S+F Sicherheit und Frieden
Security and Peace

1 2020
38. Jahrgang
ISSN 0175-274X

Nomos

Themenschwerpunkt / Thematic Focus:
Interdisciplinary Contributions to Natural Science/ Technical Peace Research
Interdisziplinäre Beiträge zur naturwissenschaftlich-technischen Friedensforschung

Schriftleitung:
Prof. Dr. Ursula Schröder, Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Redaktion:
Dr. Patricia Schneider (V.i.S.d.P.), Chefredakteurin, Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, schneider@ifsh.de
Susanne Bund, Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, bund@ifsh.de
FKpt Prof. Frank Reininghaus, Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, reininghaus@ifsh.de
Dr. Sybille Reinke de Buitrago, Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, reinkedebuitrago@ifsh.de
ORR Dr. iur. Tim René Salomon, LLM. (Glasgow), Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg; tim.salomon@law-school.de

Redaktionsanschrift:
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg
S+F Redaktion
Beim Schlump 83
20144 Hamburg
Germany
Telefon: +49 – 40 / 86 60 770
Fax: +49 – 40 / 86 60 77-88
Mail: SundF@ifsh.info
Homepage der Zeitschrift: www.sicherheit-und-frieden.nomos.de
Erscheinungsweise: 4 Ausgaben pro Jahr
Bezugspreise 2020: Jahresabonnement incl. Online Privatbezieher 98,– €, Institutionen 198,– €, Studenten und Arbeitslose (jährlicher Nachweis erforderlich) 65,– € ; Einzelheft 30,– €. Alle Preise verstehen sich incl. MWSt, zzgl. Vertriebskostenanteil. 13,00 € plus Direktbeorderungsgebühr Inland 1,65 € p.a.
Bestellmöglichkeit: Bestellungen beim örtlichen Buchhandel oder direkt bei der Nomos Verlagsgesellschaft Baden-Baden
Kündigungsfrist: jeweils drei Monate vor Kalenderjahresende
Bankverbindung generell: Zahlungen jeweils im Voraus an Nomos Verlagsgesellschaft, Postbank Karlsruhe: BLZ 660 100 75, Konto Nr. 73636-751 oder Sparkasse Baden-Baden Gaggenau: BLZ 662 500 30, Konto Nr. – 5-002266

Druck und Verlag:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestr. 3-5, D-76530 Baden-Baden
Telefon (07221) 2104-0/Fax (07221) 2104-27
E-Mail nomos@nomos.de

Anzeigen:
Sales friendly Verlagsdienstleistungen, Inh. Frau Bettina Roos, Pfaffenweg 15, 53227 Bonn
Telefon (0228) 978980 Fax (0228) 9789820
E-Mail roos@sales-friendly.de

ISSN 0175-274X

S+F Sicherheit und Frieden
Security and Peace

38. Jahrgang, S. 1–63
1/2020

S+F lädt Autorinnen und Autoren zur Einsendung von Beiträgen zur Veröffentlichung ein

S+F ist die führende deutsche Fachzeitschrift für Friedensforschung und Sicherheitspolitik. **S+F** will Forum der Kommunikation für Wissenschaft und Politik, zwischen ziviler Gesellschaft und Streitkräften sein, in dem Analyse, Insiderbericht, Standortbestimmung und Einschätzung Platz haben. Entscheidend für die Veröffentlichung ist der Beitrag eines Textes zu nationalen und internationalen Diskussionen in der Sicherheitspolitik und Friedensforschung, von naturwissenschaftlichen Aspekten der Rüstungskontrolle bis zu Fragen der Nationenbildung in Nachkriegsgesellschaften. Jedes Heft von **S+F** ist einem Schwerpunktthema gewidmet. Neben Beiträgen zum Schwerpunkt werden aber auch Texte zu allgemeinen Themen der Sicherheitspolitik und Friedensforschung veröffentlicht.

Autorinnen und Autoren haben die Wahl zwischen Beurteilung der Texte durch Herausgeber und Redaktion oder einem zusätzlichen Begutachtungsverfahren mit externen Gutachtern (peer-reviewed, anonymisiert). Dieses Verfahren nimmt mehr Zeit in Anspruch (zur Erstellung der Gutachten, für die Überarbeitung etc.). **S+F** strebt an, den Anteil der extern referierten Aufsätze zu erhöhen, wird aber auch weiterhin Texte veröffentlichen, deren Qualität von der Redaktion und dem für ein Heft verantwortlichen Herausgeber beurteilt wurde. Die nachfolgend angegebenen „Deadlines" gelten für die Einreichung von Beiträgen im Rahmen der jeweiligen Schwerpunktthemen. Aufsätze zu Themen außerhalb der Schwerpunkte können jederzeit eingereicht werden.

Call for Papers/ Herausgeber und Redaktion rufen zur Einsendung von Beiträgen auf

2/2020: Friedensstörer oder Dealmaker? US-Sicherheits- und Außenpolitik nach vier Jahren Präsidenschaft Trumps, *Deadline 15. Juni 2020*

3/2020: Friedenslogik – Idee, Praxis, Kritik, *Deadline 22. Juni 2020*

Für die „Beiträge aus Sicherheitspolitik und Friedensforschung" und das „Forum" ist S+F fortlaufend auch an Artikeln außerhalb des jeweiligen Themenschwerpunkts interessiert.

Texte können in englischer oder deutscher Sprache verfasst sein und sollten 25.000 bis 30.000 Zeichen (inkl. Leerzeichen) umfassen. Weitere Hinweise für Autorinnen und Autoren finden sich auf der Webseite der Zeitschrift unter „Autorenhinweise".

Bitte richten Sie Ihre Fragen an:
E-mail: SundF@ifsh.info
Website: http://www.sicherheit-und-frieden.nomos.de

S+F invites authors to submit suitable papers for publication

S+F is the leading German journal for peace research and security policy. **S+F** aims to serve as a forum of analysis, insider reports and opinion pieces for research and politics linking civil society and the armed forces. Decisions on publication are made on the basis of the contribution of a text to national and international discussions on peace and security issues, considering scientific aspects of arms control to questions of nation-building in post-war societies. Every issue of **S+F** is focused on a particular theme. In addition, texts addressing general aspects of security policy and peace research are also published.

Authors can choose to have the text evaluated by the publisher and editorial team or by an external evaluation process (double-blind peer-review), the latter is more time intensive (for the evaluation process, revision, etc.). **S+F** intends to increase the number of externally evaluated contributions but will continue to publish texts which have been assessed by the editorial team and the publisher responsible for the issue. The deadlines listed below are for contributions for a specific theme. Contributions on other topics can be made at any time.

Call for Papers/ Publisher and editorial team call for contributions

2/2020: Peacebreaker or Dealmaker? US Security and Foreign Policy after Four Years under President Trump, *Deadline 15. June 2020*

3/2020: Peace Logic – Idea, Practice, Criticism, *Deadline 22. June 2020*

Outside the special focus topic, S+F also welcomes submissions under the sections "Contributions to Security Policy and Peace Research" and "Forum".

Texts may be written in English or German and should be between 25,000-30,000 characters long (incl. spaces). Further information for authors can be found on the magazine website under "Notes to Authors".

Please direct your queries to:
E-mail: SundF@ifsh.info
Website: http://www.sicherheit-und-frieden.nomos.de/?L=1

Die Artikel der Zeitschrift **S+F** werden in mehreren nationalen und internationalen bibliografischen Datenbanken nachgewiesen. Dazu gehören u.a. Online Contents OLC-SSG Politikwissenschaft und Friedensforschung, PAIS (Public Affairs Information Service) International Database, Worldwide Political Science Abstracts und World Affairs Online (hrsg. vom Fachinformationsverbund Internationale Beziehungen und Länderkunde FIV) (siehe auch www.ireon-portal.de).

Articles of the journal **S+F** are entered in various national and international bibliographic databases. Among them are Online Contents OLC-SSG Politikwissenschaft und Friedensforschung (Political Science and Peace Research), PAIS (Public Affairs Information Service) International Database, Worldwide Political Science Abstracts and World Affairs Online (by the Fachinformationsverbund Internationale Beziehungen und Länderkunde FIV/The German Information Network International Relations and Area Studies) (see also www.ireon-portal.de).

Editorial: Interdisziplinäre Beiträge zur naturwissenschaftlich-technischen Friedensforschung

2019 veröffentlichte der Wissenschaftsrat, das wichtigste wissenschaftspolitische Beratungsgremium in Deutschland, seine Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung und zur dringenden Notwendigkeit, die naturwissenschaftlich-technische Friedens- und Konfliktforschung zu stärken. Wissenschaftliche Entdeckungen und technologische Innovationen haben schon immer großen Einfluss auf Frieden und Sicherheit ausgeübt.

Heute prägen Ereignisse wie der mögliche Zusammenbruch des Iran-Abkommens, Diskussionen über autonome Waffensysteme oder Cyber-Bedrohungen das aktuelle weltpolitische Geschehen. Nukleare Rüstungskontrolle und Abrüstung sind gefährdet, neue Technologien verändern soziale und politische Verhältnisse. Somit gewinnt die naturwissenschaftlich-technische Friedensforschung an Bedeutung. Auf Grundlage vorhandener Erkenntnisse aus unterschiedlichen Disziplinen (wie z.B. Physik, Biologie, Chemie und Informatik) befasst sich diese Forschung mit der Rolle der naturwissenschaftlichen und technischen Möglichkeiten im Kontext von Krieg, Frieden, Auf- und Abrüstung.

Diese Zusammenstellung verschiedener Artikel, die auf die Darmstädter Konferenz SCIENCE – PEACE – SECURITY '19 aufbaut, bietet gute Einblicke in die aktuelle Forschung. Darüber hinaus möchte diese Ausgabe das Verständnis bestehender Herausforderungen im Bereich Frieden und Sicherheit erhöhen. Sie enthält naturwissenschaftliche, technische und interdisziplinäre Beiträge aus verschiedenen Forschungsbereichen. Nach zwei Begutachtungsrunden wurden folgende Beiträge ausgewählt.

Der einführende Beitrag „Natural Science and Technical Peace Research: Definition, History and Current Work“ beschreibt das Forschungsfeld, seine Geschichte und aktuelle Arbeit.

Der Beitrag „A Developing Arms Race in Outer Space? De-constructing the Dynamics in the Field of Anti-Satellite Weapons“ wurde von *Daniel Lambach* und *Arne Sönnichsen* verfasst. Die Autoren erklären, dass bestehende Ängste vor der Militarisierung des Weltraums oft zu technik-deterministischen Argumenten führen. Dieser Beitrag verfolgt einen sozialkonstruktivistischen Ansatz von Technik, um die Dynamiken des angeblichen Wettrüstens zu dekonstruieren.

Das Paper „Towards IT Peace Research: Challenges on the Intersection of Peace and Conflict Research and Computer Science“ von *Christian Reuter* verdeutlicht, dass Fortschritte in Wissenschaft und Technik, einschließlich der Informationstechnik, eine entscheidende Rolle für Frieden und Sicherheit spielen. Dieser Beitrag hebt die Notwendigkeit weiterer Arbeit in der „IT-Friedensforschung“ hervor.

Der Beitrag „The state of cyber arms control. An International Vulnerabilities Equities Process as the way to go forward?“ von *Matthias Schulz* analysiert Vorschläge zu Cyber-Rüstungskontrolle, die sich an traditionellen Rüstungskontrollregimen orientieren. Obwohl die Bedrohung durch Cyber-Konflikte zunimmt, ist bisher mit Cyber-Rüstungskontrollregimen nicht viel erreicht worden. Der Autor stellt fest, dass Herausforderungen innerhalb der digitalen Domäne, Verifikationsprobleme sowie fehlender politischer Wille große Hemmnisse für die Übertragung auf die Cyberdomäne darstellen.

Der Artikel „Cyber Threat Intelligence Sharing between States“ von *Philipp Kühn, Thea Riebe, Lynn Apelt, Max Jansen* und *Christian Reuter* untersucht Cyber Threat Intelligence-Plattformen, die im IT-Sicherheitsmanagement zur gemeinsamen Nutzung und Analyse von Cyber-Bedrohungen für ein kollektives Krisenmanagement eingesetzt werden. Im Beitrag wird darüber diskutiert, ob CTI-Plattformen zwischen Staaten und internationalen Organisationen als vertrauensbildende Maßnahmen eingesetzt werden können.

Der Beitrag „Towards a Prospective Assessment of the Power and Impact of Novel Invasive Environmental Biotechnologies“ von *Johannes L. Frieß, Anna Rößing, Gunnar Jeremias und Bernd Giese* untersucht neue Biotechnologien, nämlich Gene Drives und Horizontal Environmental Genetic Alteration Agents, die über die klassischen Anwendungen von gentechnisch veränderten Organismen hinausgehen. Der Beitrag betrachtet vorläufig die Eignung des derzeitigen rechtlichen Rahmens im Hinblick auf Konflikte, die sich aus der feindseligen oder wohlwollenden Nutzung dieser Technologien ergeben.

Das letzte Paper „New Military Technologies: Dangers for International Security and Peace“ von *Jürgen Altmann* behandelt neue militärische Technologien, die mit hohem Tempo entwickelt werden; die USA sind auf diesem Gebiet führend. Probleme für internationale Sicherheit und Frieden – Wettrüsten und Destabilisierung – werden sich wahrscheinlich aus den gemeinsamen Eigenschaften mehrerer Technologien ergeben: breitere Verfügbarkeit, leichterer Zugang, kleinere Systeme, kürzere Zeiten für Angriffe, Warnungen und Entscheidungen sowie konventionell-nukleare Verstrickung.

Zusammenfassend sind wir zuversichtlich, dass diese Themenschwerpunktausgabe einen Überblick über aktuelle Forschungsprojekte und Herausforderungen in der naturwissenschaftlich-technischen Friedensforschung gibt.

Außerhalb des Themenschwerpunktes analysiert *Sophie Scheidt* Gewissensentscheidungen im militärisch-operativen Planungsprozess bei der Anwendung militärischer Gewalt im Verhältnis zur Akzeptanz ziviler Schäden. *Julia Böcker* beschreibt Deutschlands andauernden Kampf mit der Aufarbeitung seiner vergangenen kolonialen Gräueltaten in Namibia.

Christian Reuter, Jürgen Altmann, Malte Göttsche, Mirko Himmel

Prof. Dr. **Christian Reuter** ist Inhaber des Lehrstuhls Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) an der Technischen Universität Darmstadt. Schwerpunkte: interaktive & kollaborative Technologien im Kontext der Sicherheits-, Krisen- und Friedensforschung.

PD Dr. **Jürgen Altmann** ist Privatdozent für Experimentelle Physik an der Technischen Universität Dortmund. Schwerpunkte: Militärtechnik-Folgenabschätzung von autonomen Waffensystemen; Fragen der naturwissenschaftlich-technischen Friedensforschung.

Prof. Dr. **Malte Göttsche** ist Juniorprofessor und Leiter der Forschungsgruppe „Nukleare Verifikation und Abrüstung“ an der RWTH Aachen. Schwerpunkte: nukleare Verifikationstechnologien, Strahlungstransportsimulationen; Abrüstungspolitik.

Dr. **Mirko Himmel** ist wissenschaftlicher Mitarbeiter am Carl Friedrich von Weizsäcker-Zentrum für Naturwissenschaft und Friedensforschung, Universität Hamburg. Schwerpunkte: neue, präventive Methoden zur Abwehr biologischer und chemischer Bedrohungen; bio-ethische Normen; effiziente Selbstregulierungsmechanismen.

Editorial: Interdisciplinary Contributions to Natural Science/Technical Peace Research

In 2019, the Science Council, the most important scientific-political advisory panel in Germany, published its recommendations on the further development of peace and conflict research and the urgent need to strengthen natural science/technical peace research. Scientific discoveries and technological innovations have always exerted a great influence on peace and security.

The possible complete breakdown of the Iran Agreement, discussions about autonomous weapon systems or cyber threats are shaping current world political events. Nuclear disarmament and arms control are in danger, and new technologies entail changes in social-political environments. Thus, natural science and technical peace research are gaining importance. On the basis of existing findings from various natural sciences and technical disciplines (such as physics, biology, chemistry and computer science), this research deals with the role of scientific and technical possibilities in the context of war, peace, armament, and disarmament.

This compilation of different articles, which is based on the conference SCIENCE PEACE SECURITY '19 in Darmstadt, gives good insights into current research. Furthermore, this special issue aims at enhancing the understanding of current peace and security challenges. It includes contributions from natural science, technical peace research as well as interdisciplinary contributions. After two rounds of peer review, the following articles have been accepted.

The first article, "*Natural Science and Technical Peace Research: Definition, History and Current Work*", describes the research field, its history and current work.

The article, "A Developing Arms Race in Outer Space? Deconstructing the Dynamics in the Field of Anti-Satellite Weapons", was written by *Daniel Lambach* and *Arne Sönnichsen*. The authors explain that existing fears of the militarization of space often lead to techno-determinist arguments. This article takes a Social Construction of Technology approach to deconstruct the dynamics of this supposed arms race.

The article "Towards IT Peace Research: Challenges on the Intersection of Peace and Conflict Research and Computer Science", by *Christian Reuter* explains that advances in science and technology, including information technology, play a crucial role in the context of peace and security. This article highlights the need for further work for "IT peace research".

The article "The State of Cyber Arms Control. An International Vulnerabilities Equities Process as the Way to go Forward?", by *Matthias Schulze* analyses proposals for cyber arms control, modelled after traditional arms control regimes. Although the threat of cyber-conflict rises, not much ground has been gained with cyber arms control regimes. The author finds that challenges of the digital domain, issues of regime verification and the lack of political will are significant inhibitors in transferring these to the cyber-domain.

The article "Cyber Threat Intelligence Sharing between States", by *Philipp Kühn, Thea Riebe, Lynn Apelt, Max Jansen* and *Christian Reuter* investigates Cyber Threat Intelligence (CTI) platforms which are used in IT-security management to share and analyse cyber threats for a collective crisis management. The article discusses whether or not CTI platforms can be used as a confidence-building measure between states and international organizations.

The article "Towards a Prospective Assessment of the Power and Impact of Novel Invasive Environmental Biotechnologies", by *Johannes L. Frieß, Anna Rößing, Gunnar Jeremias and Bernd Giese* examines new biotechnologies, namely gene drives and Horizontal Environmental Genetic Alteration Agents, which exceed classical applications of genetically modified organisms. This article preliminarily examines the suitability of the current legal framework with regard to conflicts arising from the hostile or benevolent use of these technologies.

