Meyer, ed, *Eine Welt oder Chaos?*, Frankfurt: Suhrkamp, pp. 399-428.

Müller, Harald/Schörnig, Niklas 2006. *Rüstungsdynamik und Rüstungskontrolle: Eine exemplarische Einführung in die Internationalen Beziehungen*. Baden-Baden: Nomos.

Newmyer, Jaqueline 2010: The Revolution in Military Affairs with Chinese Characteristics. *Journal of Strategic Studies* 33 (4), pp. 483-504.

Russel, Stuart/Vaidya, Sheila/Le Bras, Ronan 2010: Machine learning for Comprehensive Nuclear-Test-Ban Treaty monitoring, in: *CTBTO Spectrum 14,* Retrieved from https://www.ctbto.org/fileadmin/user_upload/pdf/Spectrum/2010/Spectrum14_page32_machinelearning.pdf. Last access: June 12, 2019.

Scharre, Paul 2018. *Army of None. Autonomous Weapons and the Future orf War*. New York, London: W.W. Norton & Company.

Schörnig, Niklas 2010. *Robot Warriors. Why the Western investment into military robots might backfire. PRIF Report No. 100*. Frankfurt: HSFK.

Schörnig, Niklas 2015 From Quantitative to Qualitative Arms Control: The Challenges of Modern Weapons Development. In M. Roth, C. Ulbert and T. Debiel, eds, *Global Trends*

2015. Prospects for World Society, Bonn: Stiftung Entwicklung und Frieden/Development and Peace Foundation, pp. 87-100.

Spitzer, Hartwig 2014: Open Skies: transparency in stormy times. In: Trust & Verify 146, July-September 2014, 1-5. https://www.vertic.org/media/assets/TV/TV146.pdf

Spitzer, Hartwig 2018. The Open Skies Treaty as a transparency regime. Retrieved from https://www.bits.de/public/pdf/Open-Skies_2018_11_02_HS-CS.pdf

UNIDIR 2003. *Coming to terms with Security. A Handbook on Verification and Compliance*. Geneva/London: UNIDIR/VERTIC.

Waltz, Kenneth N. 1979. *Theory of International Politics*. Reading: Addison Wesley.

Wiesner, Jerome B. 1986. Introduction. In K. Tsipis, D. W. Hafemeister and P. Janeway, eds, *Arms Control Verification. The Technologies That Make It Possible*, Washington: Pergamon Brassey's pp. xiii-xvi.

Echoes of the Past? New Technologies and Securitization in the Next Phase of the Space Age

Arne Sönnichsen
University of Duisburg-Essen

### [#40-EXT.-ABSTRACT]

Extended Abstract

Is the governance framework fit for the next phase in the space age? The answer to this question proves difficult. While scientists look for answers in the skies about the universe and Earth alike, a wide variety of new actors are becoming engaged in pursuing their interests in outer space: ‘New Space’ corporations dream of exploiting resources or to colonize heavenly bodies, the old space-faring countries dream of new ‘space firsts’ for political capital or to dominate this new domain, and countries new to space-faring are looking forward to become part of the exclusive space club marking great power status in the 21st century (Paikowsky 2017). The multitude of developments has been dubbed the commercialization, democratization, and militarization of outer space (Pekkanen 2019). All of these possibilities are heavily interlaced with the advent of new technologies – new launcher systems, miniaturization, and fragmentation allow for easier access and thus easier use of outer space. Simultaneously, the rules to engage space and to keep peace still rest on the ‘five treaties’ [59] that successfully governed outer space operations in the past 50 years and which were able to prevent peaceful cooperation. But several of the newest challenges like commercialization and democratization were never covered in the treaties, and the recent actions of China and the recent anti-satellite weapons (ASAT) test of India of March 2019 might lead to a new wave of militarization and securitization of outer space.

My dissertation attempts to answer how new technologies stimulate ordering processes by actors. Due to new technologies, new actors are engaged in pursuing their interests in outer space. Actors create order and governance unilaterally or multilaterally that serve their needs – they are ‘ordering’ outer space.

[59] The most important one is the „Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies“, or in short OST (Outer Space Treaty), from 1967, which is flanked by ARRA (1968), LIAB (1972) and REG (1975). The most recent treaty, MOON (1979), was not fully ratified.

I employ two approaches. While scholars of classical geopolitics argue, that the materiality of geography is fixed and dictate the behaviour of actors, scholar of critical geopolitics argue, that places do have a distinct materiality, but its usage is constructed through knowledge, discourses, and ideas. They create order – the rules, institutions, activities, and strategies in different historical periods (Agnew und Corbridge 1995, 15) which at one point lead to the creation of Governance, defined as the "definition of actors, rules of operation, principles of interaction, and widely shared assumptions about trade, force and diplomacy." (Agnew und Corbridge 1995, S. 16). The existing outer space governance rests on the five treaties and has been successfully prevented conflict in outer space while serving the interests of the old space-faring nations, but new technologies shift the interpretation of outer space as a place for human activity. The shifting understanding and implication of outer space is best addressed by scholars of Critical Geopolitics who argue that the knowledge about spaces is the prerequisite to do things in spaces (Ó Tuathail 1997). In this perspective, a place becomes a place once actors attach meaning to it. For instance, once capabilities become available to make use of outer space, actors are inclined to 'territorialize' these spaces (Lambach 2017). The knowledge about outer space has been around for quite a while, but recently new technologies – understood as applied knowledge – enable actors to pursue their interests anew. That means that technology is the reason why outer space and its governance is becoming contested.