The last article, "New Military Technologies: Dangers for International Security and Peace", by *Jürgen Altmann* focuses on new military technologies that are being developed at a high pace, with the USA in the lead. Problems for international security and peace – arms races and destabilisation – will likely result from properties shared by several technologies: wider availability, easier access, smaller systems; shorter times for attack, warning and decisions; and conventional-nuclear entanglement.

In sum, we are confident that our special issue contains an overview of current research projects and challenges in natural science and technical peace research.

Outside the thematic focus, *Sophie Scheidt* analyses decisions of conscience in the military operational planning process in the use of military force in relation to the acceptance of civil damage. *Julia Böcker* describes Germany's ongoing struggle to come to terms with its past colonial atrocities in Namibia.

Prof. Dr. **Christian Reuter**, full professor for Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt. Focus: interactive and collaborative technologies in the context of crises, security, safety, and peace.

PD Dr. **Jürgen Altmann**, head of the research group on Physics and Disarmament at TU Dortmund. Focus: military-technology assessment of automated and autonomous weapon systems; questions related to natural science and technical peace research.

Prof. Dr. **Malte Göttsche**, assistant professor and head of the Nuclear Verification and Disarmament Group at RWTH Aachen. Focus: nuclear verification technologies, related simulation tools, radiation detection and non-proliferation and disarmament policy.

Dr. **Mirko Himmel**, scientist at the Carl Friedrich von Weizsäcker-Centre for Science and Peace Research, University of Hamburg. Focus: technologies for preventive biological and chemical arms control; infectious biology; bioethics.

S+F Sicherheit und Frieden
Security and Peace
1 2020
38. Jahrgang
S. 1–63

THEMENSCHWERPUNKT

Natural Science and Technical Peace Research: Definition, History, and Current Work

Christian Reuter, Jürgen Altmann, Malte Göttsche, Mirko Himmel

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 uninhabited weapon systems. Issues of nuclear disarmament, missile defence or space armament as well as chemical and biological weapons remain 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 natural science/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. This special issue presents selected contributions based on discussions at the conference.

Keywords: Natural Science/Technical Peace Research, Computer Science, Peace and Conflict Studies
Schlagwörter: Naturwissenschaften/Technische Friedensforschung, Informatik, Friedens- und Konfliktforschung

1. Introduction

In July 2019, the Science Council, 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 natural science/technical peace and conflict research, which in Germany is now structurally too precarious to meet the massive need for policy advice.[1] Scientific discoveries and technological innovations have always exerted a great influence on peace and security.[2] New civil and military technologies are

1 Wissenschaftsrat, 'Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung (Drs. 7827-19)', 2019, 1–178.
2 Jürgen Altmann, Ute Bernhardt, and others, *Naturwissenschaft – Rüstung – Frieden*, Wiesbaden: Springer VS, 2017.

DOI: 10.5771/0175-274X-2019-4-1

revolutionizing warfare.[3] To address these challenges to peace and security by academic research requires an interdisciplinary approach. For example, issues of cyber-attacks or cyber-weapons must be addressed by computer science and political science, among others.

The ending of the Intermediate-Range Nuclear Forces Treaty, the use of chemical weapons in Syria, discussions about autonomous weapons systems or cyber threats are shaping current world political events. Especially in these days, in which nuclear, biological and chemical disarmament and arms control are facing major challenges and new technologies entail changes in social-political environments, natural science and technical peace research is gaining in importance. On the basis of existing findings from various natural sciences and technical disciplines (e.g. physics, chemistry, biology, computer science), natural science/technical peace research deals with the role of scientific and technical possibilities in the context of war, peace, armament and disarmament.[4]

Inspired by different approaches toward the above-mentioned topics, this compilation of different articles, which is based on the conference SCIENCE · PEACE · SECURITY '19 in Darmstadt[5], gives good insights into current research. Furthermore, this special issue on natural science/technical peace research wants to enhance the understanding of current peace and security challenges. Therefore, it includes natural science, technical as well as interdisciplinary contributions from different fields of research, focusing on international security and peace.

2. Definition and History of Natural Science/ Technical Peace Research

Within the interdisciplinary field of peace and conflict research, technology, based on findings from various natural sciences and technical disciplines (e.g. physics, chemistry, biology, computer science), plays a key role in various forms of conflict resolution[6].

Peace and conflict studies researches peace and war on the basis of scientific methods and theories from several relevant disciplines, as war and conflicts have almost always been present in humankind.[7]

Natural science/technical peace research is a broad field of research that deals with the role of natural scientific and technical possibilities in the context of war and peace, armament and disarmament.

The latter came into being with the development and proliferation of nuclear weapons in the East-West conflict since the 1940s.[8] With the possibility of using nuclear weapons in war, scientific and technological innovations became strategically and politically relevant. Despite many public concerns, deterrence became the means of first choice. The best-known example of existing doubts from science is the „Russell-Einstein Manifesto" from 1955, which calls for nuclear disarmament and a rejection of war in general. As a result, the Pugwash Conferences on Science and World Affairs were established. At the first conference in 1957 in Pugwash, Canada, 22 scientists from ten countries and from both sides of the Iron Curtain discussed strategies for nuclear disarmament. Ever since, the so-called „Pugwash Movement" has been organizing workshops and conferences and conducting research concerning problems of nuclear weapons. A similar development occurred in West Germany with the „Göttingen Declaration" of 1957, when leading physicists and chemists rejected the German government's demand for nuclear armament for the newly founded German military, the *Bundeswehr*. The Pugwash activities formed an important basis that enabled and supported subsequent international treaties on arms control. Based on such initiatives, scientific research groups were founded at renowned US universities in the 1960s. During the East-West conflict they investigated nuclear disarmament, arms control, non-proliferation and international security. In Germany, Carl Friedrich von Weizsäcker (by that time at the University of Hamburg) established a research centre on global issues. He can thus be considered as the founding father of the country's scientific and technical peace research.

In the 1980s, the first small German working groups were founded in Bochum, Darmstadt, Hamburg and Kiel. Since then, internationally renowned competencies have been built up. Within those groups, young researchers started to work in natural science/technical peace research and performed research on security policy implications of technologies. Furthermore, they became familiarized with associated interdisciplinary research methods. Highlights of this long-term development were the founding of the Research Association for Science, Disarmament and International Security (FONAS) in 1996, and the establishment of the first endowed professorship in the field of scientific peace research in 2006 at the Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF) at the University of Hamburg. In 2010, the endowed professorship for Science and Technology for Peace and Security in the Department of Biology at the Technical University of Darmstadt was filled, but only for a few months. Seven years later, in 2017, a corresponding professorship was filled in the Department of Computer Science at the same university. Nowadays, only these two locations have university professorships in natural science/technical peace research. Furthermore, there is a junior professorship at the Rheinisch-Westfälische Technische Hochschule (RWTH) Aachen as well as other positions in peace research institutes, most of which with a political science focus. Nevertheless, research in this area is very much needed. [9]

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

4 Christian Reuter and others, 'Zur Naturwissenschaftlich-Technischen Friedens- und Konfliktforschung – Aktuelle Herausforderungen und Bewertung der Empfehlungen des Wissenschaftsrats', *Zeitschrift für Friedens- Und Konfliktforschung (ZeFKo)*, 2020.

5 Christian Reuter and others, *SCIENCE PEACE SECURITY '19 – Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research* (Darmstadt, Germany: TUprints, 2019) <https://tuprints.ulb.tu-darmstadt.de/id/eprint/9164>.

6 Altmann, Bernhardt, and others; FONAS, 'Forschungsmemorandum – Naturwissenschaftliche Friedensforschung in Deutschland', *Wissenschaft & Frieden*, 2016, 31–33 <http://www.wissenschaft-und-frieden.de/seite.php?artikelID=2102>; Neuneck G., 'Frieden und Naturwissenschaft', in *Handbuch Frieden.*, ed. by Hans-J. Gießmann and Bernhard Rinke Wiesbaden: VS Verlag für Sozialwissenschaften, 2011.

7 Thorsten Bonacker, 'Forschung für oder Forschung über den Frieden? Zum Selbstverständnis der Friedens- und Konfliktforschung', in *Friedens- und Konfliktforschung*, ed. by Peter Schlotter and Simone Wisotzki, Baden-Baden: Nomos, 201, pp. 46–78.

8 Jürgen Altmann, Martin Kalinowski, and others, 'Naturwissenschaft, Krieg und Frieden', in *Friedens- und Konfliktforschung*, ed. by Peter Schlotter and Simone Wisotzki (Baden-Baden: Nomos, 2011), pp. 410–445.

9 Reuter and others, 'Zur Naturwissenschaftlich-Technischen Friedens- und Konfliktforschung – Aktuelle Herausforderungen und Bewertung der Empfehlungen des Wissenschaftsrats'.

These examples show that on the one hand, natural science/technical peace research includes disciplinary, theoretical and experimental research that is initially motivated by a political problem. On the other hand, science-based peace research also has to work on relevant scientific and technical questions over a long period of time which do not have an interdisciplinary character. An example of the Comprehensive Nuclear Test-Ban Treaty is geophysical research on whether or not one can tell from seismic signals if they come from an earthquake or an underground nuclear explosion.[10] On the other hand, natural science/technical peace research addresses more actual issues and attempts to develop important statements for policymakers within a short time period. In such cases, interdisciplinarity, particularly the cooperation with social sciences, is fundamental. For example, one question here is whether missile defense in space could negate nuclear missiles so effectively that states could do without deterrence.[11] In summary, it can be stated that both types of research require a long-term continuity of scientific knowledge and methods.

In conclusion, natural science/technical peace research nowadays supports political processes of war prevention, disarmament and confidence building. Furthermore, this discipline analyses characteristics and consequences of new types of weapons and develops proposals for limitations as well as technical solutions.[12] Scientists who are aware of possible negative consequences of new technologies are researching, among other things, verification (i.e. checking of compliance with disarmament treaties), the restriction of innovations to peaceful goals, and the proliferation-resistant design of civil technologies with dual-use potential. This research serves to complement political science peace research.[13]

3. Current Work: Articles in this Special Issue

As already illustrated, natural science/technical peace research covers a broad methodological spectrum, ranging from disciplinary to interdisciplinary work. This special issue contains work from different research areas, varying in the degree of interdisciplinarity. We received many suggestions for articles. After two rounds of peer-review the following articles have been accepted:

The article "*A Developing Arms Race in Outer Space? De-constructing the Dynamics in the Field of Anti-Satellite Weapons*" was written by Daniel Lambach, lecturer for political science at the University of Duisburg-Essen, and Arne Sönnichsen, research assistant at the same university. The authors explain that existing fears of the militarization of space often lead to techno-determinist arguments. For example, the recent development of Anti-Satellite (ASAT) capabilities among space powers like China and India is often described in terms of a technologically driven arms race. This article takes a Social Construction of Technology approach to deconstruct the dynamics of this supposed arms race. Using a case study of Mission Shakti, the 2019 test of an Indian ASAT system, it finds that while state officials made some security-related claims about their ASAT project, they placed a greater emphasis on status-seeking arguments. This offers possibilities for de-securitizing outer space.

In the article "*Towards IT Peace Research: Challenges on the Intersection of Peace and Conflict Research and Computer Science*" by Christian Reuter (Science and Technology for Peace and Security (PEASEC) at Technical University of Darmstadt) explains that advances in science and technology, including information technology (IT), play a crucial role in the context of peace and security. However, research on the intersection of peace and conflict research as well as computer science is not well established yet. This article highlights the need for further work for "IT peace research" which includes both empirical research on the role of IT in peace and security, as well as technical research to design technologies and applications for, amongst others, limitations and verification. Based on the elaboration of the disciplines, central challenges, such as regarding insecurity, actors, attribution and laws are outlined.

The article "*The state of cyber arms control. An International Vulnerabilities Equities Process as the way to go forward?*" by Matthias Schulze (German Institute for International and Security Affairs, SWP) analyses proposals for cyber arms control, modelled after traditional arms control regimes. Although the threat of cyber-conflict rises, not much ground has been gained with cyber arms control regimes. The author finds that challenges of the digital domain, issues of regime verification and the lack of political will are big inhibitors in transferring these to the cyber-domain. To overcome these inhibitors, cyber experts proposed a new type of regime focusing on zero-day vulnerabilities. Since nobody so far explained, what a so-called International Vulnerabilities Equities Process (IVEP) could look like, the article takes up the task and presents two original models. It then checks, whether or not these can overcome the identified inhibitors. The article concludes that at the current state, an IVEP is not feasible as a cyber-arms control alternative and that future research into the structural elements and interest constellations is needed.

The article "*Cyber Threat Intelligence Sharing between States*" by Philipp Kühn, Thea Riebe, Lynn Apelt, Max Jansen and Christian Reuter (Technical University of Darmstadt) investigates Cyber Threat Intelligence (CTI) platforms which are used in IT-security management to share and analyse cyber threats for a collective crisis management. The article discusses if CTI platforms can be used as a confidence-building measure between states and international organizations. Current CTI platforms are portrayed, deducting political requirements, and answers are offered to the question of how CTI communication may contribute to confidence-building in international affairs. The results suggest further development of analytical capabilities, as well as the implementation of a broad social, political, and legal environment for international CTI sharing.

10 P G Richards and J Zavales, 'Seismic Discrimination of Nuclear Explosions', *Annual Review of Earth and Planetary Sciences*, 18.1 (1990), 257–286.
11 David Hafemeister, 'The Defense: ABM/SDI/BMD/NMD', in *Physics of Societal Issues*, New York, NY: Springer 2014, pp. 55–76.
12 Jürgen Altmann, 'Einführung', in *Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung*, ed. by Jürgen Altmann and others,Wiesbaden: Springer VS, 2017, pp. 1–7.
13 Reuter and others, 'Zur Naturwissenschaftlich-Technischen Friedens- und Konfliktforschung – Aktuelle Herausforderungen und Bewertung der Empfehlungen des Wissenschaftsrats'.

The article "*Towards a Prospective Assessment of the Power and Impact of Novel Invasive Environmental Biotechnologies*" by Johannes L. Frieß and Bernd Giese (both University of Natural Resources and Life Sciences in Vienna) and Anna Rössing as well as Gunnar Jeremias (both Carl Friedrich von Weizsäcker-Centre for Science and Peace Research, Hamburg) investigates novel invasive environmental biotechnologies, namely gene drives and Horizontal Environmental Genetic Alteration Agents, which exceed the classical applications of genetically modified organisms. This article presents a first preliminary examination whether international regulation is prepared for possible conflicts caused by benevolent or hostile use of these technologies. Potentially relevant international treaties are identified, and open questions regarding export control are briefly addressed. The authors conclude that further investigation is called for and recommend scenario-building as a useful tool to explore potential consequences that may arise from application contexts of these novel technologies.

The article "*New Military Technologies: Dangers for International Security and Peace*" by Jürgen Altmann (Technical University of Dortmund) focuses on new military technologies that are being developed at a high pace, with the USA in the lead. Intended application areas are space weapons and ballistic missile defence, hypersonic missiles, autonomous weapon systems and cyber war. Generic technologies include artificial intelligence, additive manufacturing, synthetic biology and gene editing, and soldier enhancement. Problems for international security and peace – arms races and destabilisation – will likely result from properties shared by several technologies: wider availability, easier access, smaller systems; shorter times for attack, warning and decisions; and conventional-nuclear entanglement. Preventive arms control is urgently needed.

4. Summary

In sum, our special issue gives an overview of current research projects and challenges in natural science and technical peace research. The articles focus on (1) anti-satellite weapons, (2) challenges on the intersection of peace and conflict research and computer science, (3) cyber arms control, (4) cyber threat exchange, (5) novel environmental biotechnologies, and (6) increased threats of novel military technologies. We are very grateful to all authors and reviewers for their contributions as well as to the editorial team of the journal S+F (Security and Peace) who made this special issue possible.

Acknowledgements: Parts of this research work have been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE, by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 – 236615297 and the VolkswagenStiftung.

Prof. Dr. **Christian Reuter**, full professor for Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt. Focus: interactive and collaborative technologies in the context of crises, security, safety, and peace.

PD Dr. **Jürgen Altmann**, head of the research group on Physics and Disarmament at TU Dortmund. Focus: military-technology assessment of automated and autonomous weapon systems; questions related to natural science and technical peace research.

Prof. Dr. **Malte Göttsche**, assistant professor and head of the Nuclear Verification and Disarmament Group at RWTH Aachen. Focus: nuclear verification technologies, related simulation tools, radiation detection and non-proliferation and disarmament policy.

Dr. **Mirko Himmel**, scientist at the Carl Friedrich von Weizsäcker-Centre for Science and Peace Research, University of Hamburg. Focus: technologies for preventive biological and chemical arms control; infectious biology; bioethics.

4. Bibliography

Altmann, Jürgen, 'Einführung', in Jürgen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann, and Dieter Wöhrle, *Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung*, (Wiesbaden: Springer VS, 2017), pp. 1–7.

Altmann, Jürgen, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann, and Dieter Wöhrle, *Naturwissenschaft – Rüstung – Frieden*, *Naturwissenschaft – Rüstung – Frieden*, Wiesbaden: Springer VS, 2017.

Altmann, Jürgen, Martin Kalinowski, Ulrike Kronfeld-Goharani, Wolfgang Liebert, and Götz Neuneck, 'Naturwissenschaft, Krieg und Frieden', in *Friedens- und Konfliktforschung*, ed. by Peter Schlotter and Simone Wisotzki (Baden-Baden: Nomos, 2011), pp. 410–445 <https://doi.org/10.1007/978-3-531-92009-2>.

Bonacker, Thorsten, 'Forschung für oder Forschung über den Frieden? Zum Selbstverständnis der Friedens- und Konfliktforschung', in *Friedens- und Konfliktforschung*, ed. by Peter Schlotter and Simone Wisotzki (Baden-Baden: Nomos, 2011), pp. 46–78.

FONAS, 'Forschungsmemorandum – Naturwissenschaftliche Friedensforschung in Deutschland', *Wissenschaft & Frieden*, 2016, 31–33 <http://www.wissenschaft-und-frieden.de/seite.php?artikelID=2102>.

Hafemeister, David, 'The Defense: ABM/SDI/BMD/NMD', in *Physics of Societal Issues* (New York, NY: Springer, 2014), pp. 55–76 <https://doi.org/10.1007/978-0-387-68909-8_3>.

Neuneck G., 'Frieden und Naturwissenschaft', in *Handbuch Frieden.*, ed. by Hans-J. Gießmann and Bernhard Rinke, Wiesbaden: VS Verlag für Sozialwissenschaften, 2011.

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

Reuter, Christian, Jürgen Altmann, Malte Göttsche, and Mirko Himmel (eds.), *SCIENCE PEACE SECURITY '19 – Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research*, Darmstadt, Germany: TUprints, 2019. <https://tuprints.ulb.tu-darmstadt.de/id/eprint/9164>.