In much of the literature on international politics, technology is treated as a given fact. Of course, some historicity is implicated but once an actor is in possession of say, nuclear weapons, he is treated as an actor of many different qualities, an actor of the 'nuclear club'. This view is complicated, because technologies do not materialize out of thin air, technologies are constructed by people and in the case of high-technology it is unlikely that it happened without the knowledge of the states. In fact, the Apollo space program is thought to be one of the most important events that changed how states (here the U.S.) were involved in research and development of new big-scale technologies (McDougall 1997). The study of technology in IR had some early works (Skolnikoff 1993; Herrera 2006) and is recently rediscovered by scholars of IR (McCarthy 2018). Most of the studies are heavily influenced by Science and Technology Studies (STS). For my work, I understand technology both as the product and the driver of societal processes, for which a social constructivist approach of technology (SCOT) is best suited. Technology here is not confined to the narrow conception of technology as an artefact with a determinist usage or materialist capability, but as part of societal processes. Technologies follow a path of path-dependency and contingencies that mirror the determinist view, but are influenced by choices made by designers or consumers (Manjikian 2018, 27), an issue much especially problematic in the case of dual-use goods. The advent of technology thus influences the discourses surrounding outer space.

My basic argument is that new technologies change the way outer space is viewed. New technology lowers the threshold to do things in space. First, it enables new actors to do things in space – both states and non-governmental entities. Second, it allows new activities in outer space. Because of this, actors attempt at 'ordering' – they try to create or change the governance in a way that favours their interests, either by creating hard or soft law or by influencing discourses about outer space. This can clearly be witnessed in human spaceflight. Asteroid mining is an example. Harvesting asteroids is thought to be a solution to the growing hunger for raw materials and minerals. Because the OST did not clearly specify the circumstances of mining asteroids and because of legal uncertainties the U.S. Congress (2015) and Luxembourg (2017) passed laws that would allow corporations in their countries to keep minerals harvested in outer space, thus fostering further investment and research, but undermining effective governance, too (Man 2017). Simultaneously we can witness discussions surrounding the creation of a 'space situational awareness' (SSA) that would help coordinate the intensified activities in outer space and address the issue of space debris.

In security issues we witness similar developments. In 2001, a commission warned the U.S. public of a possible 'space pearl harbour', if the U.S. would not develop counterspace capabilities (Commission to Assess United States National Security Space Management and Organization 2001). Only in 2018, U.S. president Donald Trump announced the creation of a sixth branch in the U.S. armed forces, one specifically designed "to fight and win wars". While it is not surprising, that at one point outer space would be subject to deepened security concerns (Wolter 2006), it is a clear indicator, that the change is more of a recent one and can be read as an attempt to pool the outer space capabilities that are dispersed throughout U.S. government entities (Hunter und Bowen 2018). In June 2019, the NATO announced that it will draft a strategy paper to account for heightened security concerns stemming out of Russian and Chinese counterspace capabilities (Peel 2019). Attempts to harness the possible militarization were not yet successful (Gindullis 2016).

REFERENCES

Agnew, John A.; Corbridge, Stuart (1995): Mastering Space. Hegemony, Territory and International Political Economy. London, New York: Routledge. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=80071.

Commission to Assess United States National Security Space Management and Organization (2001): Report of the Commission to Assess United States National Security Space Management and Organization. Washington D.C. Retrieved from http://www.dod.gov/pubs/space20010111.html, zuletzt geprüft am 24.05.2017.

Gindullis, Marinke (2016): Is the European Initiative for an International Code of Conduct the right Step forward for Conflict Prevention in Outer Space? IFSH. Hamburg (IFAR² Fact Sheet).

Herrera, Geoffrey Lucas (2006): Technology and International Transformation. The Railroad, the Atom Bomb, and the Politics of Technological Change. Albany: State University of New York Press.

Hunter, Cameron; Bowen, Bleddyn (2018): Donald Trump's Space Force isn't as new or as dangerous as it seems. ed. by The Space Review. Retrieved from http://www.thespacereview.com/article/3559/1, [12.06.2019].

Lambach, Daniel (2017): Kings of the Wild Frontier: International Society and the Territorialization of Empty Space.

Man, Philip de (2017): State Practice, Domestic Legislation and the Interpretation of Fundamental Principles of International Space Law. In: *Space Policy* 42, S. 92–102.

Manjikian, Mary (2018): The Social Construction of Technology. How Objects Acquire Meaning In International Security. In: Daniel R. McCarthy (ed.): Technology and World Politics. An Introduction. London: Routledge.

McCarthy, Daniel R. (ed.) (2018): Technology and World Politics. An Introduction. London: Routledge.

McDougall, Walter (1997): The Heavens and the Earth. A Political History of the Space Age. Baltimore: Johns Hopkins University Press.

Ó Tuathail, Gearóid (1997): Critical Geopolitics. The Politics of Writing Global Space. London, New York: Routledge.

Paikowsky, Deganit (2017): The Power of the Space Club. Cambridge: Cambridge University Press.

Peel, Michael (2019): Nato prepares first outer space strategy to deal with new threats. Alliance looks to combat growing military capabilities of Russia and China beyond Earth. Financial Times. Retrieved from https://www.ft.com/content/08bb833c-9439-11e9-aea1-2b1d33ac3271, zuletzt aktualisiert am 26.06.2019.

Pekkanen, Saadia M. (2019): Governing the New Space Race. In: *AJIL Unbound* 113, S. 92–97. DOI: 10.1017/aju.2019.16.