———, 'Zur Naturwissenschaftlich-Technischen Friedens- und Konfliktforschung – Aktuelle Herausforderungen und Bewertung der Empfehlungen des Wissenschaftsrats', *Zeitschrift für Friedens- und Konfliktforschung (ZeFKo)*, 2020.

Richards, P G, and J Zavales, 'Seismic Discrimination of Nuclear Explosions', *Annual Review of Earth and Planetary Sciences*, 18 (1990), 257–86 <https://doi.org/10.1146/annurev.ea.18.050190.001353>.

Wissenschaftsrat, 'Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung' (Drs. 7827-19), 2019, 1–178.

A Developing Arms Race in Outer Space? De-Constructing the Dynamics in the Field of Anti-Satellite Weapons*

Arne Sönnichsen, Daniel Lambach

Abstract: Fears about the militarization of space are widespread. For example, the recent development of Anti-Satellite (ASAT) capabilities by rising powers like China and India is often described as a technologically driven arms race. This article takes a social constructivist approach to deconstruct the dynamics of this supposed arms race. Using a case study of Mission Shakti, the 2019 Indian ASAT test, the conclusion is that the ASAT arms race is more complex than it seems at first glance. Most importantly, states seem less motivated by security gains but frequently make status-seeking arguments. This offers possibilities for de-securitizing outer space again.

Keywords: Outer space, arms race, anti-satellite weapons, militarization, science & technology studies
Stichwörter: Weltraum, Rüstungswettlauf, Anti-Satelliten-Waffen, Militarisierung, Wissenschafts- und Technologiestudien

1. Introduction

Recent years have witnessed a boom in human activity in space and in the development of space-related technologies. This includes, among other trends, 'NewSpace' industries which have significantly cut launch costs, the widespread deployment of microsatellites, space activities by nations who are relative newcomers to the 'space club', the prospective inauguration of a Space Force as an independent branch of the United States military, and much more. These developments have raised worries of a 'new space race' (Pekkanen, 2019), a new iteration of the original space race of the 1950s and 1960s which was marked by the rivalry between the United States and the Soviet Union.

Such fears of a renewed geopolitical competition for space are very likely overblown, at least over the short and medium term. The original space race represented two major powers directing huge resources towards science and research in order to outdo the other. But the situation today is more complex and less obviously conflictual than during the Cold War. Today, the main space-faring actors – the United States, China, Russia, India, several European countries under the umbrella of the European Space Agency, Canada, and Japan – cooperate in many areas even as they strive for national prestige in space. Furthermore, near-Earth space is witnessing a veritable 'Gold Rush' (Pelton, 2017) of commercial exploitation. With satellite communications as a backbone of globalization, states are entangled in a web of interdependencies. In short, there are significant benefits for everyone not to disrupt human activity in space.

However, this general alignment of interests does not preclude the possibility of arms races. As human activity in space increases, so does the need for governance and conflict management in 'space safety' fields like space traffic management, space situational awareness, debris mitigation etc. 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 space-faring nations. This is partly due to the institutional architecture of outer space governance (OSG) which only provides a thin layer of regulation (Hertzfeld, Weeden, & Johnson, 2016). The security-related language in the so-called 'Five Treaties'[1] mostly consists of normative exhortations with few concrete rules or enforcement mechanisms. As a result, the present system of OSG is ill-equipped to prevent or contain arms races. Alternative institutions are also ineffective. The proposed Prevention of an Arms Race in Outer Space (PAROS) Treaty is in limbo at the UN Conference on Disarmament, while initiatives like the European Union's International Code of Conduct for outer space activities (ICoC) and Russia's and China's PPWT (Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects) are also not getting much buy-in (Gindullis, 2016). This is all the more problematic since space powers are renewing a securitized view of space (Peoples, 2011).[2] The increase in national space capabilities among major space powers is exacerbating these tensions (Handberg, 2018).

Three factors in particular increase escalation risks. First, the relevant treaties do not prohibit the placement of non-nuclear arms in space. Also, there is no agreement about what constitutes 'arms' in space. Second, states are increasingly reliant on space assets, but these assets are highly vulnerable to disruption and attack. We see the renewed interest in Anti-Satellite Weapons (ASAT) as evidence of this (see Section 2.2). Third, there is widespread agreement that space assets are inherently dual-use in nature which makes their regulation more difficult, inevitably securitizing many otherwise innocuous debates. This raises questions of what may constitute legitimate defence against real or perceived threats (Chow, 2017). Although we are sceptical of the merits of these claims, there is no denying that this represents an established frame among defence communities and is affecting actors' behaviour accordingly.

* This article has been double blind peer reviewed. The authors are grateful to Jürgen Altmann, Christian Reuter, the editorial team of S+F and two anonymous reviewers for their helpful comments.

1 The major treaty is the Outer Space Treaty (OST) of 1967. Further treaties are the Rescue Agreement of 1968, the Space Liability Convention of 1972, the Registration Convention of 1976, and finally the Moon Treaty of 1979 which has not been ratified by major space-faring countries.

2 We understand securitization (treating outer space as an asset for or threat to national security), militarization (viewing outer space in terms of military risks) or weaponization (deploying arms or parts of military systems in outer space) of outer space as different elements on a spectrum of a 'securitized view of outer space'.

The aim of this article is to subject claims of arms races in outer space to critical scrutiny. Focusing on 'Mission Shakti', India's first successful test of a kinetic ASAT system in March 2019, we ask whether this episode is evidence of a wider arms race in the field of ASAT weapons. We take a sceptical view of overly techno-centric explanations of arms races. Indeed, many of the arguments summarized above boil down to assertions that new technologies will inevitably be weaponized. Instead, we argue that arms races dynamics are not solely determined by technological development but also by social dynamics. In line with most of Science & Technology Studies, we argue that the development, purpose and effects of technology are socially situated, and that arms races are therefore best understood through the interaction of technology and politics. Specifically, drawing on a Social Construction of Technology (SCOT) approach, we argue that anti-satellite weapons are created not just, and maybe not even primarily, for national security purposes, but are also treated as symbols of national status and prestige. This is not to deny the possibility of escalation or the existence of security dilemmas in this field, but rather to probe how such dynamics emerge in sociotechnical assemblages of national security and what they imply for peace and security.

2. Arms Races and Arms Control in Space

2.1 Debates about the Militarization of Space

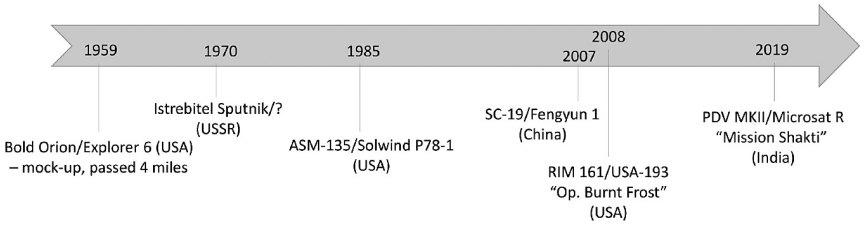
The risks, benefits or even inevitability of militarization has always featured prominently in debates about outer space. In the 1950s and 1960s, the superpowers explored possibilities of stationing weapons of mass destruction, especially nuclear arms, in orbit, and to develop anti-satellite weapons. These options were foreclosed by the Outer Space Treaty (1967) and the Anti-Ballistic Missile Treaty (ABM, 1972), although the language of these two treaties is somewhat ambiguous (Peoples, 2011, pp. 78-79). But militarization has never been simply about placing arms in space (which is more properly referred to as the 'weaponization' of space), a costly and difficult prospect at the best of times. An easier way of militarizing space is not to treat it as a separate domain but to view it as an extension of earthbound military activity as NATO (2019) did recently. In many nations, space exploration and human spaceflight projects grew out of military programs and are evaluated, at least in part, according to their contributions to national defence and security. Space infrastructure is an integral part of the Revolution in Military Affairs, with satellites providing crucial intelligence, surveillance and communications capabilities. While space assets have been used in terrestrial warfare since the early days of spaceflight, Maogoto and Freeland (2007) consider the Gulf War (1990-91) to be the first 'space war', in which space assets contributed significantly to military success.

But beyond this, there are renewed discussions about war *in* space, not just *involving* space. The recent move by the United States government to establish a Space Force has to be seen as an attempt to improve the US armed forces' capabilities for in-theatre action, as are similar projects by other nations. Discussions about 'spacepower' have been going on for decades (Bowen, 2019) as have discussions about the protection of space assets from aggression (Wolter, 2006). Yet, in spite of these historical continuities, recent moves seem to signal a shift in discourse and perception towards the possibility of warfare in space (Pavelec, 2012). However, it is not clear whether the build-up of military assets for such scenarios is driven by genuine security concerns or whether it could also be interpreted as a symbolic move that underpins a nation's claims for great power status. The 'space club' (Paikowsky, 2017) is now complementing the famed 'nuclear club' and is expanding beyond the 'traditional' space powers (Harding, 2013).[3]

2.2 Anti-Satellite Weapons (ASAT) and the Difficulties of Arms Control

ASAT in itself is not a new technology but has been envisioned since the early days of man-made objects in space (Bulkeley & Spinardi, 1986). Starting in the late 1950s, the US and the USSR developed the earliest ASAT systems using missiles or interceptor satellites launched either from the ground or (for the 1985 US test) from a fighter jet (see Fig. 1). Both countries also experimented with ground-based lasers, masers and other high-energy beams, as well as 'killer satellites' and co-orbital battle stations, such as the Soviet 17F19DM Skif-DM Polyus, but these systems never became operational. The earliest ASAT systems were mostly discontinued or mothballed at the end of the Cold War. But interest in counterspace capabilities was re-invigorated by a study headed by then-US Defence Secretary Donald Rumsfeld which warned of a possible 'space Pearl Harbor' (Commission to Assess United States National Security Space Management and Organization, 2001). In the wake of this and of the terrorist attacks of 2001, the Bush Administration withdrew from the ABM Treaty in 2002, allowing it to pursue counterspace capabilities again.

Fig. 1: Successful ASAT tests (systems used/satellites targeted)



ASAT capabilities have since been developed by other space powers. China had pursued ASAT capabilities since the 1960s and in January 2007 successfully destroyed a defunct weather satellite using a ground-launched missile. This set off a series of tests by other nations. The US Navy destroyed a malfunctioning US spy satellite using a ship-fired kinetic missile in February 2008. Since 2015, Russia has undertaken several flight tests of its PL-19 Nudol anti-ballistic missile and anti-satellite system between 2015 and 2018. China has reportedly conducted further tests

3 This process is in line with findings from recent research into status and prestige in international relations. See, e.g., Ward (2017).

of more advanced systems capable of reaching higher altitudes. Most recently, in March 2019, India successfully tested its ASAT system ('Mission Shakti', see below) (Weeden & Samson, 2019).

In total, it seems appropriate to speak of an ASAT arms race, where states view ASAT as a useful deterrent against enemies targeting a nation's space assets. However, there are two ways in which this arms race is more complex than it seems: first, relationships within the arms race are not always reciprocal. For instance, while India justifies its ASAT program by pointing to the relative space superiority of China, China seems mostly unconcerned about this, referring to the United States as its main competitor instead. Second, the escalatory dynamic of ASAT technologies is complex. States seem more worried by the scenario that a competitor uses technological capabilities acquired through ASAT to advance its ABM program than by the ASAT program itself.

Beyond these dedicated systems, there are other means for counterspace operations, such as cyber warfare (Neuneck & Rothkirch, 2006, pp. 26-32; Rajagopalan, 2019). Since recently, defence communities are discussing the possibility of using satellites to target space assets by placing them on collision courses, or otherwise sabotaging or disabling other satellites through On-Orbit Servicing technology since they carry the same kinetic energy as a dedicated Kinetic Kill Vehicle (Chow, 2017). This alerts us to the fundamental definitional problems for arms control in outer space: Should 'arms' include space-based assets that are integrated into Earth-based systems, such as satellites providing guidance for drones, or should it be restricted to systems that target objects in space? Does it make sense to restrict the definition to assets which are explicitly designed as weapons? Such questions are difficult to resolve and we cannot provide an answer here. But in the absence of international consensus, it is noticeable that states mainly rehash discussions, going back to the 1950s, about what constitutes legitimate defence (Brandau, 2015).

3. The Social Construction of Arms Races

Arms races are not a technologically induced inevitability but are just as much socio-politically driven. The basic formulation of an arms race sometimes glosses over this part of the equation: if nation A develops capability Z, then nation B is under pressure to also develop capability Z so as not to be at a strategic disadvantage. But nation B is only under pressure to develop capability Z if it sees nation A as a threat. Evidently, arms races are not just driven by 'hard' factors like security, economy and technology, but are also shaped by such 'soft' factors as perceptions, narratives and identity constructions. Of course, without technological development, qualitative arms races would be an impossibility – national rivalries would play out in other ways, or in purely quantitative terms. Technological shifts force states to re-evaluate and clarify their relationship and to provide important touchstones for conflict or cooperation. To make sense of this interplay of technology and politics, we use the SCOT approach as an inspiration.

The core premise of SCOT is that the meaning, use and impact of technology are socially constructed. It takes a broad view of technology, looking not only at physical artefacts but also at 'social techniques' and how such technologies are embedded into human activities and bodies of knowledge (Bijker, 1995, p. 231). Crucially, while SCOT foregrounds social processes, it does not view technology simply as a dependent variable of social processes. It acknowledges that technology follows developmental paths that are characterized by contingencies and critical junctures but argues that the design choices made along these trajectories are influenced by perceptions among key stakeholders and that research should problematize these processes and their social implications (Williams & Edge, 1996, p. 866).

While a full recapitulation of SCOT is beyond the scope of this article (see Pinch & Bijker, 1984), we draw from it that the meaning of technology is never inherently obvious. In the process of intersubjective construction, multiple meanings can be attached to an artefact by relevant groups. In contrast, theories of arms races typically treat actors as single-minded and focusing on security concerns and uncertainty about other states' intentions (Tang, 2009). However, there is much research showing that political actors attach a multitude of meanings to space technologies, e.g. their effects on local economies and employment (the 'space industry' argument), or use them to suppress internal discord (Olbrich & Shim, 2017). For ASAT, we argue that states are not only motivated by security fears but also emphasize the symbolic and ideological value of ASAT capabilities.

4. Methodology

To support our argument, we use 'Mission Shakti', the March 2019 test of an Indian ASAT system. We identified meanings attached to this technology in India and its regional competitors, China and Pakistan. We used publicly available commentary on the event from Indian, Chinese and Pakistani sources. Our search (using keywords like "ASAT", "anti-satellite" or "Shakti") was focused on three main sources: a) official webpages of state institutions (e.g. the gov.pk domain), b) government-affiliated Twitter accounts, c) Lexis Nexis for national press coverage and commentary by local analysts, supplemented by commentary from outside experts in the secondary literature. We then identified recurring discursive elements in justifications and explanations of the Indian ASAT program and classified those as primarily security- or status-seeking arguments.

5. Mission Shakti

On 27 March 2019, India launched 'Mission Shakti' ('power'), a ground-launched interceptor missile which destroyed Microsat-R via kinetic impact at an altitude of 283 km in Low Earth Orbit. Microsat-R, an Indian earth observation satellite, had only been in orbit since 24 January 2019 and had likely been intended as a practice target from the beginning. The ASAT system was spun off from India's ABM program and was developed by the Defence Research and Development Organisation (DRDO), the 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 (Lele, 2019b, pp. 12-13).

From our analysis, we find three distinct objectives attached to the ASAT program in Indian political discourse. First, in line with

an arms race 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, 2019 March 27a). In contrast, Pakistan did not feature much in the Indian decision due to its lack of comparable space capabilities.

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, p. 73), and ASAT is portrayed as symbolic capital in evidence of that fact. It is repeatedly stressed that India is only the fourth country globally 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, 2019, March 31). Government representatives point out that the effort was completely indigenous and developed solely by Indian scientists, thereby underscoring further the nationalist narrative (narendramodi, 2019, March 27). This also ties in with a long-standing aim of successive governments to 'indigenise' Indian defence procurement (Pardesi & Matthews, 2007).

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 kinetic interceptor missile to minimize debris creation. If a space object is hit at an angle, debris is propelled into higher orbits, threatening other objects. Furthermore, these fragments take longer to re-enter and burn up in the Earth's atmosphere. But independent analysts conclude that the impact was not precisely head-on and launched fragments into much higher altitudes, some even above the orbital band of the International Space Station (~410 km) (Akhmetov, Savanevych, & Dikov, 2019). 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), referring to an emerging global 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 banned (Davis, 2019) – a situation that India already experienced with the Non-Proliferation Treaty (Weeden & Samson, 2019, section 6-2).

Third, the ASAT test also had a domestic politics angle. Some opposition parties framed the mission as a political stunt ahead of the national elections in April 2019, a narrative that is also picked up by Chinese and Pakistani commentators. 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, 2019, March 27b). 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 (Lele, 2019a; Gupta, 2019). In July 2019, the Indian armed forces held its first space warfare exercise (IndSpaceEx), a table-top wargame involving all branches of the military.

The second and third objective show how arms technology can be a symbolic and political resource for governments. Also, they are not incompatible with the first aim of deterring Chinese aggression. But Mission Shakti is not a clear-cut case of arms race escalation: there is very little evidence that other states, especially India's regional rivals Pakistan and China, perceive this as a particularly threatening move. China gave no official statement on the test at all. Semi-official commentary in the state-controlled press was more critical of IndSpaceEx and the creation of space debris rather than India having ASAT capabilities (Weijia, 2019; Global Times, 2019). Pakistani government officials decried risks to regional stability in abstract terms and highlighted the domestic interests of Prime Minister Modi, who faced political pressure for his handling of conflict in the contested region of Jammu and Kashmir. But there were no calls for Pakistan to develop similar capabilities (Ministry of Foreign Affairs, 2019; Jaspal, 2019). This may be conditioned by Pakistan's general lack of space expertise compared to India, but even taking that into account, the official statements did not evoke a sense of threat. Instead, China and Pakistan seemed to understand that India was mainly or partly playing a status game and their comments were aimed at undercutting the status narratives that Indian officials had put forward, often referring to the creation of space debris, quoting Bridenstine's critique, or insinuating that the ASAT test was only made possible by technology transferred from the United States.

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 within a complex and entangled set of aims and aspirations by key actors in India, and international responses back up this interpretation. 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.

6. Conclusion

In our introduction we indicated widespread worries about a potential new space race. At face value, the recent Indian ASAT test seems like a milestone to further militarization in a space arms race. In brief, we find that there may be an ASAT arms race but that its risks of escalation are lower than might be expected. Our findings indicate that states do not develop space weapons only, and maybe not even mainly, to seek security in space – and crucially, they also interpret a rival's behavior in terms of both security- and status-seeking. Generalizing from the Indian case, we argue that status-seeking and the symbolic capital of being a member of the space club are a goal in themselves and that space-faring nations pursue these goals through the development

of military capabilities in space. Weapons systems are symbolically important as they can be made to support narratives of national greatness and international status.

Somewhat paradoxically, this opens possibilities to lessen pressures towards the weaponization and militarization of outer space. We are convinced that a progressive de-securitization of outer space is possible and even necessary as civilian and commercial activities grow. Current and future cooperative projects to develop lunar bases or deep space gateways can be seen as comparable opportunities in this direction, which represent status symbols for participating countries without the attendant risks of weaponization. Other possibilities include the development of norms and protocols for remote proximity operations, i.e. emerging technologies for controlled rendezvous between space objects, so as to defuse fears of sabotage and damage by other satellites.

Arne Sönnichsen (M.A.) is Research Associate at the Chair of International Politics and Development at the University of Duisburg-Essen. His PhD project is about New Technologies and Governance in Outer Space, and he is a member of the research network 'Security and Technology in Outer Space'.

Daniel Lambach (PD Dr.) is a Heisenberg Fellow at the Research Unit Normative Orders, Goethe-Universität Frankfurt, and a Privatdozent at the Faculty of Social Sciences, Universität Duisburg-Essen. He is the coordinator of the research network 'Security and Technology in Outer Space'.

7. References

Akhmetov, V., Savanevych, V., & Dikov, E. (2019). Analysis of the Indian ASAT test on 27 March 2019. *arXiv*. doi:arXiv:1905.09659

Aliberti, M. (2018). *India in Space: Between Utility and Geopolitics*. Cham: Springer.

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]. 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/1110886268408233984.

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.

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.

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*. 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? *ASPI Strategist*. 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*. https://spacenews.com/nasa-warns-indian-anti-satellite-test-increased-debris-risk-to-iss/.

Gindullis, M. (2016). *Is the European Initiative for an International Code of Conduct the right Step forward for Conflict Prevention in Outer Space?* Hamburg: IFAR[2] Fact Sheet. http://epub.sub.uni-hamburg.de/epub/frontdoor.php?source_opus=66245&la=de.

Global Times. (March 29, 2019). Anti-satellite test shouldn't stir India's nationalism. *Global Times (China)*. http://www.globaltimes.cn/content/1143866.shtml.

Gupta, S. (March 29, 2019). After A-SAT testing, PM Modi asks NSA Ajit Doval to prepare draft space doctrine. *Hindustan Times*. 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.

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.

Jaspal, Z. N. (2019): India's Destabilizing ASAT Missile Test. *HILAL English*. https://www.hilal.gov.pk/eng-article/india%E2%80%99s-destabilizing-asat-missile-test/MzI5OA==.html.

Lele, A. (2019a). India needs its own space force. *SpaceNews*. 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.

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.

Ministry of Foreign Affairs (April 5, 2019): Daily Press Briefing. http://mofa.gov.pk/record-of-press-briefing-by-spokesperson-on-friday-05-april-2019/.

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]. 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*. https://www.nationalheraldindia.com/opinion/herald-view-modi-stakes-claims-to-others-achievements-again-this-time-of-drdo-scientists

NATO (2019, November 19): Press conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Ministers of Foreign Affairs. https://www.nato.int/cps/en/natohq/opinions_170972.htm

Neuneck, G., & Rothkirch, A. (2006). *Weltraumbewaffnung und Optionen für präventive Rüstungskontrolle*. Osnabrück: Deutsche Stiftung Friedensforschung. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-260300

Olbrich, P., & Shim, D. (2017). Symbolic practices of legitimation: exploring domestic motives of North Korea's space program. *International Relations of the Asia-Pacific, 19*(1), 33-61.

Paikowsky, D. (2017). *The Power of the Space Club*. Cambridge: Cambridge University Press.

Pardesi, M. S., & Matthews, R. (2007). India's Tortuous Road to Defence-Industrial Self-Reliance. *Defence & Security Analysis, 23*(4), 419-438.

Pavelec, S. M. (2012). The Inevitability of the Weaponization of Space: Technological Constructivism Versus Determinism. *Astropolitics, 10*(1), 39-48.

Pekkanen, S. M. (2019). Governing the New Space Race. *AJIL Unbound, 113*, 92-97.

Pelton, J. (2017). *The New Gold Rush. The Riches of Space Beckon!* Cham: Copernicus.

Peoples, C. (2011). The Securitization of Outer Space: Challenges for Arms Control. *Contemporary Security Policy, 32*(1), 76-98.

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.

Rajagopalan, P. (2019). *Electronic and Cyber Warfare in Outer Space*. Geneva: United Nations Institute for Disarmament Research. https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf

Rej, A., & Sagar, R. (2019). The BJP and Indian Grand Strategy. In M. Vaishnav (Ed.), *The BJP in Power: Indian Democracy and Religious Nationalism* (pp. 73-82). Washington D.C.: Carnegie Endowment for International Peace.

Tang, S. (2009). The Security Dilemma: A Conceptual Analysis. *Security Studies, 18*(3), 587-623.

Tellis, A. J. (2019). India's ASAT Test: An Incomplete Success. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884.

Ward, S. (2017). *Status and the Challenge of Rising Powers*. Cambridge: Cambridge University Press.

Weeden, B., & Samson, V. (2019). *Global Counterspace Capabilities: An Open Source Assessment*. Broomfield: Secure World Foundation. https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf.

Weijia, H. (July 24, 2019). Space offers new scope for China-India cooperation. *Global Times (China)*. http://www.globaltimes.cn/content/1159062.shtml.

Williams, R., & Edge, D. (1996). The social shaping of technology. *Research Policy, 25*(6), 865-899.

Wolter, D. (2006). *Common Security in Outer Space and International Law*. Geneva: United Nations Institute for Disarmament Research.

Towards IT Peace Research: Challenges at the Intersection of Peace and Conflict Research and Computer Science*

Christian Reuter

Abstract: Advances in science and technology, including information technology (IT), play a crucial role in the context of peace and security. However, research on the intersection of peace and conflict research as well as computer science is not well established yet. This article highlights the need for further work in the area of research "IT peace research", which includes both empirical research on the role of IT in peace and security, as well as technical research to design technologies and applications. Based on the elaboration of the disciplines, central challenges, such as insecurity, actors, attribution and laws, are outlined.

Schlüsselwörter: IT-Friedensforschung; Technische Friedensforschung; Cyberspace; Cyber-Angriffe
Keywords: IT peace research; technical peace research; cyberspace; cyber attacks

1. Introduction

In 2017, numerous cyber attacks have occurred worldwide. In December 2017, an invasion of the German government network which connects federal ministries and responsible authorities was discovered (cf. Reinhold, 2018). Another example that represents one of the major ransomware attacks in the recent past is the "NotPetya" attack from June 2017. After large parts of Europe, especially the Ukraine, were attacked, the ransomware spread to other countries such as Brazil and the US. NotPetya worked by "modifying the Windows´s system´s Master Boot Record which caused the crashing of the system" (Aidan, Verma, & Awasthi, 2018, p. 124). Cyber attacks like WannaCry ransomware and NotPetya have led to the introduction of initiatives such as the Digital Geneva Convention (cf. Brinkel, 2018).

Besides the fact that those cases illustrate a serve IT security problem, they are also discussed as examples for espionage where an unknown group tried to obtain political information for unknown reasons. On this point, it is important to point out that cyber warfare does not know any boundaries, which is why it poses a threat for all countries and for international peace. Incidents such as the ones mentioned above and the current tensions between the US and Iran after the targeted killing of General Suleimani illustrate an increasing relevance of information technology for peace and security (cf. Kanno-Youngs & Perlroth, 2020; cf. Reinhold & Reuter, 2019). US American cybersecurity experts have already observed increases in malicious cyber activities by pro-Iranian hackers in their systems. They believe that the hackers try to destroy US government databases (cf. Kanno-Youngs & Perlroth, 2020). Those frictions evidence that cyber attacks can lead to an escalation on a political, diplomatic, and military level.

Innovations in scientific and technical research have always been used for military purposes and therefore had a strong influence on warfare. In the First World War, chemists, mathematicians, physicists and engineers were systematically involved in the production of war material (cf. Thee, 1988). Further on, telephones, radio, and digital communication were introduced on the battlefields. Transmission Control Protocol/Internet Protocol (TCP/IP) was developed by Vinton Cerf, an American scientist, in order to communicate under nuclear-war conditions, to create a common protocol for inter-network exchange of information and to let tank formations communicate on the battlefield (cf. Restivo & Denton, 2008, p. 262). Ever since, IT, with its extensive developments in crises, conflicts, and wars, has become increasingly important and part of international political agendas. With the aim of maintaining international peace and security, issues such as cyber attacks and cyber weapons have steadily been addressed in the last few years (cf. Bernhardt & Ruhmann, 2017).

This article aims to highlight the role of IT and computer science in peace and conflict studies, and it outlines challenges at their intersection. The research question in this article therefore is: **What are the central challenges for research at the intersection of peace and conflict studies as well as computer science?**

After presenting such a broad question, it should be noted that an answer containing all possible challenges is beyond the scope. However, some central ones will be outlined. As a first step, the disciplines of peace and conflict studies, natural science/technical peace research, computer science and cyber security are presented in this article as the basis of IT peace research. As a second step, central challenges of IT peace research, including insecurity, actors, attribution, verification, transparency, dual-use, proliferation and laws are analysed. The article closes with conclusions.

2. Towards a Definition of IT Peace Research

In the following sections, the author understands IT peace research as a field of research, which includes various other disciplines

* This article has been double blind peer reviewed. Parts of this article are based on the book "Information Technology for Peace and Security" (cf. Reuter, 2019), especially parts of section 1 and 2 (cf. Reuter, Aldehoff, et al., 2019) as well as some parts of section 3 (cf. Reinhold & Reuter, 2019; Riebe & Reuter, 2019a). The original contribution of this article is the outline of challenges on the intersection of the disciplines. The author would like to thank Laura Guntrum for her valuable support, Thea Riebe and Thomas Reinhold for discussions on the topic, as well as the (anonymous) reviewers for their feedback. This research work has been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Centre for Applied Cybersecurity ATHENE as well as the *Deutsche Forschungsgemeinschaft* (DFG, German Research Foundation) – SFB 1119 CROSSING – 236615297.

DOI: 10.5771/0175-274X-2019-4-10

such as peace and conflict studies and computer science. First, the article will show the relations of computer science and peace and conflict. Second, a definition of IT peace research is given.

2.1 Peace and Conflict Studies

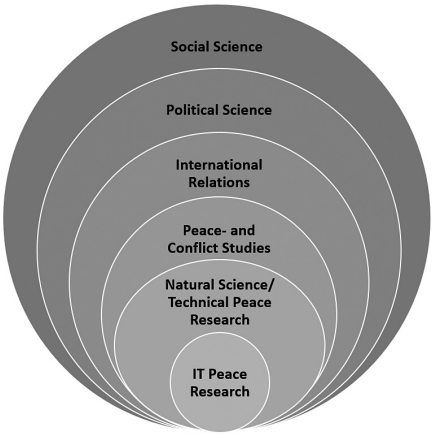
This section provides an overview of peace and conflict studies and classifies IT peace research within it. IT peace research is, amongst others, part of peace and conflict studies, which is an interdisciplinary research field in International Relations (IR). Peace research analyzes the causes of peace and war on the basis of scientific methods and theories from several relevant disciplines, as war and conflicts have almost always been present in mankind (cf. Bonacker, 2011). The oldest empirical study on peace can be dated back to the nineteenth century. Already between 1817 and 1819, the Massachusetts Peace Society investigated human losses in wars. Some of the oldest organisations of peace and conflict studies such as the Carnegie Endowment for International Peace (funded in 1910) and the World Peace Foundation (funded in 1911) are still working in the research field of peace and conflict nowadays (cf. Koppe, 2006). Besides peace and conflict studies, "International Security Studies (ISS) grew out of debates over how to protect the state against external and internal threats after the Second World War" (Buzan & Hansen, 2009, p. 8) and still play an important role in IR today.

As the research on wars previously meant the pure empirical investigation of war and the causes of war, the discipline of peace and conflict studies reinvented itself in the 1950s and early 1960s. Instead of seeing war as a necessary, or even inevitable, social phenomenon (cf. Bonacker, 2011), scientists like Boulding (1963), who saw war namely as a social but preventable phenomenon, attempted to radically change the methodology of the discipline and explain war by using existing social science methods (cf. Bonacker, 2011). This perspective was increasingly and step by step accepted and thereby established inter alia the field of peace research (cf. Gleditsch, Nordkvelle, & Strand, 2014; Koppe, 2006).

Peace research was particularly shaped by Johan Galtung who distinguished between negative and positive peace (cf. Galtung, 1998, p. 66f.). Initially, this new discipline understood itself as very normative – as a "research for peace". Although normativity never completely disappeared and is still nowadays more or less subliminally present, the self-conception of the discipline has changed over time. This is evidenced by the description of the discipline via the term "research on peace". This means that peace is the actual object of empirical research and not necessarily a goal that has to be achieved through it (cf. Bonacker, 2011). The understanding of peace research as a disciplinary field has also been controversially discussed: on the one hand, it can be seen as a field of research in IR, and on the other hand, it is often understood as an interdisciplinary field that makes use of methods and theories of various different disciplines (cf. Bonacker, 2011) in order to explain phenomena related to war and peace. Additionally, it addresses conflict management, conflict resolution, and peacebuilding.

The following figure (Figure 1) provides an overview of how IT peace research can be classified from a peace and conflict research and social science perspective.

Figure 1: IT Peace Research embedded in Peace and Conflict Studies and Social Science.



Source: Own illustration.

2.2 Natural Science/Technical Peace Research

In the interdisciplinary field of peace and conflict studies, technology plays a key role for various forms of conflict resolution. According to Reuter et al. (2020), natural science/technical peace research is a broad research field that deals with the role of scientific and technical possibilities in the context of war and peace, armament and disarmament. Technology is based on findings from various natural sciences and technical disciplines such as physics, chemistry, biology, and computer science. Natural science/technical peace research supports the political processes of preventing war, reducing armament and building confidence with technical solutions. This is necessarily based on the inherent ambivalence of technology and the fact that technological developments have changed the dynamics of war and therefore determine the conditions for disarmament and peace processes (cf. Altmann, 2017). Scientists who are aware of potential negative consequences of these technologies are working on technical solutions in order to reduce or even prevent possible damage. Potential examples of approaches include enabling verification (i.e. checking of compliance with disarmament treaties) or the restriction of innovations to peaceful aims (i.e. regulation of intrusion software as dual-use good). The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a good example for this (cf. Reinhold, 2015). Altmann (2019) points out that this research is strongly needed to complement political-scientific peace research.

The emergence of natural science/technical peace research was a consequence of the emergence and spread of nuclear weapons in the East-West conflict since the late 1940s. With the possibility of using nuclear weapons in war, technical innovations also became strategically (war-)relevant. Despite public concerns, deterrence became the choice at the time as the concept of mutually assured destruction (MAD) would imply (Sokolski, 2004). The best-known example for the existing doubts is the "Russell-Einstein Manifesto" from 1955 which calls for nuclear disarmament and the rejection of war in general. The concerns about the dangers posed by nuclear weapons were shared by wider scientific circles. As a consequence of this appeal, the Pugwash Conferences on Science and World Affairs were created. At the first conference in 1957 in Pugwash,

Canada, 22 scientists from ten countries, from both sides of the Iron Curtain, discussed strategies for nuclear disarmament. Ever since, the so-called "Pugwash Movement" has organised workshops and conferences and conducted research on the problems of nuclear weapons. A similar development could also be observed in Germany with the "Declaration of Göttingen" from 1957. Leading physicists and chemists stated their disapproval of the German government's demand for the nuclear armament of the newly founded German Armed Forces. Such activities represented an important basis which enabled and supported subsequent international treaties on arms control (cf. Altmann et al., 2010; Neuneck G., 2011).

Based on such initiatives, scientific research groups were founded at renowned U.S. universities in the 1960s. During the continuous East-West conflict they investigated nuclear disarmament, arms control, proliferation, and international security. In Germany, Carl Friedrich von Weizsäcker established a working group at the Federation of German Scientists and can therefore be seen as the founding father of natural science and technical peace research in the country. Further working groups such as IANUS at TU Darmstadt, were formed in the 1980s and have ever since deepened their institutionalisation. However, it is agreed that the weak structural establishment and support of this area of research is in big contrast to its importance (cf. FONAS, 2015; Wissenschaftsrat, 2019). Only universities in Hamburg and Darmstadt have full professorships with such a denomination. Furthermore, there is an assistant professorship in Aachen and further positions at peace research institutes that often focus mostly on political science peace research.

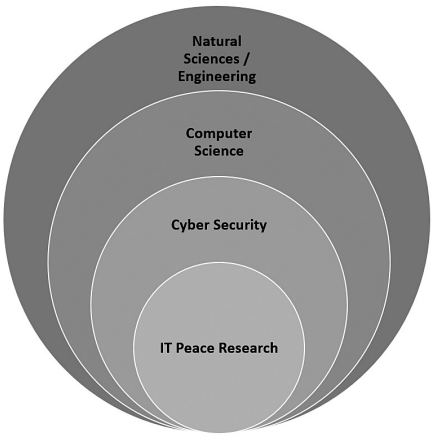
2.3 Computer Science

IT peace research is not only peace research, but also computer science research. Computer science is "the study of computers and the major phenomena that surround them" (Newell, Perlis, & Simon, 1967) or "the systematic study of algorithmic processes that describe and transform information: their theory, analysis, design, efficiency, implementation, and application" (Denning et al., 1989, p. 12).

According to French dictionaries, the origin of the academic use of *Informatique* goes back to 1962, when Dreyfus used the term as an artificial word, consisting of the words "Information" and "*Automatique*" or "*Electronique*". It was understood as the science of the rational processing of information, in particular information by automatic machines (in Coy, 2001, p. 4). This definition assumes that computer science was understood as science even before it became institutionalised. In the German language, the French term was established very quickly, whereby the comprehensive definition was replaced by an American-influenced interpretation. However, automatic machines are still regarded as a central aspect of computer science and computer engineering. Some argue(d) that technical problems and their theoretical-mathematical basics play an important role, whereby economic and social effects are dealt with in other areas. In contrast to the U.S., for example, where computer science and information science are covered under the definition from the *Académie* (and computer engineering is neglected), in Germany computer science is regarded as a link between the understandings of (more theoretical) computer science and (more practical) computer engineering (cf. Coy, 2001).