Skolnikoff, Eugene B. (1993): The Elusive Transformation. Science, Technology, and the Evolution of International Politics. Princeton, NJ: Princeton University Press.

Wolter, Detlev (2006): Common Security in Outer Space and International Law. Geneva: UNIDIR.

The question of swARMS CONTROL – Challenges to Ensuring Human Control over Military Swarms

MAAIKE VERBRUGGEN

INSTITUTE FOR EUROPEAN STUDIES, VRIJE UNIVERSITEIT BRUSSEL

## [#41-ABSTRACT]

ABSTRACT

In light of the increasing efforts to develop military swarms, it is important to increase our understanding of the opportunities for human control over swarms. This paper will translate the technical engineering literature on swarms to a political context, in order for the international community to better understand what the implications of military swarms will be. This paper will set out what swarms are and how they work, and what we already know about the challenges to (Meaningful) Human Control, as well as the potential solutions. It is followed by a review of the state of the art in the swarm's robotics literature highlighting the various challenges to Human Control and Human-Swarm Interaction. The technical literature shows that operating swarms are highly cognitively demanding. Humans struggle to keep track of many units at the same time and accurately predict the exact effect of their commands, especially under latency and low bandwidth. Furthermore, emergent swarms are inherently unpredictable and impossible to verify and validate. As the limits to adjusting swarm behaviour after launch provides limited space for operational control, the opportunities for human control should be maximized during the design phase. This would be helpful from both a strategic and a humanitarian perspective.

Comparison of Seismic Signals of Tracked Vehicles on Asphalt and Sand Road

HUBERTUS SONNTAG AND JÜRGEN ALTMANN

EXPERIMENTAL PHYSICS III, TU DORTMUND UNIVERSITY

[#42-EXT.-ABSTRACT]

Extended Abstract

When a treaty is concluded to create or keep peace in a certain area, different types of sensing can be used for verification whether the involved parties comply with the treaty. Such sensing can be visual, acoustic or, as in this case, seismic.

The data used in this work come from measurements that took place in 1992 at Amersfoort, Netherlands, and were carried out by the 'Bochum Verification Project' (Altmann 2004). There were two types of tracked vehicles, one was a 'Leopard 1' main battle tank (MBT) and the other was a 'YPR765' armoured personnel carrier (APC). There were two vehicles of each type, to also have the possibility to find out whether there are type-specific characteristics or not. Further, there is interest in the differences between the various types. The vehicles were driven on an asphalt and a sand road, with different velocities in two directions, to achieve more knowledge about the properties of the vehicle signals. It is also important to see how well the sensing works further away from the vehicle path and to determine up to which distance signals are still usable for verification.

Geophones were set up in various distances to measure how the signal changes with distance. On some of them, the most distant ones, there were short disturbance pulses in the measured signals. To have an appropriate data quality, these pulses were removed with a program using the 'short time average/long time average' method that is often used to detect earthquakes. This program can detect and erase outliers of the data, based on characteristics of the undisturbed signal.

Seismic waves from tracked vehicles are caused by the piston movement in the engine, the force on the track elements rolled over to be the road wheels and the movement of the vehicle over rough ground. Also, the acoustic signals, caused by the exhaust pressure pulses from the engine and the driving of the tracks by the sprocket wheels cause seismic waves when impinging on the ground.

We are evaluating the measurements made with velocities of 20 and 40 km/h in two opposite directions, east and west. The evaluation firstly focused on the amplitude of the soil velocity. Secondly,

the spectral power was computed and plotted against the frequency, to see where there are noticeable parts in the spectrum and to get two important frequencies from it. One is the frequency of rolling over the track elements v_T, the other is the rotation frequency of the engine crankshaft v_E. In the spectrum there are also harmonics of these two frequencies, where it is remarkable that usually for the MBT the fifth multiple of v_E is the strongest of the engine series, as shown in figure 2. This is because the 10-cylinder engine has five cylinders for each of its two exhausts. From v_T and v_E the vehicle velocity and the engine rotation rate, respectively, can be determined. For the calculation of the velocity the length of the track element l_T is multiplied with v_T. For the passes on the asphalt road the velocity could be gained from infrared breakbeams across the road, too.

For the amplitude the signal strength is plotted against the distance between the road and the sensor, as shown in figure 1. In the figure the maximum peak-to-peak value of seismic velocity, that is the absolute value of the difference between the highest and the lowest measured value of every sensor, is shown for passes of the APC. The data show that the amplitudes with 20 km/h speed are somewhat higher than the ones from 40 km/h.

Our preliminary evaluations have not shown significant differences between the different grounds. The final conclusions will need further analyses.

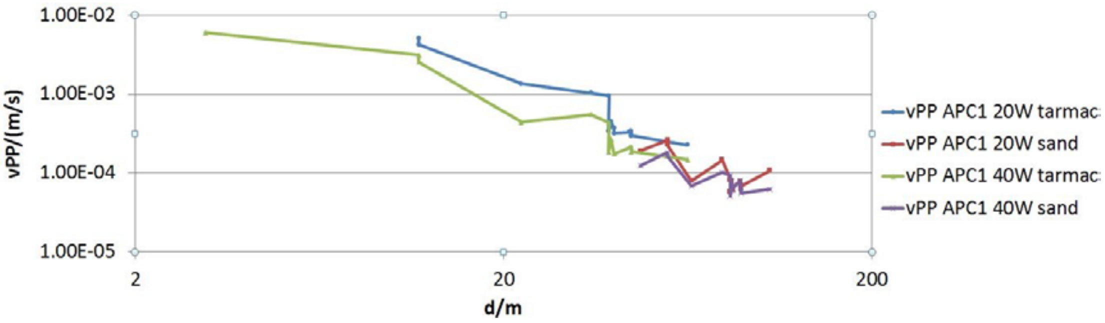


Figure 1: Maximum peak-to-peak values of vertical ground velocity versus distance during passes of APC 1 on the asphalt and the sand road. At the right the nominal speed in km/h, the direction (only west in this case) and the road type are indicated.