The following figure (Figure 2) provides an overview of how IT peace research can be classified from a natural sciences/ engineering perspective.

Figure 2: IT Peace Research embedded in Computer Science and Cyber Security



Source: Own illustration

2.4 Cyber Security

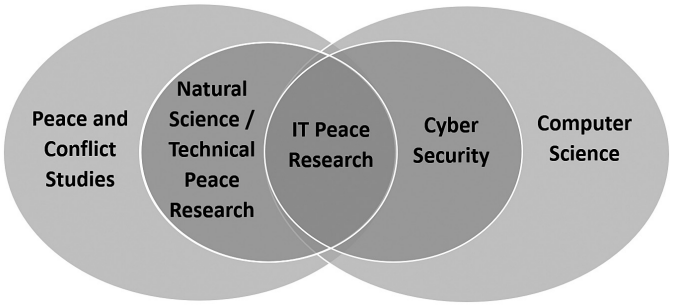
Nowadays, cyber security research can be seen as an important part of computer science, as well as of IT peace research. Initially coming from the Latin word "*securitas*", the term security stands for "without concern". In contrast to the German language, where the word security is only known as "*Sicherheit*", the term can be differentiated between safety and security in English. According to Storey (1996, p.2.), safety can be understood as a protection against unintended events such as natural occurrences or incidents induced through errors or malfunction. Security, on the other hand, means the protection against external or malicious actors like terrorists, perpetrators, or armed forces.

According to ISO/IEC 27001, IT security is defined as "preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved" (ISO, 2013). The term cyber security is often used interchangeably with the term information security. However, as von Solms and van Niekerk (2013, p. 97) state, "cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him- / herself. In information security, reference to the human factor usually relates to the role(s) of humans in the security process."

2.5 IT Peace Research

The above described areas of peace and conflict studies, in particular natural science/technical peace research and computer science, above all cyber security, form the basis for IT peace research (see Figure 3). IT peace research is in particular necessary to restrict the dangers of a cyber arms race and to offer better tools for verification and disarmament (cf. Altmann, 2019).

Figure 3: IT peace research as the intersection of peace and conflict studies and computer science.



Source: Reuter, 2019, p. 24.

The author suggests the following as descriptions:

- Motivated by the relevance of IT for peace and security, **IT peace research** is an interdiciplinary discipline that addresses the role of IT in peace and security from a theoretical, empirical and technical perspective.
- IT peace research is both part of **peace and conflict studies** (especially natural science/technical peace research) as well as of **computer science** (especially cyber security). This is the case because peace and security are either the aim or the object of investigation. Moreover, cyber activities nowadays play a crucial role in war, which is why research on cyber conflicts is becoming increasingly important (cf. Bonacker, 2011). Further, algorithmic processes and IT with reference to security have been important for peace research (Denning et al., 1988; cf. Newell et al., 1967). In summary, IT peace research can be seen as a part of both social and technical research.
- From the **social science perspective**, the aim of the discipline is to (empirically research and) understand the role of IT and computers in peace and security. IT has revolutionised peoples´ lives and has therefore become more important in, for example, organizing protest movements all over the world. Further, IT applications can be used in order to prevent and manage conflicts, crises and disasters.
- From the **technical (natural science/engineering) research perspective**, the aim of the discipline is to design and develop technical possibilities (normative) for preventing war and escalation of cyber conflicts and attacks, avert international security threats and to develop damage control from intergovernmental (and in some cases interpersonal) insecurity. In addition, the discipline helps with the verification in other areas in arms control, such as the processing of big data and satellite images.

3. Research Challenges for IT Peace Research

Cyber attacks often have a transnational component, as the above-mentioned examples of the incident in the German government network and NotPetya show. This is why they are becoming increasingly relevant for IR and international security. In-depth research is necessary in order to find adequate social, political and legal approaches in addition to just technical ones. This type of research has to integrate computer science just as much as approaches from peace and conflict studies and can therefore be described as IT peace research. In the following, some characteristics and exemplary challenges of IT peace research will be outlined.

3.1 Uncertainty regarding Cyber Forces

Challenge 1: Uncertainty about the targets and aims of emerging cyber forces and the probability of targeting civilian infrastructures unintentionally.

One big challenge is the uncertainty, which exists, inter alia, in the recognition of targets, the intentions of cyber attacks and involved key figures. More and more national defence ministries include the cyber domain as a field of its own. For instance, the US Department of Defense defines the cyberspace as an operational domain apart from land, air, water and space (cf. United States Department of Defense, 2011). In 2016, all NATO member states recognised cyberspace as a military domain in order to identify cyber operations as an attack, to adapt to the cyber threat scenarios or to take military actions themselves (cf. NATO, 2016). Furthermore, the NATO decided that cyberspace is an essential domain that needs to be covered by the collective defence strategies and that attacks over cyberspace can invoke the alliance case of Article V of the Charter (cf. NATO, 2019). "The enduring challenge of cyber threats requires that the alliance continuously evaluates whether it is adapting and responding appropriately" (Brent, 2019).

All of this affects military organisational structures: E.g., since 2017, cyber and information space is a separate military organisational area in the German Federal Armed Forces, besides Army, Navy and Air Force, which implements the forces' defensive and offensive capabilities in cyberspace (cf. Bundesministerium der Verteidigung 2016). Often, both capabilities and activities are not obvious, which is why a targeted pursuit and the attribution of the cyber attacks is quite difficult. To date, neither the size of armed forces nor the offensive and defensive distribution of resources can be determined in a targeted manner because many attacks remain hidden and do not occur under a particular, official force. Thus, there are risks of escalation and destabilisation as well as a certain risk that civilian infrastructures could be unintentionally attacked as unintended collateral damage, which could lead to complications or risks for the public sphere. To sum up, we have little information about cyber forces because much of it remains secret and because "normal" hacker groups also carry out cyber attacks without being part of a superior group. This increases the uncertainty between two or more opponents, because the intentions can hardly be gauged.

3.2 Variety of Actors

Challenge 2: Variety of (state and non-state) potential assailants.

A second challenge is the difficult distinction between state and non-state actors, which is not obvious, based on the possibilities of handling cyber weapons – in contrast to nuclear weapons – also by non-state actors. It is also often unclear whether the actors pursue military-strategic or commercial objectives and whether they have no political, but maybe commercial interests maybe on behalf of the private sector or on behalf of a state or group with political intents.

Moreover, cyber activities are more intransparent, since it is more difficult to identify involved actors in the operational domain. The role and responsibilities of state actors in cyber conflicts such as in *defensive* protection procedures need to be strengthened. Further *active* cyber defensive measures (especially counter-attacks) by companies should be forbidden. Offensive operations by non-state actors (e.g. commercial) and the influence of foreign states on democratic processes, such as elections, should be reduced.

3.3 Difficulty of Attribution

Challenge 3: Attribution of security-threatening or even offensive activities.

In order to implement a security strategy, the cyber attack has to be attributed to a person, a state or other unit, such as an organisation. In the case of safety-endangering and offensive-aggressive activities where the perpetrator cannot be identified, it is quite difficult to apply the security strategy in a targeted manner (cf. Rid & Buchanan, 2014). For Wheeler and Larsen (2003, p. 1), attribution is "determining the identity or location of an attacker or an attacker's intermediary". In contrast, Rid and Buchanan (2014, p. 4) state that "attribution is the art of answering a question as old as crime and punishment: who did it?". Despite these different perceptions, 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.

The attribution of cyber attacks consists of technical, legal, and political processes. While the methods of attacker allocation have made significant progress in recent years, digital technologies often still do not provide sufficient evidence for the real-world identity of an attacker (cf. Saalbach, 2019). Research distinguishes two types of cyber attribution challenges (cf. Davis et al., 2017). First, there is the challenge of "accessing, interpreting, and comparing technical and other evidence in an effort to reach a high-confidence attribution finding in a timely manner. Second, there is an additional challenge of persuasively communicating an attribution finding to a target audience or the general public" (Davis et al., 2017, p. 9). Related to that, further research on the development of parameters that allow attribution without disturbing the privacy aspect of the entire internet is needed.

3.4 Verification and Transparency in Cyber Space

Challenge 4: Measures for verification need to be adapted to emerging technologies, and rules for transparency need to be established.

Verification is one of the pillars for treaties and regimes that facilitate members or entitled institutions to verify each other's compliance. Originally, verification has been introduced as a tool for weapons systems that have been utilised for military purposes. Now, its usage on cyberspace is impeded by specific features of this new domain. On this basis, new approaches will have to be developed (cf. Reinhold & Reuter, 2019). This includes, for instance possibilities to measure and verify the total power supply, the available supply of cooling systems, available network bandwidth capacities, the number of connections of monitored networks, and the number of required staff as some of the measurable parameters in the cyberspace.

Further research is necessary in order to tackle two existing issues: 1) How can measures be developed or strengthened to prevent the circumvention or manipulation of monitoring? 2) How can verification of cyber arms control itself work adequately? To sum up, all verification measures are used for specific purposes and use cases (cf. Reinhold & Reuter, 2019). For new or emerging technologies, standards and measurement units are needed. These enable control of the particular measurable parameters in cyberspace (cf. ibid). One sub-question is how transparent cyberspace can be and who has to be transparent to whom about what? One possibility would be an independent, international organisation for attribution that possesses secret service reconnaissance tools and could communicate its results reliably (cf. Davis et al., 2017).

As in other military areas, confidence- (and security-) building measures (C(S)BMs) can act as first steps towards creating transparency and reducing misperceptions and suspicions. Concepts for voluntary CBMs have been developed in the United Nations and are being implemented in the Organisation for Security and Cooperation in Europe (OSCE). Such activities should be improved by explicitly including cyber activities of armed forces and making agreements politically binding, as with the OSCE CSBMs for conventional forces (Altmann 2019, p. 185). In spite of existing differences, many actors try to reduce the existing uncertainties on different technical levels.

3.5 Dual-Use of IT

Challenge 5: How can military/civilian and use/misuse be differentiated?

The use of IT in peace, conflict and for security raises some questions, i.e. whether the use of IT can be limited exclusively to so-called beneficial purposes 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, e.g. in nuclear technology, chemistry, and biology. The importance of dual-use differs slightly, depending on the technology and its risks, as well as its distribution and application (cf. Riebe & Reuter, 2019).

Encryption hard- and software can be seen as dual-use products. Since only strong encryption guarantees tap-proof and confidential communication, cryptography plays a key role in security issues (cf. Vella, 2017). Further, the dual-use debate has led to the proliferation of spyware through additions to the Wassenaar Arrangement in 2013 and 2016 (cf. Herr, 2016). Although software dual-use is becoming a constant problem as part of weapons modernisation (cf. Bernhardt & Ruhmann, 2017; Reuter & Kaufhold, 2018), empirical case studies on dual-use IT are lacking (cf. Leng, 2013; Lin, 2016). On the one hand, modern software development is characterised by agile process models such as "Scrum", in which developers can react flexibly to changes in (customer) requirements (cf. Dingsøyr, Nerur, Balijepally, & Moe, 2012). Therefore, it is obvious that dual-use potentials need to be checked not only in the initial planning of software, but also during the programming itself. On the other

hand, the flexibility of using software in different application contexts is the essential challenge for dual-use impact assessment and must fundamentally differ from the situation in the life sciences (cf. Lin, 2016). The aim is both to minimize risks by non-state actors and to anticipate the risk of uncontrolled distribution of malware between states. It needs to be possible to distinguish between civilian and military use and to prevent applications from being misused. This requires a clear line between legitimate and illegitimate deployments and an appropriate reconnaissance and enforcement mechanism (cf. Riebe & Reuter, 2019).

3.6 Proliferation

Challenge 6: A code can hardly be restricted in its distribution or duplication. Furthermore, the dissemination of (dual-use) technologies within and between countries is proving to be a challenge.

It is extremely difficult to stop or restrict the distribution or duplication of codes. Furthermore, the spread of (dual-use) technologies within and across countries increases the risk of military actions as a tool of preventive action. Assessments like the cyber security index from 2013 (cf. UNIDIR, 2013) solely represent the first step towards binding regulations that restrict, reduce or even forbid the development, dissemination and use of offensive cyber tools for military purposes. Not only does the political will of a state count, there are numerous technical questions that must be analysed in order to develop solutions for existing challenges. IT peace research can help in finding relevant solution strategies. Measures need to be developed that make it possible to monitor compliance with contractual partners, practically monitor military installations or track cyber weapon components such as software vulnerability attacks. As the history of arms control shows, it is a long way to go but an indispensable step towards peaceful development of a global domain (cf. Reuter, Aal, et al., 2019).

3.7 Laws

Challenge 7: The permanent adaption of international and national laws to new technologies seems to be a challenge; e.g. there is no agreement on the technological artefacts of cyber weapons, their quality and quantity that should be monitored.

An existing challenge is the adaption and implementation of (inter-)national laws in the sector of new technologies. So far, there is still no universally valid definition of the term "cyber weapon" and it remains unclear how they can be characterised. Thus, an unhindered upgrading is possible, like with many other weapons as well, but with cyber weapons even easier (cf. Reinhold & Reuter, 2020). Therefore, a control of cyber weapons in quality and quantity turns out to be challenging (cf. Rid & McBurney, 2012). Currently existing approaches to classify and define cyber weapons are mostly user-driven or actor-centred. Furthermore, they focus on the purpose and the application of vicious IT tools. Although all these terms such as "cyber weapon" are unclear, they are currently used for political arrangements, formulating norms for state behaviour and entering into documents (cf. Reuter & Reinhold, 2020). The aforementioned terms are therefore not capable to define and limit the subset of potential cyber weapons within the broad spectrum of malware prior to deployment. Essentially, this poses the most important challenge for the restriction and monitoring of particular military cyber technologies and their evolution, and for a limitation of inventory on cyber weapons. This aims to slow down and reduce the current militarisation of cyberspace.

Regarding espionage, there is uncertainty, too. Some scholars argue "that cyber espionage is more intrusive than traditional espionage, because it allows adversaries to repeatedly exfiltrate large amounts of information clandestinely", and it therefore "should be treated as (threat of) use of force or as an armed attack under the United Nations Charter in some situations" (Melnitzky 2012, p. 537), while other scholars "have suggested to create new laws to govern cyber espionage in particular" (in Herrmann, 2019, p. 85). As discussed, attribution and verification continue to pose problems, although they are indispensable for the enforcement of international law. Cyber defence faces legal dilemmas, not least because of lack of norms regarding pre-emption, prevention and counter-operations.

4. Discussion and Conclusion

This article highlights that information technology has a significant influence on warfare and military strategies (cf. Reuter, Riebe, Aldehoff, Kaufhold, & Reinhold, 2019). This makes clear that IT peace research should be expanded in the future. On the one hand, military forces are increasingly relying on cyberspace, creating capacities for offensive action in this domain and even, as in the case of the U.S., placing it in the centre of prospective warfare. On the other hand, there are still no adequate answers for the international regulation of cyber conflicts and the current dynamics of armament. This circumstance is owed to the permanent ambiguity in cyberspace, concerning its actors and the operations carried out: There are neither dividing lines between internal and external security nor can it be clearly determined which cyber resources can be assigned to defensive or offensive purposes. Even though espionage and even cyber attacks are regularly not seen as an act of war, some cyber incidents might cause serious tensions between two or more actors. According to Rid (2013) "cyber war will not take place" – for him, cyber war is a mythos, because war contains targeted violence against people, which has not existed in previous digital attacks. Nevertheless, the number of cyber attacks is constantly increasing worldwide. The particularities of cyberspace in the context of peace and security make it necessary to consider espionage and attacks separately in order to satisfy the complexity and ambiguity of the field.

This article suggested a definition of IT peace research, which might be considered as a (sub-)discipline, a field of research or an interdisciplinary research area. It is based on peace and conflict studies as well as computer science; furthermore, it is inspired by many other disciplines nearby. Central challenges, that have been elaborated in this article, include the insecurity, the variety of actors, the difficulty of attribution, verification and transparency, dual use, proliferation, and laws. Now, further steps and research are necessary in order to address at least some of them soon. To achieve this, a strong connection to both communities, peace and conflict research, as well as computer science is

needed, in order to combine the state of the art of both disciplines as a strong basis, and then to combine methods and research approaches from both areas to solve the complex problems at hand. Interdisciplinary research making contributions to the challenges described in this article, but also contributions to the individual disciplines, have to be fostered.

Christian Reuter is Full Professor for Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at the Technische Universität Darmstadt with a secondary appointment in the Department of History and Social Sciences. His research focuses on interactive and collaborative technologies in the context of crises, security, safety, and peace.

5. Bibliography

Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2018). Comprehensive survey on petya ransomware attack. *Proceedings – 2017 International Conference on Next Generation Computing and Information Systems, ICNGCIS 2017*, 131–136. https://doi.org/10.1109/ICNGCIS.2017.30.

Altmann, J. (2017). Einführung. In J. Altmann, U. Bernhardt, K. Nixdorff, I. Ruhmann, & D. Wöhrle (Eds.), *Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung* (pp. 1–7). Wiesbaden: Springer VS.

Altmann, J. (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.

Altmann, J., Kalinowski, M., Kronfeld-Goharani, U., Liebert, W., & Neuneck, G. (2010). Naturwissenschaft, Krieg und Frieden. In P. Schlotter & S. Wisotzki (Eds.), *Friedens- und Konfliktforschung* (pp. 410–445). Baden-Baden: Nomos.

Bernhardt, U., & Ruhmann, I. (2017). Informatik. In P. Imbusch & R. Zoll (Eds.), *Naturwissenschaft – Rüstung – Frieden* (pp. 337–448). https://doi.org/10.1007/978-3-658-01974-7.

Bundesministerium der Verteidigung (2016). *Abschlussbericht Aufbaustab Cyber- und Informationsraum*. Berlin, Germany.

Bonacker, T. (2011). Forschung für oder Forschung über den Frieden? Zum Selbstverständnis der Friedens- und Konfliktforschung. In P. Schlotter & S. Wisotzki (Eds.), *Friedens- und Konfliktforschung* (pp. 46–78). Baden-Baden: Nomos.

Boulding, K. E. (1963). Towards a pure theory of threat systems. *The American Economic Review*, *53*(2), pp. 424–434.

Brent, L. (2019). *NATO's role in cyberspace*. Retrieved from https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

Brinkel, G. (2018). *7 Stimmen zur Digital Geneva Convention*. Retrieved from https://www.microsoft.com/de-de/berlin/artikel/7-stimmen-zur-digital-geneva-convention.aspx.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Coy, W. (2001). Was ist Informatik? In *Das ist Informatik* (pp. 1–22). Berlin, Heidelberg: Springer.