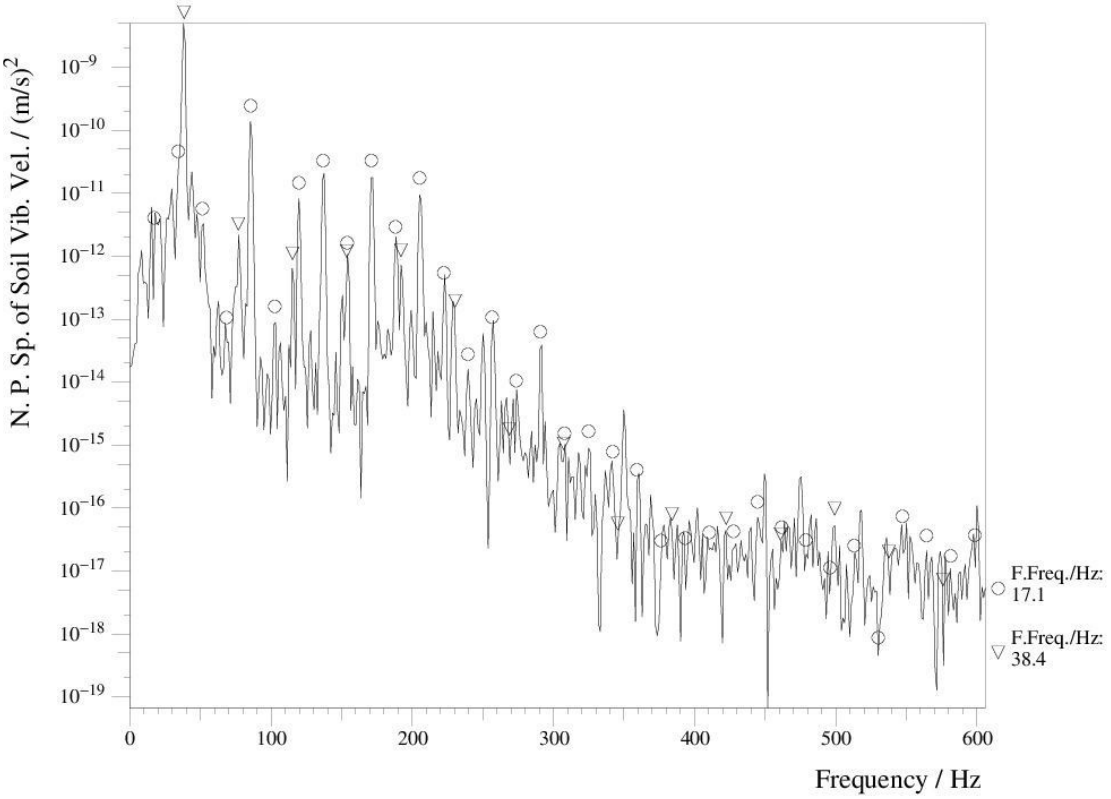


Figure 2: Power spectrum of vertical soil velocity from an MBT driving over the asphalt road with 40 km/h in western direction. It is measured with a sensor 60 meters away from the road, at the time of passing the sensor (around the closest point of approach). The frequency of rolling over the track elements v_T = 38.4 Hz and its multiples are marked with triangles, the rotation frequency of the engine crankshaft v_E = 17.1 Hz and its multiples are marked with circles. Note that the fifth multiple at 85.5 Hz is the strongest of this harmonic series.

REFERENCES

J. Altmann, Acoustic and Seismic Signals of Heavy Military Vehicles for Co-operative Verification, Journal of Sound and Vibration 273 (4-5), 713-740, 21 June 2004

TRACK IV: OPEN TRACK

Civil-Military Interactions, Dual-Use and Preventive Arms Control in Science and Technology

JÜRGEN SCHEFFRAN

INTEGRATIVE GEOGRAPHY, UNIVERSITY OF HAMBURG

[#43-PAPER]

ABSTRACT

This contribution addresses the growing interaction between military and civilian applications of science and technology as well as efforts to control it. Challenges of new technologies in complex conflict landscapes require novel approaches of preventive arms control combined with political and legal frameworks that tackle the dual-use problem in the early phases of research and development. Missile and space technologies serve as examples.

1. CHALLENGES OF CIVIL-MILITARY AMBIVALENCE AND DUAL-USE IN SCIENCE AND TECHNOLOGY

Civil-military interactions have shaped the history of science, technology and war (Altmann et al. 2017). In the past, the military was often suggested as a pacemaker of technology development, even though the spin-offs remained less than expected. In the 20th century, advanced technology has become an essential element of both the economy and national security. While the dichotomy between civilian and military technology was more pronounced during the East-West conflict when large-scale science and technology became part of the military-industrial complex, the boundaries eroded after the end of the Cold War. Scarce resources and lack of public acceptance, combined with converging demand profiles, supported the dual-use of technologies that have actual or potential military and civilian applications, systematically exploiting the ambivalence of science without being transparent (Liebert, Rilling & Scheffran 1994). The military benefited from research in the private sector by taking advantage of civilian goods and saving on development costs. The strategy of "commercial-off-the-shelf" development puts more emphasis on spin-in: taking advantage of economies of scale, a technology developed in the civilian-commercial sector is used for military purposes. Modern semiconductors, nuclear, laser, bio, space, digital, computer and communication technologies, to mention a few, are employed not only in civilian products but also in weapons. However, civilian products were not optimized for military tasks and an advantage over opponents was not guaranteed since the technology was available on the international market.

Until today scientific knowledge and technical know-how are essential preconditions for weapons development and sources of proliferation (Scheffran 2006). Countries that want to keep their advantage in military technologies or prevent negative impacts on their security are more ready to control exports of “sensitive” technologies to “critical” countries. Major suppliers have agreed that certain technologies which are devoted to the development and production of weapons of mass destruction (nuclear, chemical, or biological) and related dual-use items, including delivery systems, should be subject to strict export controls. When the Wassenaar Arrangement replaced the COCOM list in 1996, the export control focus shifted from an East-West to a North-South context, including technologies for weapons of mass destruction based on the Trigger List of the London Nuclear Suppliers Club, the Australia Group for chemical weapons, and the Missile Technology Control Regime (MTCR) (Brauch et al. 1992).

The shift towards actual warfighting has promoted a “Revolution in Military Affairs” (Neuneck & Alwardt 2008). The United States seeks to strengthen its supposed technology lead against potential competitors and focuses on scientific and technological capabilities being developed worldwide that have the potential to significantly enhance or degrade US military capabilities in the future. After the attacks of September 11, 2001, and the declared “war on terror”, the parameters changed again. The old certainties have disappeared, but the need to control the proliferation of weapons technology has not. The new security environment is much more ambiguous and the list of potentially dual-use technologies much more comprehensive.

As a result of globalization, complex crisis phenomena and diffuse enemy images have emerged, which are confronted by a modernized military with concepts of "extended security" (Scheffran 2008). Societies are drawn into interconnected wars that provide a justification for new armament and connect civilian and military infrastructures. Without clear dividing lines, armed forces act in boundless wars, against all attempts of non-proliferation and arms control which are increasingly obstructed by confrontation among the major powers. This is accompanied by a privatization of security services and modern mercenary armies. Fractioning the structures of violence inflicts great suffering on the civilian population, destroying social and political structures, and creating new sources of dissatisfaction and violence through networks from the local to the global level.

2. CONFLICTS AS DRIVERS OF THE ARMAMENT DYNAMICS

Today's crises and conflicts create new justification for armaments and military interventions. New technicised wars project comprehensive networking, robotization, and automation of the battlefields in air, water, and on the ground, in space and cyberspace (Springer 2018), right through to the hybrid wars on the home front, in social networks, and in the media world (W&F 2019). This concerns modern transport, information and communication systems across the globe as well as micro, nano- and biotechnologies in the smallest spaces. Digitization and artificial intelligence combine globalization with the miniaturization of violence, as manifested in the information wars on our computers as well as in the projected war of drones, robots and killer microbes (Reuter 2019). As a result, the war is moving into our neighbourhoods, homes and human bodies, which are interwoven with global structures through technical systems. In this way, global (in-)security and human (in)security are linked.

Interventions with high-tech armaments find their counterpart in post-modern forms of violence and terrorist networks that use civilian structures for destructive purposes. Airplanes, vehicles, ships, reactors, the chemical industry, the Internet or power grids can not only be the target of violence, but can also be weapons of their own, thanks to the amplification effect of technical systems. Accordingly, the war against terrorism pervades Western societies. The Internet gives civilians access to vast amounts of information that makes them potential combatants in cyber warfare. When the entire society is affected by hybrid conflicts, the classic division between soldier and citizen loses its importance. Civil-military cooperation gives the military new leeway to include civilian resources (Scheffran 2018).

3. Preventive arms control and technology assessment

A response to the challenges, calls for technology assessment combined with a realistic analysis of the threat, with a view on reducing the extent to which investments in new technology may increase the danger of weapons proliferation. The consequence would be a more streamlined approach towards technology control that restrains the most dangerous technologies and seeks international cooperation in other fields of dual-use technologies. A similar approach between "shield or share" (Stowsky 2003) has been suggested to manage the transfer of dual-use of technologies and demonstrate how practical measures could stimulate the transition from a confrontational relationship to one which would be based on cooperation. Initiatives would involve confidence- and security-building measures and a multilateral agreement, to ensure the transfer of dual-use technologies while curbing destabilising military use. Where to draw the line depends on political attitudes and the security context.

In order to escape the logic of interconnected wars, alternatives are needed to break up ambivalences (Scheffran 2018). Since the criticism of military intentions is often countered by reference to possible civilian benefits, it is important to ask for alternatives with less military relevance and more civilian benefits (Scheffran 1997). In addition to the concept of preventive arms control (Altmann et al. 1998), an ambivalence analysis is helpful, which contributes to more transparency at the interface of civil-military research and development and identifies nodes where development paths can be separated on the basis of concrete parameters, as is usual in armaments and export control (EC 2015). In doing so, differences between civil and military need to be made clearer rather than blurred, and the social and international framework conditions of decision-making processes are to be revealed (Liebert, Rilling & Scheffran 1994). Hence civilian structures in the area of science and technology should be strengthened, and the educational impulse of science as well as the widespread rejection of open military research in the scientific community. Important is the public discussion on such issues, related to the civil clause movement (Braun et al. 2015). Ultimately, it is about a science that works on social tasks and alternatives and is oriented towards the goals of a peaceful, sustainable and just world.