Davis, J. S. I., Boudreaux, B., Welburn, J. W., Ogletree, C., McGovern, G., & Chase, M. S. (2017). *Stateless Attribution: Toward International Accountability in Cyberspace*.

Denning, P. J., Comer, D. E., Gries, D., Mulder, M. C., Tucker, A., Turner, A. J. O. E., & Young, P. R. (1989). *Computing as a discipline*. *32*(I), 9–23.

Denning, P. J., Comer, D. E., Gries, D., Mulder, M. C., Tucker, A., Turner, A. J., & Young, P. R. (1988). *Report of the ACM task force on the core of Computer Science*.

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), pp. 1213–1221. https://doi.org/10.1016/j.jss.2012.02.033.

FONAS. (2015). Forschungsmemorandum – Naturwissenschaftliche Friedensforschung in Deutschland – Eine neue Förderinitiative ist dringend nötig. Dortmund, Forschungsverbund Naturwissenschaft, Abrüstung und internationale Sicherheit e.V.

Gleditsch, N. P., Nordkvelle, J., & Strand, H. (2014). Peace research – Just the study of war? *Journal of Peace Research*, *51*(2), pp. 145–158. https://doi.org/10.1177/0022343313514074.

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

Herrmann, D. (2019). Cyber Espionage and Cyber Defence. In *Information Technology for Peace and Security* (pp. 83–106). Wiesbaden: Springer vieweg.

ISO. (2013). *ISO/IEC 27001: 2013: Information Technology-Security Techniques--Information Security Management Systems--Requirements*. Retrieved from https://www.iso.org/standard/54534.html.

Koppe, K. (2006). Zur Geschichte der Friedens- und Konfliktforschung im 20. Jahrhundert. In P. Imbusch & R. Zoll (Eds.), *Friedens- und Konfliktforschung. Eine Einführung* (pp. 17–66). Wiesbaden: VS Verlag für Sozialwissenschaften.

Leng, C. (2013). *Die dunkle Seite: Informatik als Dual-Use-Technologie*. Berkeley.

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.

Melnitzky, A. (2012). *Defending America against Cyber Espionage Through the Use of Active Defenses*. 20 Cardozo J. Int'l and Comp. L.,

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

NATO. (2019). Collective defence – Article 5. Retrieved from https://www.nato.int/cps/en/natohq/topics_110496.htm

Neuneck G. (2011). Frieden und Naturwissenschaft. In B. Rinke & H.J. Gießmann (Ed.), *Handbuch Frieden*. Wiesbaden, VS Verlag für Sozialwissenschaften.

Kanno-Youngs, Z. & Perlroth, N. (2020). Iran´s Military Response May Be ´Concluded´, but Cyberwarfare *Threat Grown*. Retrieved from https://www.nytimes.com/2020/01/08/us/politics/iran-attack-cyber.html.

Newell, A., Perlis, A. J., & Simon, H. A. (1967). Computer science. *Science*, *157*(3795), 1373–1374.

Reinhold, T. (2015). Möglichkeiten und Grenzen zur Bestimmung von Cyberwaffen. In: Cunningham, D. W., Hofstedt, P., Meer, K. & Schmitt, I. (Hrsg.), INFORMATIK 2015. Bonn: Gesellschaft für Informatik e.V. (pp.587-596).

Reinhold, T. (2018). Hack der deutschen Regierungsnetze. Retrieved from Datenbank Relevante Cybervorfälle website: https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/hack-der-deutschen-regierungsnetze/.

Reinhold, T., & Reuter, C. (2019). Verification in Cyberspace. In C. Reuter (Ed.), *Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden, Germany: Springer Vieweg.

Restivo, S., & Denton, P. H. (2008). *Battleground Science and Technology*. California: Greenwood Press.

Reuter, C., Altmann, J., Göttsche, M., Himmel, M. (2020). Zur naturwissenschaftlich-technischen Friedens- und Konfliktforschung: Aktuelle Herausforderungen und Bewertung der Empfehlungen des Wissenschaftsrats. ZeFko, 9(1), 2020.

Reuter, C. (2019). Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden, Germany: Springer Vieweg. https://link.springer.com/book/10.1007/978-3-658-25652-4

Reuter, C., Aal, K., Aldehoff, L., Altmann, J., Bernhardt, U., Buchmann, J., Katzenbeisser, S., Kaufhold, M.-A., Nordmann, A., Reionhold, T., Riebe, T., Ripper, A., Ruhmann, I., Saalbach, K.-P., Schörnig, N., Sunyaev, A., Wulf, V. (2019). The Future of IT in Peace and Security. In *Information Technology for Peace and Security* (pp. 405–413). Springer.

Reuter, C., Aldehoff, L., Riebe, T., & Kaufhold, M.-A. (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.

Reuter, C., & Kaufhold, M.-A. (2018). Informatik für Frieden und Sicherheit. In C. Reuter (Ed.), *Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement* (pp. 577–597). Wiesbaden: Springer Vieweg.

Reuter, C., & Reinhold, T. (2020). On the nature of cyber weapons. In *Information Technology for Peace and Security*. Wiesbaden, Germany: Springer Vieweg.

Reuter, C., Riebe, T., Aldehoff, L., Kaufhold, M.-A., & Reinhold, T. (2019). Cyberwar zwischen Fiktion und Realität – technologische Möglichkeiten. In I.-J. Werkner & N. Schörnig (Eds.), *Cyberwar – die Digitalisierung der Kriegsführung* (pp. 15–38). https://doi.org/10.1007/978-3-658-27713-0.

Rid, T., & Buchanan, B. (2014). Attributing Cyber Attacks. *The Journal of Strategic Studies*, *38*(1–2), pp. 4–37. https://doi.org/10.1080/01402390.2014.977382.

Rid, Thomas (2013). Cyber war will not take place, Oxford University Press.

Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal*, *157*(1), pp. 6–13. https://doi.org/10.1080/03071847.2012.664354.

Riebe, T., & Reuter, C. (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* (p. 165-184). Wiesbaden, Germany: Springer Vieweg.

Saalbach, K.-P. (2019). Attribution of Cyber Attacks. In *Information Technology for Peace and Security* (pp. 279–303). Wiesbaden: Springer Vieweg.

Sokolski, H. D. (2004). Getting Mad: Nuclear Mutual Assured Destruction, Its Origins and Practice. In *Strategic Studies Institute*.

Storey, N. (1996). *Safety Critical Computer Systems*. London: Addison-Wesley Longman.

Thee, M. (1988). Science and Technology for War and Peace. *Bulletin of Peace Proposals*, *19*.

UNIDIR. (2013). *The Cyber Index – International Security Trends and Realities 2013*. Geneva: United Nations Institute for Disarmament Research (UNIDIR).

United States Department of Defense (2011). *Strategy for Operating in Cyberspace*. Retrieved from https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

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

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, pp. 97–102. https://doi.org/10.1016/j.cose.2013.04.004.

Wheeler, D. A., & Larsen, G. N. (2003). *Techniques for Cyber Attack Attribution*. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf.

Wissenschaftsrat. (2019). *Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung, (Drs. 7827-19)*. pp.1–178. Retrieved from https://www.wissenschaftsrat.de/download/2019/7827-19.html.

The State of Cyber Arms Control. An International Vulnerabilities Equities Process as the Way to go Forward?*

Matthias Schulze

Abstract: Although the threat of cyber-conflict is rising at the moment, not much ground has been gained with cyber arms control regimes. The article analyses proposals for cyber arms control, modelled after traditional arms control regimes. It finds that challenges of the digital domain, issues of regime verification and the lack of political will are big inhibitors in transferring these to the cyber-domain. To overcome these inhibitors, cyber-experts proposed a new type of regime focusing on Zero-day vulnerabilities. Since nobody so far explained how a so-called International Vulnerabilities Equities Process (IVEP) could look like, the article picks up the task, and presents two models with their advantages and shortcomings. The article concludes that the IVEP proposal holds some promise, but due to many open questions, it is currently not feasible as a policy option.

Keywords: International Vulnerability Equities Process, arms control, cyber-security, zero-day vulnerability
Schlagwörter: International Vulnerability Equities Process, Rüstungskontrolle, Cyber-Sicherheit, Sicherheitslücken

1. Introduction

Since the late 1990s, there have been multiple efforts to restrict collateral damage from cyber-attacks. One approach is adopting international law and the law of armed conflict for the cyber-domain (UN Governmental Group of Experts and Tallinn-Manual-Process). Closely connected are initiatives to establish informal, non-binding norms of appropriate state behavior in cyber-space (Henriksen, 2019). Another approach focuses on establishing trust and Confidence Building Measures (Pawlak, 2016). There are industry initiatives such as the Microsoft Digital Geneva Convention and first bilateral cyber-treaties. No substantial ground has been gained in terms of cyber arms control regimes. There is certainly demand for such a regime since quantitatively and qualitatively the collateral damage of cyber-attacks is rising, and cyber-crime is causing an annual damage of billions of dollars and cyber-espionage, intellectual property theft and cyber-enabled influence operations have become a nuisance in international affairs (Nye, 2015). A full-fledged international cyber regime or treaty defining binding rules of behavior is nowhere in sight. The scope of the article is to give an overview of current debates about cyber arms control regimes. The research question of the first section is: what factors inhibit the transfer of traditional arms control models to the cyber-domain? Three inhibitors are identified: an unclear object of regulation, lacking means of verification, and lacking political will.

Because of these inhibitors, cyber experts proposed to refocus arms control not on cyber-weapons, but on their ammunition – zero-day vulnerabilities in hard- and software (Mallory 2019). Experts proposed an International Vulnerabilities Equities Process (IVEP), modeled after national VEP processes. With these VEP governments decide whether to use zero-day vulnerabilities for own cyber-offense, or whether to disclose them to the software vendor, increasing cyber-defense. However, to this date, there is no explanation on how an IVEP could actually look like. The article takes this very first step and tries to answer this question by proposing two different models. It then assesses some implementation challenges. It is the hope that the assessment serves as a groundwork to trigger future analysis and debate, thus moving the abstract international discussion about a cyber-regime forward.

2. Challenges to Cyber-Arms Control Regimes: Literature Review

Arms control regimes historically have multiple goals, such as to ban or reduce certain types of weapons (disarmament) or military behavior (like testing, use or deployment) to prevent conflict and try to limit the acceleration and the cost of arms races (Reinhold & Reuter, 2019, p. 209). They also aim to reduce uncertainty, mistrust and security dilemmas between states.

Scholars proposed to use traditional arms control regimes as a blueprint model for cyber arms control. Models discussed include the nuclear arms control regime (Borghard & Lonergan, 2018), which is generally regarded as impractical because unlike nuclear arsenals, cheap and easy to conceal malware stockpiles cannot be effectively measured (Nye, 2015). Others propose to utilize the Comprehensive Test Ban Treaty (CTBT), which restricts the testing of nuclear explosions. The CTBT features a joint monitoring system which allows measuring compliance, even for smaller states with little measuring capability. Eilstrup-Sangiovanni argues that this might help to overcome the attribution problem, i.e. difficulties of identifying the originator of a cyber-attack, often due to unequal cyber-forensic capabilities of states (Eilstrup-Sangiovanni, 2018). A joint monitoring system refers to a proposal of an international attribution agency that would analyze cyber-incidents and would try to collectively "name and blame" culprits (Davis, 2017). Others propose to use the Geneva Protocol (Dumbacher, 2018) or the later Biological and Toxin Weapons Convention (BWC) that ban the use of chemical and biological weapons (Fidler, 2015; Reinhold & Reuter, 2019). These regimes face comparable issues as the cyber-domain, i.e. the dual-use nature, easy proliferation and issues of attribution, verification, compliance. Geers argues that the Chemical Weapons

* This article has been double blind peer reviewed. The author is grateful for the constructive feedback by the anonymous reviewers.

Convention (CWC) of 1997 features strong verification measures, but that these cannot be easily transferred to the cyber-domain (Geers 2010). Reuter and Reinhold come to similar conclusions with the BWC (Reinhold & Reuter, 2019, pp. 212–213). This reason and the fact that the chemical industry torpedoed the ratification in the USA explain why the Geneva Protocol failed (Dumbacher, 2018). Private sector participation in cyber-arms control seems necessary since an estimated 95% of the digital infrastructure is run by corporations and not states.

By analyzing these studies, one can deduce at least three inhibiting factors that explain why transferring traditional arms control to the cyber-domain is difficult. The first inhibiting factor is that it remains unclear what exactly the object of regulation in any type of cyber arms control regime would be. Arms control traditionally focuses on restricting certain objects, like poison gas, or they focus on restricting behavior, like nuclear-testing (Arimatsue, 2010). There is no consensus on whether digital software qualifies as an object or even a weapon (Tikk, 2017). More so, states hold different perceptions about the permissiveness of behavior like economic vs. political cyber-espionage or cyber-crime. Many famous cyber-intrusions are not based on technical, but rather on social manipulation. When focusing on objects like malware, more issues arise because "malicious code is notoriously difficult to define" (Geers, 2010, p. 559). The code is changeable, and its characteristics may look different after an update. It is also modular, meaning that individually harmless or legitimate components can be bundled together to create emergent effects. For example, encryption normally enhances cyber-security unless it is "weaponized" in form of ransomware. Code is dual-use. Tools used for cyber-offense are often necessary for cyber-defense as well. Additionally, a clear-cut distinction between military, criminal and civil code is hard to achieve. Some "living off the land" cyber-attacks rely entirely on pre-installed software like the Windows PowerShell. Banning or regulating software designed for cyber-offense might impede cyber-defense, like vulnerability research and ethical hacking (Dumbacher, 2018, p. 208).

Malware with kinetic effects like Stuxnet can, under some circumstances, be considered a cyber-weapon (Rid, 2018, pp. 73–75). However, unlike a warhead with a predetermined destructive capacity, the potential effect of a malware depends on the configuration of the target. Malware can hardly kill humans directly unless the targeted IT-system has capabilities to inflict physical harm. These conceptual difficulties imply arms control mechanisms that focus on fixed characteristics of an object "fall short in the digital age" (Dumbacher, 2018, p. 221).

The second inhibiting factor is verification (Tikk, 2017). To be effective, arms control regimes need to verify that regime members adhere to the agreed principles outlined in a treaty. Historically, this is done via on-site inspections, sensors, areal imaging and data exchange (Reinhold & Reuter, 2019). However, there is no easy way of measuring the relative strength of malware arsenals and cyber-power. A small group of high-skilled hackers might be able to inflict more damage than a large, but medium-skilled cyber-battalion. Asymmetries in cyber-power and different cyber-capabilities of states in detecting and defending attacks also are an inhibitor for verification because lesser cyber-powers cannot hold more potent states accountable. The attribution problem and high levels of secrecy surrounding cyber-espionage activities further complicate things (Borghard & Lonergan, 2017, p. 465). Everyone with sufficient knowledge can write malware on any computer around the world (Geers, 2010, p. 550). Malware is cheap and being sold on a thriving black market (Ablon, Libicki, & Golay, 2014). Additionally, there is a gray market where the traditional arms industry develops and sells malware to the highest bidder (Burgers & Robinson, 2018). Malware is easy to conceal, highly intangible, can be easily copied and cannot be destroyed. Because of these properties, proliferation is easy and permanent dismantling of software unfeasible.

For states to agree to a cyber-regime, the cost and benefit calculus of verification systems must hold up (Eilstrup-Sangiovanni, 2018, p. 391). A cyber-verification regime might come with unacceptable costs since it would technically imply a global surveillance infrastructure that monitors what is happening on every single digital device on the planet. Global surveillance programs (Ruhrmann, 2015, p. 572) that do a deep-packet inspection of dataflows at large Internet choke-points could serve that function (Geers, 2010). Likewise, infrastructures for active cyber-defense, i.e. observing adversary behavior and capability at his/her network could serve a similar function (Schulze & Herpig, 2018). Active-defense in foreign networks, even for verification or compliance monitoring, would be highly intrusive. It would run diametrically against cyber-security initiatives by states, which is keeping adversaries outside of their networks. The cost of compliance with such a verification system, thus, might be higher than the actual reduction of risk that follows from such a mechanism, especially for highly digitized economies (Ford, 2010).

The third inhibiting factor is the lack of political will. Many states regard cyber-space as an offense-dominant environment (Eilstrup-Sangiovanni, 2018, p. 384). Therefore, states do not perceive it to be in their self-interest to restrict their offensive cyber-capabilities (Dumbacher, 2018). Historically, shock situations, like the Cuban Missile crisis sometimes lead to increased political will. It is unclear whether or not such a situation is likely to occur. "Cyber-weapons" are simply not dangerous enough, at least compared to nuclear weapons (Burgers & Robinson, 2018). Even if political momentum for regulation arises, it is unlikely that states will restrict their cyber-espionage activities. States historically lack the will to restrict peacetime espionage, which is why it is neither explicitly condoned nor condemned in international law (Radsan, 2007). Cyber-attacks and cyber-espionage share many characteristics and cannot be meaningfully separated from another (Lindsay, 2013, p. 370). The intrusion chain between the two is nearly identical and only the effect of the payload differs. Because of the modular nature of malware, an espionage operation can turn into a destructive payload just with a click of a button (Buchanan, 2017, pp. 84–85). This has implications for verification. If cyber-espionage and destructive cyber-attacks cannot be technically separated from one another, any regime trying to restrict one type of behavior should logically restrict the other as well – or it would include major blind-spots. Most states will not give up their cyber-espionage capacity because it increases their strategic posture by generating intelligence. Research shows that unless arms control regimes and the overall strategic posture go hand-in-hand, they are no feasible policy option (Eilstrup-Sangiovanni, 2018, p. 381).

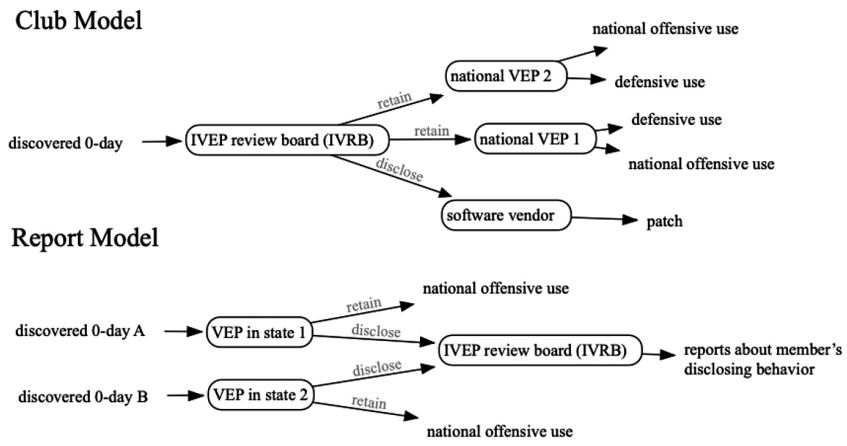
3. Is an International Vulnerability Equities Process the Way Forward?