4. The case of missile and space technologies

Important questions to be examined on the basis of specific case-by-case analyses concern the soundness, consistency and efficiency of armament programs. The general framework can be demonstrated for space and missile technologies (Scheffran 2006). Conditions have also changed for space systems and related rocket technologies. With the increasing privatization and commercialization of outer space and the emphasis on missile defence and space dominance, spaceflight moved again to the centre of the international security debate (Bulletin 2019). The “missile threat” from emerging military powers such as Iran, North Korea, India and Pakistan combines and competes with the nuclear threat. In both fields, dual-use is an essential problem that requires international control efforts to diminish the security risks. For proponents of missile defence and space dominance, outer space is inextricably linked to warfare, which would preclude any international control. For others, outer space is a common heritage of mankind that needs to be protected by international law for peaceful and sustainable uses (Bender et al. 2001). A Code of Conduct to strengthen space security has been suggested as well as a multilateral “Treaty on Common Security in Outer Space” and a prohibition of space weapons with multilateral satellite monitoring and verification systems as well as a protective regime for peaceful space objects based on immunity rules for satellites, such as a ‘rules of the road’ (Hagen & Scheffran 2003). Such political and legal frameworks need to be combined with concepts for preventive arms control that tackle the dual-use problem in the early phases of research and development.

References

Altmann, J., Liebert, W., Neuneck, G. & Scheffran, J. (1998). Preventive Arms Control as a Prerequisite for Conversion of Military-Related R&D. In: Reppy, J., Rotblat, J., Holdren, J. & Avduyevsky, V. (Eds.), *Conversion of Military R&D.* London/New York: Palgrave Macmillan, pp. 255-271.

Altmann, J., Bernhardt, U., Nixdorff, K., Ruhmann, I. & Wöhrle, D. Eds. (2017). *Naturwissenschaft – Rüstung – Frieden*. (2nd ed.). Wiesbaden: Springer.

Bender, W., Hagen, R., Kalinowski, M., Scheffran, J. Eds. (2001). *Space Use And Ethics*. Münster: Agenda-Verlag.

Brauch, H.G., van de Graaf, H.J., Grin, J. & Smit, W., Eds. (1992). *Controlling the Development and Spread of Military Technology*. Amsterdam: VU University Press.

Braun, R., Bultmann, T., Förster, et al. (2015). Zivilklauseln – Lernen und Forschen für den Frieden. *Wissenschaft & Frieden*, Dossier No. 78.

Bulletin (2019) Space: Military frontier or arms control opportunity? Special issue, *Bulletin of the Atomic Scientists,* 75(4), July.

European Commission/EC (2015). *Data and information collection for EU dual-use export control policy review*. Final report, written by SIPRI and Ecorys, 6.11.2015.

Hagen, R. & Scheffran, J. (2003). Is a space weapons ban feasible? Thoughts on technology and verification of arms control in space. *UNIDIR Disarmament Forum* 1/2003: 42-51.

Liebert, W., Rilling, R. & Scheffran, J., Eds. (1994). *Die Janusköpfigkeit von Forschung and Technik*: *Zum Problem der zivil-militärischen Ambivalenz.* Marburg: BdWi-Verlag.

Neuneck, G. & Alwardt. C. (2008). The revolution in military affairs: Its driving forces, elements, and complexity. *Complexity* 14(1): 50-61.

Reuter, C, Ed. (2019). Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden: Springer.

Scheffran, J. (2006). Dual-Use in a New Security Environment - The Case of Missiles and Space. *INESAP Information Bulletin* No.26 (June): 48-53.

Scheffran, J. (2008). The Complexity of Security. *Complexity* 14(1):13-21.

Scheffran, J. (2018). Militarisierung oder Zivilisierung? - Ambivalenz der Wissenschaft in der Krise. *Wissenschaft & Frieden* 2/2018: 15-20.

Springer, P.J. (2018). Outsourcing War to Machines: The Military Robotics Revolution. Praeger Security International.

Stowsky, J. (2003). *Secrets to Shield or Share? New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age*, BRIE Working Paper 151.

W&F (2019) Hybrider Krieg? Special Issue, Wissenschaft & Frieden, 3/2019 (September).

The Stewardship Race

ALFRED NORDMANN

INSTITUTE FOR PHILOSOPHY, TECHNISCHE UNIVERSITÄT DARMSTADT

[#44-PAPER]

ABSTRACT

The following pages outline a research program for IANUS in the coming years. It is not the only research program for IANUS but one that sets it apart from other forms of science-and-engineering-based peace research. It is meant to complement and contextualize current IANUS-related work on software engineering and cybertechnologies as well as work elsewhere on nuclear or biotechnologies. To the extent that it is addressed to natural scientists and engineers, this research program offers a timely perspective for collaborative work in the spirit of IANUS, FONAS or UCS – but one that goes beyond the consideration of weapons systems or specific technologies and their military or civilian use. [1] The ambition to offer a timely perspective is the ambition to engage specifically in the historical situation of the early 21st century. This ambition is at risk of course. Still, in the midst of identifying new challenges, we might find ourselves cast into yet another world which poses a whole new set of problems.

1. THE SITUATION

The Bradbury Science Museum is “Your Window into Los Alamos National Laboratory”. To the visitor who enters it physically or by way of its URL (www.lanl.gov) it is readily apparent that one is not looking from the outside in. Instead, visitors are drawn into the insider’s perspective. The museum speaks for the National Laboratory and serves to underscore its demonstration of nuclear power, capability, and might. But this demonstration is not one of military or strategy might, it does not concern a stockpile of arms and the capacity to strike here or there around the globe. In more ways than one the museum is a window into the Laboratory’s mission of “Stockpile Stewardship”, that is, the “mission to solve national security challenges through scientific excellence.”

The museum helps us understand what this means. The scientific excellence in question is not that of building and assembling nuclear weapons and their delivery systems. It is excellence at

[1] The programmatic proposal evolved from IANUS discussions over the last several years. As such, it has many authors who should be mentioned, among them Matthias Englert, Jens Geisse, Anne Harrington, Annette Ripper, Christina Schües, and Sonja Schmid. — Like most programs or manifestos, the following text is short on references to the scientific literature.

producing meaningful information from indirect evidence. This is how the problem is stated: We (the Los Alamos National Laboratory) need to report to the President of the United States about the quality and readiness of the nuclear arsenal – but we must do so without the benefits of actual tests. Therefore, we need to accrue immense knowledge of materials and how they age, and we need to bring this knowledge into highly complex simulations not of the "theatre of war" but of the conditions over time of fissile material, its casings, its storage methods. A highly generalized yet greatly advanced engineering and modelling competence is required to stay on top of things as they just sit around in their storage facilities.

"Stockpile stewardship" thus amounts to very general as well as specific capacities of maintenance, monitoring, and management. Not only the President but the whole world has to trust that the stockpile is in good hands with the scientists at the National Laboratory – safe in times of peace, ready for times of war. In a democratic society, this includes social technologies of communication and debate – the Bradbury Science Museum exhibits those just like any other modern museum of science and technology. Not only does it demonstrate the basis of trust in scientific excellence, but it also provides space in the exhibition for critics of their program, including citizen groups in New Mexico who worry about the lab in their backyard. "We hear you," the National Laboratory appears to be saying, "and thus we confidently include you in our mission of being good stewards of a dangerous technology in a precious and vulnerable environment."

A film in the museum finally features the long-term legacy and vision of the Los Alamos National Laboratory. Eloquent testimonials are provided especially by former Secretary of State William Perry, one of the so-called "Four Horsemen" who have been promoting a World Free of Nuclear Arms. Even once we have achieved this goal, Perry says in the film, we will need the Los Alamos National Laboratory, perhaps more so than ever. For, when the arms have vanished from view entirely and are no longer physically present, the competence of building and maintaining and monitoring nuclear arms must not be lost. It is the ultimate deterrent – now and in the future.

Though it may seem like a long time ago, William Perry's promise of a World Free of Nuclear Arms was taken up by Barack Obama. And quite in line with Perry and his compatriots, Obama also saw the need to underwrite this promise by strengthening engineering competence not only in the field of nuclear engineering.

Nuclear disarmament, in other words, goes along with the armament of civil society – which remains a civil society but which has to now shoulder all the responsibilities of good stewardship. It must be a society that can handle dangerous materials and technologies, that is resilient in times of economic, environmental, or infrastructural crisis, that is not only a knowledge-society but has learned to deal with the limits and absence of knowledge, that does not delegate questions of security to its politicians and questions of safety to its engineers, but that evolves a comprehensive "safety culture". It is by its safety culture that a nation is tested and judged, fairly or not. On the assumption that a good safety culture can thrive only in an open and just and democratic society, fissile materials cannot be entrusted, supposedly, to certain countries like North Korea or the Iran. And on the assumption that Germany has advanced engineering capabilities and stewardship skills as well as a resilient civic culture, it is in effect a nuclear power just like the United States. Possessing nuclear arms or not is no longer the decisive criterion at a time when the arms race has been superseded by the stewardship race which revolves around demonstrations of scientific and economic, managerial and socio-technical capability. The self-imposed criterion of excellence by the leaders in the stewardship race amounts to the simple question: "Is this a safe country for dangerous technologies and destructive capabilities – are these technologies in good hands, in the right hands?"

2. THE PROBLEMS

It is one thing to identify and analyse the stewardship race, quite another to critique and, ideally, to orient, constrain, or otherwise influence it. It is not openly conducted as a "race" – or only to the extent that the capabilities in question also protect markets and gain advantage in a global marketplace. [2] Also, the capabilities in question are not subject to disarmament. A militarized society where citizen decide to police their nation and exhibit belligerence might be pacified and civilized – with programs to trade guns for cell-phones, with incentives for public transportation as opposed to individualized Humvees. In contrast, a well-developed safety culture is generally seen to be a good thing as citizens take responsibility and monitor the operation of critical technologies in their environment – even if this is the best defence against attacks on infrastructure and even if this implies the gathering of know-how on launching such attacks – working knowledge of highly complex socio-technical systems, in particular, knowledge of security breaches and their manageability are major elements of the stewardship race.

Even though the development of stewardship capabilities and an attendant safety culture are all-encompassing and highly prized, it is necessary to develop a critical stance that acknowledges the predicament. On the one hand, the question "Does our society provide a safe operating environment for highly complex, potentially dangerous technologies?" needs to be raised and its answer not simply presumed: What are the criteria for arguing that technologies which pose risks for safety and security are in good hands with our police, our intelligence community, our army, our regulatory system, our organization of industrial processes, or our import/export rules and regulations? On the other hand, the problematic assumptions need to be exposed which lead us to raise the questions in the first place.