To overcome these inhibitors, scholars suggested to focus arms control not on cyber-weapons but rather on their ammunition – software vulnerabilities (Fidler 2015). Zero-day vulnerabilities are errors in a soft or hardware code that the vendor is not aware of and that, at time of discovery by researchers, is not fixed by a patch. Zero-day attacks utilizing this vulnerability, in principle, allow undetectable intrusions and are typically used for high-profile sabotage and cyber-espionage operations. If a software vendor fixes a zero-day vulnerability with a patch, it becomes an N-day vulnerability that is publicly known. N-day cyber-attacks only work against unpatched systems.

Zero-days are interesting for an arms control approach because they may overcome one central inhibitor, which is the lack of political will. Currently, we are witnessing the trend that states start to restrict their zero-day use. The USA, the United Kingdom, Australia, Canada, and China have published so-called Vulnerability Equities Processes (VEPs), while other countries like Germany are working on one (Herpig & Schwartz, 2019). VEPs are national, administrative processes that gauge the offensive and defensive value of zero-day vulnerabilities for cyber-offense and defense. For that purpose, an inter-agency review board including both cyber-offense (intelligence agencies, military) and cyber-defense actors is created. The board tries to answer whether a government-obtained zero-day vulnerability is kept secret and being utilized for cyber-offensive purposes, or whether the knowledge of this vulnerability is being disclosed to the software vendor, thus increasing cyber-defense. If a vulnerability is being disclosed, the respective software vendor ideally patches the vulnerability, and thus provides immunization against any further attacks. 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 zero-days that entail little risk (Healey, 2016). Vulnerabilities in the core Internet protocols would entail global and collective risks, while others, software in country-specific military equipment, only entail localized risks.

Since states started to restrict zero-days for their own cyber-offense, this momentum could be used to expand into an International Vulnerabilities Equities Process (IVEP) (Mallory, 2018; Fidler, 2014). There have been very abstract and general calls for an IVEP from policy experts, but to date no one has really presented a format of how a specific IVEP can look like (United Nations Institute for Disarmament Research, 2018). Since there is no systematic, prior research on the subject, the author takes the first step and presents two different models in an attempt of original research (Figure 1). These models were deduced from the institutional design of the national VEP in the US (Healey 2016, p. 4). Comparative research on VEPs indicates some best practices for VEP design. In most national VEPs, a vulnerability-researching entity discloses a discovered zero-day vulnerability to some sort of review board, which then decides, based on agreed indicators, how to proceed, either disclosing or retaining a vulnerability (Herpig, 2018, p. 17). From this it follows logically, that an *international* VEP requires an international body, which potentially consists of member states that are involved in the equities deliberation at some stage. Therefore, national and international equity boards need to be aligned to create an IVEP. If one takes this as a foundation, there are only two logical ways to implement this: either having an International Vulnerability Review Board (IVRB) as the first stage of a vulnerability review process, and the national VEP as the second stage, or vice versa.

Figure 1. IVEP Models



In the first model, an international vulnerability review board would serve as the first stage in the process. In other words, the IVRB decision to retain or disclose vulnerabilities would be upstream to any national VEP decision. In this model, researchers or other governments would disclose the zero-day vulnerabilities they found to the IVRB. That board then would decide, akin the national VEPs, whether to disclose this vulnerability to the vendor for patching, or whether knowledge of this vulnerability is retained. The internal governance structure of the IVRB, i.e. questions of external expert participation or voting modalities, can follow best practices from national VEPs (Herpig 2018). If the IVRB decides to retain the knowledge of a reported vulnerability, it would then, in a second stage, share this knowledge with the member states of the IVRB. This would give them exclusive access to a zero-day vulnerability. Member states could exploit this knowledge for own cyber-attacks, giving them a temporal offensive edge. Alternatively, they could immunize their systems or upgrade their intrusion detection systems based on this knowledge. This would provide them with a head-start against future attacks that might exploit this vulnerability, while it remains unpatched. Due to this mechanism, less potent cyber-states might have access to more zero-days to use and it would provide all members with a better situational awareness of zero-days being in circulation. This type of defensive sharing could be modeled after already existing threat-sharing programs in cyber-security, for example, the Zero Day Initiative. Threat indicators to detect certain types of attacks are often shared in

exclusive circles with limited access (Traffic Light Protocol). This fact makes the club model politically feasible, because some of the required infrastructure already exists. Fidler argues that this would only work in high-trust environments of like-minded states like NATO (Fidler, 2014, p. 162). Membership in the IVRB would thus be exclusive, which is why I call this the club model. In a club model, governance issues such as membership, meeting-schedules and voting modalities can probably be agreed on more easily. This model could also include further rules, for example, that members would not attack each other with the shared zero-days. Withholding access to this exclusive vulnerability sharing model could serve as a sanction instrument.

There are downsides to the club model. First, there is potential for spoilers. If the IVRB decides to retain a vulnerability for exclusive club-sharing, a spoiler state could disclose this vulnerability to the vendor anonymously with plausible deniability. This would counteract the IVEP's decision. Another downside is that it adds another layer of complexity to the already existing vulnerability disclosure infrastructure. It would be always more efficient for researchers to disclose vulnerabilities to vendors directly instead of going through an additional layer of international bureaucracy. Ethical hackers would certainly not contribute to any regime that favors cyber-offense over defense. Spoiler states could also feed bogus or non-critical zero-day information into the process, to slow it down. Another unresolved issue is how to verify compliance in such a regime.

In the second model, the IVRB would be set up downstream to any national VEP. Therefore, the IVRB would collect information about the disclosing behavior to software vendors by national VEP review boards within the member states. Any member with a national VEP would have the obligation to share with the IVRB all the vulnerabilities its national review board decided to disclose to vendors. If a national VEP retains a zero-day vulnerability, it would not be shared and could be used for national offensive. The IVRB would then draft reports about the disclosing behavior of member states, collecting general statistics as well as some characteristics about disclosed vulnerabilities. The reporting of national VEP to the IVRB, of course, must be standardized. It could be modeled after declaration policies in other regimes, such as the Chemical Weapons Convention. In the CWC for example, states must declare national chemical production facilities and output quantities. Similarly, states in an IVEP regime could declare quantities of vendor-disclosed zero-days to the IVRB.

This information can help member states to determine the quality and quantity of disclosed vulnerabilities, thus giving some insight into the relative strength and cyber-power of others. Even the information about disclosed vulnerabilities can tell an adversary a lot about intended targets, capacity, and skill of a cyber-offense actor (Aitel & Tait, 2016). For an international regime, this "meta-data" on vulnerabilities could create shared situational awareness and serve as a confidence-building measure. By sharing only meta-data about disclosed vulnerabilities, national operational capacity for cyber-offense would not be harmed, because highly potent zero-day exploits would not be shared with the IVRB anyway. This fact allows membership to be more inclusive, integrating even antagonists in the IVRB structure.

This idea also has its disadvantages. The problem of complexity remains the same. Since the second model excludes the most potent zero-days, which would not be reported to the IVRB, it reduces harmful zero-day operations only by a fraction. This also reduces the value of participation in this structure compared to the club model. Reports about disclosed vulnerabilities are operationally less valuable compared to the sharing of potent zero-day information among club members. This would also reduce the sanctioning power of such a regime, because withholding these reports to non-compliant states would imply tolerable costs. The general problem of verification remains the same as in the club model. Then there is the issue of free-riding: one state disclosing a lot while others disclosing nothing or little of value. The incentive structure of this proposal is still a problem. More so, focusing on governments alone, the private sector is mostly being excluded from this dynamic.

4. Discussion

How does an IVEP regime score against the previously identified inhibitors of adopting traditional arms control regimes to the cyber-domain? First, a regime focusing on zero-days has the advantage, that the object of regulation is straight-forward. The definition of zero-days is not really contested.

Second, a regime prohibiting the use of zero-day attacks could overcome the challenge of lacking political will and self-interest. Many states agree that zero-days are highly problematic and many initiatives for cyber-norms and confidence-building measures also focus on them (Pawlak, 2016). Restricting only zero-days while allowing the use of N-days and phishing would still leave states with enough room to maneuver for limited offensive operations. Not giving up all, but only the most dangerous cyber-attack capability might serve the interest of states.

Third, an arms control regime focusing on zero-days could partly facilitate the involvement of the private sector. Software companies are the primary emitters of zero-day vulnerabilities, but they are also the main responsible actors for patching. There already exists a worldwide ecosystem and infrastructure for coordinated vulnerability disclosure to vendors, such as bug-bounties (Schulze, 2019). Building on this existing structure could reduce opportunity costs in setting up a regime.

Fourth, an IVEP regime could help to mediate asymmetries in cyber-power and different capabilities of states. By sharing offensive information, the playing field could be leveled, at least for members in the club model. The report model would only enhance situational awareness and knowledge about attack capabilities a bit.

Like the other proposed cyber-regimes, an IVEP falls short in terms of reliable and unobtrusive verification, as well as attribution and enforcement of sanctions for non-compliant behavior. Since zero-day attacks are by nature not detectable if one does not possess the knowledge about the attack vector, the attribution problem remains (Rid & Buchanan, 2014). The proposals also do not really address the aspect of espionage and the dual-use nature of zero-day capabilities. Lastly, they imply a large bureaucratic overhead while addressing only a tiny portion of cyber-attacks.

5. Conclusion

The article presented the first step in the conception of an IVEP regime that has been called for by cyber-experts. It presented two models of how such a regime could look like. The IVEP proposal holds some promise, but due to many open questions, it is currently not feasible as a policy option. There remain several issues.

First, future research should investigate alternative models for an IVEP. Could there be a model that fares better than the two presented? Maybe disclosing vulnerabilities to a centralized international body is the wrong way? Second, more research needs to be done on incentive structures of the two presented models. How do we overcome the issue of spoilers not sharing vulnerability information with an IVRB? Does it make sense to adopt monetary mechanisms like bug-bounty or reward programs for an IVEP regime? Where would the IVRB get the funding from? Third, one could think about expanding the mandate of an IVRB, for example by adding a capacity-building function: potent cyber-powers could help lesser-developed states with the mitigation of reported zero-days. That could be an option for the club model, but maybe not necessarily for the report model. This could be an incentive for smaller states to participate. Fourth, an alternative could be to rethink an IVEP not as a full-fledged regime but as a confidence-building-measure.

The findings presented here are only a first step to move the abstract international discussion about IVEPs forward. Future research must show whether a vulnerability regime is indeed the way forward to enhance peace and security in the cyber-domain.

Matthias Schulze is a researcher at the security division of the German Institute for International and Security Affairs – SWP. His research fo-cuses on the strategic use of cyber-capabilities in international relations, cyber-conflicts, cyber-espionage and information operations. He hosts the percepticon.de podcast.

6. Bibliography

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, from Lawfare: 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 C. Czosseck & K. Ziolkowski (Eds.), 4th International Conference on Cyber Conflict. Tallinn.

Borghard, E. D., & Lonergan, S. W. (2017). The Logic of Coercion in Cyberspace. Security Studies, 26(3), 452–481.

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

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

Burgers, T., & Robinson, D. R. S. (2018). Keep Dreaming: Cyber Arms Control is Not a Viable Policy Option. Sicherheit & Frieden, 36(3), 140–145.

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

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

Eilstrup-Sangiovanni, M. (2018). Why the World Needs an International Cyberwar Convention. Philosophy & Technology, 31(3), 379–407.

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. Journal of law and Policy for the Information Society, 11(2), from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2706199.

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

Geers, K. (2010). Cyber Weapons Convention. Computer Law & Security Review, 26(5), 547–551.

Healey, J. (2016). The U.S. Government and Zero-Day Vulnerabilities.: From Pre-Heartbleed to Shadow Brokers, from https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process.

Henriksen, A. (2019). The end of the road for the UN GGE process: The future regulation of cyberspace. Journal of Cybersecurity, 5(1), 425.

Herpig, S. (2018). Governmental Vulnerability Assessment and Management: Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities. Berlin: Stiftung Neue Verantwortung, from https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf.

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

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404.

Mallory, J. C. (2018). Cyber arms control: risk reduction under linked regional insecurity dilemmas, from Institute for International and Security Studies: https://www.iiss.org/events/2018/09/cyber-arms-control.

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

Pawlak, P. (2016). Confidence-Building Measures in Cyberspace Current Debates and Trends. In A.-M. Osula & H. Roigas (Eds.), International Cyber Norms. Legal, Policy & Industry Perspectives. Tallinn.

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

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

Rid, T. (2018). Mythos Cyberwar: Über digitale Spionage Sabotage und andere Gefahren. Hamburg: Edition Körber.

Rid, T., & Buchanan, B. (2014). Attributing Cyber Attacks. Journal of Strategic Studies, 38(1-2), 4–37.

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

Schulze, M. (2019). Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik. Stiftung Wissenschaft und Politik, from https://www.swp-berlin.org/10.18449/2019S10/.

Schulze, M. & Herpig, S. (2018). Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them, from Council on Foreign Relations: https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them.

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

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

Sharing of Cyber Threat Intelligence between States*

Philipp Kuehn, Thea Riebe, Lynn Apelt, Max Jansen, Christian Reuter

Abstract: Threats in cyberspace have increased in recent years due to the increment of offensive capabilities by states. Approaches to mitigate the security dilemma in cyberspace within the UN are deadlocked, as states have not been able to achieve agreements. However, from the perspective of IT-Security, there are Cyber Threat Intelligence (CTI) platforms to share and analyze cyber threats for a collective crisis management. To investigate, if CTI platforms can be used as a confidence-building measure between states and international organizations, we portray current CTI platforms, showcase political requirements, and answer the question of how CTI communication may contribute to confidence-building in international affairs. Our results suggest the need to further develop analytical capabilities, as well as the implementation of a broad social, political, and legal environment for international CTI sharing.

Keywords: Cyber Threat Intelligence, confidence-building measures, cyberspace, International System
Schlagwörter: Informationen zu Cyberbedrohungen, Maßnahmen der Vertrauensbildung, Cyberraum, internationales System

1. Introduction

Incidents in cyberspace have increased in the last decade (Symantec Corporation, 2019). The tremendous use of cloud services, mobile computing, and Internet of Things (IoT) add to this pressure, even between states. Given the cyberspace's militarization with state-owned cyber weapons like Stuxnet (Falliere et al., 2011) or NotPetya (McQuade, 2018), and an associated cyber security dilemma (Buchanan, 2017), some observers warn of the dangers the competition for digital supremacy and a conjoint cyber arms race could bring (Pawlak, 2016). Hence, there is a growing demand for cyber threat intelligence (CTI) sharing and IT peace research by experts to support the management of threat indicators within organizations and the IT security community (Dandurand & Serrano, 2013; Reuter, 2020; Skopik et al., 2016, 2018). Such CTI sharing would increase the cyber situational awareness (CSA) of all participants to be able to react to threats in a timely manner (Páhi et al., 2017). Even if there are ways to decrease the aforementioned tension in the international system, however not yet in cyberspace. Confidence-building measures (CBMs) have shown to be a well suited operational measure to decrease the strains between hostile states, even in times of conflict, since they are a voluntary measure (Meyer et al., 2015). They support mutual communication and cooperation on the operational level, below the political level. CBMs date back to 1975 with the OSCE's Helsinki Final Act and have been established in its current form by the OSCE's Vienna Document in 1990. They are a tool that aim to provide transparency on military doctrines, resources by improved communication and contacts between government officials. As a result, they contribute to stability, transparency and a restrain of offensive behavior (Pawlak, 2016). Other options to decrease the instability, and with it, possible conflicts, are multilateral arms-control treaties. But the negotiations for such treaties are currently deadlocked, partly due to the difficulties to agree on a definition of cyber weapons (Dickow et al., 2015). This deadlock of the top-down approach to find agreeable definitions and procedures leads to the increase of unregulated cyber operations by states, as there are little restrains not to.[1] As a result, the security of critical national infrastructure (CNI) remains highly at risk. However, as CBMs in other security-critical areas such as nuclear technology have shown (Altmann, 2019), this problem can be approached by initiating a bottom-up approach from the operational and technical perspective, which combines the organizational and technical approaches of IT-Security and CBMs. Respective international efforts for collaboration to simultaneously face threats are a vibrant topic that will be of key importance for the coming decade (Mohaisen et al., 2017).

Already, organizations collect, analyze and sometimes share cyber threat information. Cyber threat information is any information which can "help an organization identify, assess, monitor, and respond to cyber threats" (Johnson et al., 2016). They must be (i) relevant, (ii) timely, (iii) accurate, (iv) complete, and (v) ingestible, *i.e.*, they must be actionable (ENISA, 2015). Through sharing such information, organizations can improve their own security postures, as well as those of other organizations (Johnson et al., 2016). Thus, states exchanging such information would have similar benefits. Sharing, processing, and analyzing threat information is done in so-called CTI platforms, which are either federated platforms, *i.e.*, hosted by each organization itself, offering an interface for exchanging their information with each other, or used as a platform-as-a-service, *i.e.*, running in the cloud. They differ from simple data-warehouses based on their analytical capabilities, which mitigate or even remove the potential of information overload (Kaufhold et al., 2019). Shortcomings of such platforms have been discussed in prior work (Sauerwein et al., 2017; Skopik, 2016). Furthermore, developing a CTI platform faces diverse challenges, such as a lacking common terminology (Pawlak, 2016), privacy issues, as well as the reluctance by states to share security-related information (Badsha et al., 2019). Nonetheless, CTI sharing is a vital ingredient for a more secure cyberspace: due to (i) the edge of states knowing of upcoming cyber threats and (ii) the necessary communication and associated confidence building of nations about them. Besides building confidence by communicating about current threats, the publisher of threat information offers insights into the own security by giving hints in which way a state/an entity is vulnerable to them, which in itself offers or shows trust in partners.

* This article has been double blind peer reviewed. The authors thank all (anonymous) reviewers for their helpful comments and remarks.

1 Reasons for the regulative deadlock can be found in foreign and domestic policies interests which create the cyber security dilemma (Buchanan, 2016, 2017; Dunn Cavelty, 2014).

DOI: 10.5771/0175-274X-2019-4-22

Since current CTI platforms are designed with the aim to function as inter-organizational CTI sharing tools, this article strives to answer the research question: *(i) Can CTI sharing contribute to confidence building between states, and (ii) what are technical and organizational requirements by states to use CTI sharing?* Section 2 outlines the applied research methodology. Section 3 presents our findings for platforms (Section 3.1), as well as requirements defined by academics, states, and international organizations (Section 3.2). Our evaluation of identified platforms in accordance with the obtained requirements is presented in Section 4. The concluding Section 5 highlights various approaches for future research.