The prominence of the question owes to an abdication of politics, that is, of deliberate and negotiated mechanisms for building trust, e.g., by way of lawful relations and legal instruments such as treaties, agreements, commitments and public scrutiny. The wide distribution of responsibility throughout safety cultures is to offer a technological and managerial compensation for this abdication of politics – which, arguably, cannot be compensated.

- As we may be witnessing today, the international system of security is becoming more vulnerable to erratic action that eludes an all too subtle game of deterrence through preparedness or stewardship.

[2] A more detailed presentation would highlight the ways in which countries like China demonstrate good stewardship in order to participate in the global economy and gain reputation as a trustworthy actor on the international stage.

- The stewardship race delivers a sense of safety and security at the national level but is constantly challenged as to its legitimacy when one nation claims, in effect, cultural superiority over another, and similarly when states claim to have achieved the always impeachable status of providing a safe, reliable, trustworthy operating environment.
- In the meantime, individual engineers, workers, citizens as contributors to and presumed guarantors of the safety culture are underprepared for their role and overtaxed by it – they have to function reliably to ensure the maintenance of safely operating socio-technical systems and are at the same time committed to shift gear at any time from the position of permanent heightened vigilance to that of whistleblowing.

3. THE AGENDA

On the basis of this diagnosis, where is a research program for IANUS and for science-and-engineering based peace research? Only a few points can be mentioned here in a very preliminary fashion:

- The diagnosis does not allow for a limited focus on particular weapons systems and their development. In fact it does not provide a meaningful differentiation between an aggressive and defensive stance or even for the distinction between war and peace: Those who are engaged in the stewardship race might be interested in peace but in a permanent state of war, vying to be a most developed safety culture that is trustworthy within society and the global community and that is able to absorb significant shocks to the system.
- Assuming that responsible stewardship aims to preserve or create peace, one of the main questions is to ask what it means for technological development and an articulated safety culture to be committed to the value of peace. Just as we may ask what are the criteria for judging an engineering approach to be "sustainable", we should take on the question of how to evaluate a safety culture as one that adheres to „peace" as a public value. The discussion of how *Sicherheitskultur* can be transformed into a *Friedenskultur* may well involve the European Commission or national research councils in the task of establishing "peace" as a core (European) value for Responsible Research and Innovation (RRI).
- Redundancy and independence/autonomy (German: *Autarkie*) are technical and managerial virtues for safe-guarding critical infrastructures. An international system of safety and security, in contrast, relies on mutual commitments and dependencies. Is the best way to make ourselves less vulnerable really to shut ourselves off as far as possible – to achieve total self-sufficiency and isolation if necessary? This question implies that one needs to discuss gas-pipelines from Russia to Germany or the Chinese construction of the 5G networks for advanced industries in the context of science-and-engineering-based peace research. Some worry about these as unacceptable vulnerabilities, others see them as guarantors of peaceful mutual relations. This may turn out to be question of design – how to design contractual relations, how to ensure mutuality, how to design the collaboration of engineers and of the technical structure itself – how to evolve a transnational safety culture.

The abdication and restitution of politics and diplomacy, the integration of “peace” into the canon of RRI, the design of transnational socio-technical systems, the criteria for peace-oriented safety cultures (i.e., *Friedenskulturen*), the education and socialization of engineers, managers, citizens that are to sustain these cultures – all of this requires the active participation of scientists and engineers along with peace researchers and philosophers of technology. IANUS should provide a forum for this, one that encompasses international research activities and dialogue on the one hand, practical engagement with a new generation of citizen-scientists and engineers on the other hand.

APPENDIX

Group Photo

Group photo of the 100 conference participants from over 50 organizations, ranging from the natural and engineering sciences (physics, biology, chemistry, computer science) to the humanities and social sciences (political science, peace and conflict research, psychology, philosophy).

Visual Impressions from the Conference

PEASEC
fonas
Forschungsverbund Naturwissenschaft, Abrüstung und internationale Sicherheit

Opening of the conference by Prof. Christian Reuter (TU Darmstadt) with Prof. Malte Göttsche (RWTH Aachen), Dr. Jürgen Altmann (TU Dortmund) and Dr. Mirko Himmel (University of Hamburg) (from left to right)

IFSH
Three Decades of Chemical Weapons Destruction: Lessons for WMD Abolition
Paul F. Walker, Ph.D.
Senior Visiting Fellow
Institute for Peace Research and Security Policy (IFSH)
University of Hamburg, Germany
Science, Peace, Security 19
TU Darmstadt, Germany
PEASEC
fonas

Keynote by the American chemical weapons expert Dr. Paul F. Walker, winner of the Right Livelihood Award, Director of the International Green Cross and currently Senior Visiting Fellow at IFSH in Hamburg

PEASEC
TECHNISCHE UNIVERSITÄT DARMSTADT

PEASEC

IANUS

PEASEC

PEASEC

PEASEC
TECHNISCHE UNIVERSITÄT DARMSTADT

PEASEC
of U.S. Nonprolifera
on ROK Nuclear Dev

PEASEC
TECHNISCHE UNIVERSITÄT DARMSTADT
Wissenschaft und Technik für Frieden

PEASEC

PEASEC
TECHNISCHE UNIVERSITÄT DARMSTADT
Wissenschaft und Technik für Frieden und Sicherheit

PEASEC

PEASEC
TECHNISCHE UNIVERSITÄT DARMSTADT

Thea Riebe · Marc-André Kaufhold · Taru
Thomas Reinhold · Christian Reuter
PEASEC

PEASEC
TECHNISCHE UNIVERSITÄT DARMSTADT