2. Research Methodology

To investigate the issue at hand, a combination of scientific literature and so-called grey literate is used in the review process. Scientific literature in the fields of Cyber Studies and Research, Science and Technology Studies as well as International Intelligence and Security Studies constituted the core background for this analysis. Since cyber threat (intelligence) is a matter of academic interest, but even more a matter for the private sector such as state-employed or private IT operators, the used review process minimizes the gap between research and the private sector and provided a more comprehensive picture of state-of-the-art technology in this particular field.

The literature search was conducted using the following search engines: ACM Digital Library, IEEE Xplore Digital Library, Google Scholar, and Google. The search-term deeply affiliates with the question at hand, *i.e.*, cyber (threat, exchange, platform, security, intelligence), cyber sharing (platform, tool), and cyber (space, warfare) confidence (building). Using these search terms, we used a snowball sampling technique to identify relevant literature in this field and drew on earlier works related to threat intelligence sharing, *e.g.*, Sauerwein et al. (2017). Handling our procedure openly allowed us to focus on search results most promising in regard to inter-state CTI sharing.

Using this method, we identified 40 relevant CTI platforms (see Table 1) as well as requirements for CTI sharing (platforms) as possible CBMs measures in inter-state cyberspace covering both the scientific and political field. All requirements were deduced from the obtained sources as well as official documents by regional, bi- and multilateral arrangements (see Section 4.2).

This material was used as a starting point for our investigation into current CTI sharing platforms and their potential use for confidence building between states. Similar to Sauerwein et al. (2017), we analyzed our platform sample according to a variety of perspectives, *e.g.*, (i) use cases, (ii) supported threat intelligence constructs, (iii) collaboration capabilities, and (iv) level of analysis. Additionally, we applied a list of certain criteria with special importance for inter-state confidence building (see Section 3.3).

In this context, we analyzed the sample on how the included platforms comply with the identified criteria and evaluate their potentials as tools for interstate confidence building in cyberspace (see Section 5).

Table 1: Identified platforms/data-/tool-sets

Name	Acronym	Free-to-use	Open-source	maintained	selection
Accenture Cyber Intelligence Platform				✓	
Anomali Threat Platform				✓	
Anubis Networks Cyberfeed				✓	
Automated Indicator Sharing	AIS	✓		✓	
AutoShun		✓		✓	
Barncat		✓		✓	
Bearded Avenger	BA	✓	✓	✓	✓
Blueliv Threat Exchange Network		✓		✓	
CheckPoint Cyber Security Management				✓	
Cisco Talos		✓		✓	
ClowdStrike FalconX				✓	
Collaborative Research into Threats	CRITs	✓	✓	✓	✓
Collective Intelligence Framework	CIF	✓	✓		
Cyber Defense Data Exchange and Collaboration Infrastructure	CDXI				
Cybersecurity Information Exchange Framework (X.1500)	CYBEX				
Cysiv Cyber Threat Exchange	Cysiv			✓	
Cyveillance LookingGlass Scout Prime	scout-PRIME			✓	
Defense Security Information Exchange	DSIE			✓	
Eclectiv IQ				✓	
Facebook Threat Exchange		✓		✓	
HP ThreatCentral					
IBM X-Force Exchange				✓	
Threat Intel feeds and Message Queueing system	IntelMQ	✓	✓	✓	✓
Infoblox Threat Intelligence		✓		✓	
Last Quarter Mile Toolset	LQMT	✓	✓		
Malstrom		✓	✓		
Malware Information Sharing Platform	MISP	✓	✓	✓	✓
MANTIS Management Framework		✓	✓		
McAfee Threat Intelligence Exchange		✓		✓	
Megatron		✓	✓		
Microsoft Interflow					
Nippon-European Cyberdefense-Oriented Multilayer threat Analysis	NECOMA	✓	✓		
Open Threat Exchange	OTX	✓		✓	
PassiveTotal		✓		✓	
Recoreded Future				✓	
Retail and Hospitality Information Sharing and Analysis Center	RH-ISAC			✓	
Soltra Edge		✓		✓	
ThreatConnect				✓	
ThreatQuotient				✓	
ThreatTrack ThreatIQ				✓	

3. Approaches for Cyber Threat Intelligence Sharing

Our research is driven by the motivation to discuss the question if CTI sharing tools can contribute to inter-state confidence building and, if so, what are the requirements to do so. Thereby, it is our objective to apply a broader understanding of cyber

threats. Section 3.1 introduces confidence-building measures as an approach of international politics for preventive crisis management between states. Section 3.2 presents identified tools and platforms, and Section 3.3 identifies requirements for such tools by states and international organizations.

3.1 Confidence-Building Measures as Communication and Cooperation

Confidence-building measures are instruments "which aim to prevent the outbreak of war or an (international) armed conflict by miscalculation or misperception of the risk, and the consequent inappropriate escalation of a crisis situation. CBMs achieve this by establishing practical measures and processes for (preventive) crisis management between States." (Ziolkowski, 2013, p. 5) These measures support transparency, cooperation and stability (ibid, p. 12). However, introducing binding CBMs or any other norms in cyberspace has been difficult, because states could not agree on definitions of central concepts. Thus, the debate on CBMs has been linked to development of norms on state behavior (Pawlak, 2016).

Even though CTI is not addressing the question of behavioral norms, and what states might define as cyber hostility, CTI platforms contribute to the aspects of cooperation and transparency between states, as they enable regular and structured exchange of incoming threats and possibly unknown vulnerabilities, and offer an insight into a state's IT infrastructure. In this manner, it is possible to improve the state's individual crisis management by cooperation, transparency and exchange, which is exactly what CBMs aim for when used in international policy. CTI is increasingly used as part of public and private cyber awareness and defense (Skopik et al., 2016; Skopik et al., 2018), states, such as the US and Germany and even international organizations like NATO already use CTI databases (Dulaunoy et al., 2019; Strobel, 2015). The question is, which requirements the existing CTI platforms need to fulfill in order to become part of a bi- and multilateral exchange on cyber threats.

3.2 Platform Selection

CTI sharing platforms are a mandatory part in today's approaches for better inter-state confidence building in cyberspace. We limit ourselves to open-source and maintained platforms, due to the open innovation capabilities of the IT community. Table 1 gives information about CTI platforms, identified using the research methodology described in Section 2. There are several platforms which are provided free-to-use, while most are closed-source and only few are released under an open-source license. Due to our limitations, only four platforms remain relevant for further investigation, namely:

- Bearded Avenger (BA, 2019)
- Collaborative Research into Threats (CRITs, 2016)
- Threat Intel feeds and Message Queueing system (ENISA, 2019)
- Malware Information Sharing Platform (MISP, 2018)

3.3 Requirement Selection

Requirements aiming to increase threat intelligence sharing and according platforms can be identified in two domains, *i.e.*, the scientific and the political domain. Both provide theoretical and practical requirements related to functionality, usability, and security. In this section we cover both domains to give a comprehensive overview on requirements oriented towards theory and practice.

Dandurand and Serrano (2013) named three fundamental requirements for CTI platforms: (i) facilitate information sharing, (ii) enable automation, and (iii) facilitate the generation, refinement, and vetting of data. Those build the core of CTI platforms and will not be listed as separate requirements in our requirement selection. Sauerwein et al. (2017) identified several key findings, which their surveyed CTI platforms lacked. We use their findings to identify the difference between their revelations and ours. Their key findings state a necessity for (i) open formats for cyber threat information, (ii) built-in functionalities for data analysis, and (iii) open-source platforms. The first requirement relates to the ability of different CTI platforms to exchange their data with each other to give operators and decision makers an overview of the cyber situation. Furthermore, the formats can be discussed within the community and possibly improved in later iterations. The second requirement communicates a necessity for analysis abilities. Sauerwein et al. (2017) showed, platforms are mainly focused on data aggregation instead of data analysis, indicating that current platforms increase the information overload rather than guiding decision makers in making their infrastructures more secure. The last requirement is based on the following fact: software needs to be certified with every update to ensure compliance to security standards, *e.g.*, ISO 27001. With an open-source platform, the whole CTI platform community is able to track every update and identify possible deficiencies (Hoepman & Jacobs, 2007), decreasing the necessity for a certification.

Besides the scientific requirements, the political domain define some as well, dealing with actionable information (see Section 1) and analytical capabilities of CTI platforms. In order to extract specific requirements, we focused on documents of organizations that already established communications between states, such as the European Union (EU), Organization for Security and Co-operation in Europe (OSCE), or United Nations (UN). We ended up gathering requirements in the reports by Bourgue et al. (2013), ENISA (ENISA, 2015, 2017), OSCE (2013), and EU Directive 2016/1148 (EU, 2016).

Table 2: Results of the requirement research in the scientific (top) and political (bottom) domain.

	actionable information	open-source	open formats	compatibility	interoperability	common glossary	secured	analysis
Dandurand et al. (2013)		✓	✓					
Sauerwein et al. (2017)		✓	✓					✓
Bourgue et al. (2013)								
Directive 2016/1148 (2016)	✓	✓			✓	✓		✓
ENISA (2015, 2018)	✓	✓	✓	✓	✓	✓	✓	✓
OSCE (2013)		✓			✓	✓		

Table 2 depicts the results of the identified requirements in the scientific and political domain with relating references. The open-source and open-formats requirements are combined to a single one. Compatibility, interoperability, and a common glossary all refer to the usage of an open standard, which includes the common glossary by design. The security aspect is split into the two requirements of confidentiality and integrity, since both can be achieved by different technologies. The last derived requirement is the analytical capability of a platform.

Hence, we conclude with the following requirements being especially important for the analysis in the following section:

- open-source and open standards
- confidentiality and integrity
- analytical capabilities

4. Advancing Cyber Security through Transnational CTI Sharing

Comparing the state-of-the-art of CTI sharing platforms with the obtained requirements, this section highlights areas in which the essential needs formulated by the scientific and political domain are met.

4.1 Technical and Organizational State of the Art

Open-Source and Open Standards

Threat information must be shared in a clear and understandable manner (Howard & Longstaff, 1998). All platforms in our sample fulfill this requirement by using open standards for communication. They operate with predefined terms, as well as incident classes and types, to easily enable actors to deal with the information provided (Bodeau et al., 2018; Strom et al., 2018). Nevertheless, as the discussed literature suggests, there remains an urgent call for more harmonization of all common standards in regard to CTI sharing in general.

All platforms included in our sample feature a general characterization, thus, their potential depends mainly on the specific communities that contribute and further develop the specific platforms. The ability to gain deeper insights into the communities can be seen as a starting point for future research.

Since different actors interpret cyber events differently, a feedback element helps to manage uncertainty. This allows users to discuss the underlying issue (Serrano et al., 2014). Besides compiling information on threats in an commonly understandable way, further recommendations on how to handle them contributes to cyber security. Feedback options are included in different platforms in our sample. MISP offers a system to collaborate on events (Team CIRCL, 2017). CRITs supports comments in addition to feedback patterns integrated into the threat information format STIX (Barnum, 2014; Mitre Corporation, 2015). IntelMQ offers a harmonized structure to communicate threats, however, there is no way to comment directly or share solutions to threats (IntelMQ, 2019). Bearded Avenger does not offer this feature.

Confidentiality and Integrity

When considering how CTI can contribute to confidence building between states, there are different practical issues. First of all, the success of each CTI platform depends mainly on the willingness of its community to share threat information. As advanced approaches, mainly by the EU, Organization for Economic Co-operation and Development (OECD), and North Atlantic Treaty Organization (NATO), show, willingness tends to be stronger among parties that have a common history and stable framework for communication. Besides a lack of political will, there can be restrictions due to an organization's limited availability of free resources or adequately skilled employees (Sauerwein et al., 2017). In regard to CTI sharing, such political willingness depends not only on the general trust and confidence among all parties involved, but to a similar degree on the trust the parties have regarding the reported cyber incidents covered on the platform. Therefore, there are two dependencies of trust, *i.e.*, the platform user's trust towards the provider and vice-versa (Sauerwein et al., 2017). Inserting malicious CTI data into the platform makes its users possibly insecure. Hence, the trust between users and providers is of critical importance. This also includes the trust in the storage of platforms, *i.e.*, the confidentiality and integrity of stored data. All selected platforms use open-source database implementations to store their data. Hence, every provider can compare his / her security criteria against the available source-code.

Analytical Capabilities

It is important for every single actor within a community to contribute to CTI platform development and improve its analytical capabilities. Only analytical advancements distinguish CTI platforms from pure data collection (Bourgue et al., 2013).

Analytical capabilities include categorization and ranking of threats, as well as automated prioritization. IntelMQ is equipped with the most favorable potentials for CTI sharing, as such capabilities are most developed on this specific platform. Its analytical features are implemented using third-party implementations, so-called bots. They can be stacked and nested together to build an analysis framework. Hence, the quality of analytical capabilities of IntelMQ depends on the quality of the available bots. MISP offers interfaces to analyze the available data with external tools, using a so-called MISP SEC-Ops System (MISP, 2018). But there are no integrated analytics capabilities in MISP. CRITs and Bearded Avenger offer no way to integrate external tools into the platform's workflow.

Table 3: Fulfillment of requirements per platform. A tick denotes the platform fulfills the requirement. A circle denotes partially fulfillment (e.g. with use of third-party applications). A cross denotes the platform does either not fulfill the requirement or there is limited to no documentation about it.

Name	BA	CRITs	IntelMQ	MISP
analytical capabilities	✗	✗	○	○
automatic communication of current threats	✓	✓	✓	✓
confidentiality and integrity of the platform	○	○	○	○
open-source	✓	✓	✓	✓
open standards	✗	✓	○	✓

Table 3 depicts which requirements, elaborated in Section 4, are fulfilled by each platform, showing that there is no state-of-the-art open-source CTI platform that is able to fulfill all requirements stated by states, international organizations, and academia.

4.2 Additional Findings

While this article strives to explore questions investigating technical and organizational issues connected to transnational CTI sharing, we want to highlight the importance of social and theoretical concerns. They are especially relevant when it comes to future academic research and are not yet elaborated in the field of inter-state confidence building focusing on CTI sharing.

CTI is mainly about human intelligence and as with all technological changes, this will not take place by simply adopting new technical frameworks or designs. Adopting effective information-sharing techniques through such channels might provide information on secure cyber behavior. However, without a greater socio-political and legal environment facilitating their functionality, they will not be effective at all. This is why it is crucial for political decision makers to closely follow trends and developments, re-evaluate their policies and have an agreed procedure for modifying them, if necessary (Horizon 2020, 2017; Johnson et al., 2016).

In the field of inter-state security or CTI sharing, sensitivity is reached by creating a stable and predictable environment for the discussed measures. Political and legal arrangements build the foundations for such an environment. Embedded in a stable socio-political and legally equipped environment constituted by common frameworks and emerging international norms for appropriate state behavior in cyberspace, CTI sharing platforms can provide effective advancements in security and support international preventive crisis management (Ziolkowski, 2013). However, as the dynamics of the international strategic stability are causing a crisis in CBMs and Arms Control, CTI can be implemented even on national or regional levels as part of anti-cybercrime strategies (Skopik, 2016). As CTI will be helpful with communication and cooperation aspects for confidence building, the implications for a future cyber arms control regime are unclear. Cyber arms control measures would need additional information on state-driven cyber operations, depending on the definition of cyber weapons, as well as the metrics for their measurements (Altmann & Siroli, 2018; Reinhold & Reuter, 2019; Ziolkowski, 2013). However, CTI can be a part of an attribution regime, which would collect technical indicators for cyber attribution and IT forensics (Davis et al., 2017).

Furthermore, any kind of information sharing is faced with a liability issue: When actors in an information-sharing community know about a potential threat (for example, by receiving feeds from this particular community), they have to secure their own capability to address this particular threat in a suitable way. Otherwise, they might find themselves confronted with the question, why they did not take appropriate action before this particular threat started to materialize. Omitted action might prove especially relevant in the context discussed here, since CTI sharing between states is not only connected to international security, but similarly to domestic security, especially for critical infrastructures (critIS) managed and secured by governmental bodies. As numerous incidents in the past, *e.g.*, the Baltimore Fallout in early 2019 (Liptak, 2019) or US digital incursions into Russia's electric power grid (Perlroth & Sanger, 2019), proved that public infrastructures are possible targets for cyber-attacks. Due to their unique social and political nature, omitted actions are of special importance when it comes to (de-)escalating a bi-, regional, or international conflict. Hence, analytical capabilities of CTI sharing platforms have to be as high as possible, while their coverage should be regional or even global to be effective. As these remarks suggest, improvements that go beyond the pure technical nature of CTI sharing are of high importance on every level within the sharing community.

5. Conclusion and Future Work

Today's increase of large scale cyber operations by organized criminal groups or even political actors (Reuter, 2019) demand new forms of cross-organizational and international sharing of information to discover cyber threats at an early state on and enable an early warning infrastructure (Skopik et al., 2016). States collect threat information, and sharing them to gain a large-scale cyber situational awareness would contribute to an increase in trust and security. As the risk of unintended collateral damage or even conflict remains as long as states have more incentives to behave offensive than defensive in cyberspace (Buchanan, 2017; Dunn Cavelty, 2014), we suggest to use CTI as a tool for confidence building between states. CBMs support communication and cooperation on an operational level, and help to increase stability. Due to the obstacles to define the term of cyber weapons internationally (Dickow et al., 2015), CTI focusses on the improvement of information sharing and cooperation, thus providing situational awareness and support of common understandings of threats. As an instrument, CTI platforms can serve as a tool for preventive crisis management and IT forensics in an attribution regime (Davis et al., 2017). Therefore, we answered the question, whether or not CTI platforms can be used as CMB, followed by a literature review of the field of available CTI platforms and the field of states and inter-state organizations and identified requirements for (i) open-source and open standards, (ii) confidentiality and integrity, and (iii) analytical capabilities. We matched the identified platforms, their features and the obtained requirements against each other. Our results suggest that many CTI platforms lack further analytical capabilities as suggested in prior work (Sauerwein et al., 2017). In order for technical improvements to take further effect, the evolution of a broader social, political, and legal environment for international CTI sharing is crucial. Hence, we suggest future work on the analytical capabilities of CTI platforms, open standards and definitions for a common understanding, as well as the general evolution of a supportive socio-political environment.

6. Acknowledgements

This research work has been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE as well as the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 CROSSING – 236615297.

Philipp Kuehn is a PhD researcher at the Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at Technische Universität Darmstadt. His research focuses on cyber security, attribution and vulnerability disclosure, as well as threat communication.

Thea Riebe is a PhD researcher at the Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at Technische Universität Darmstadt. Her research focusses on cyber security, dual-use and technology assessment.

Lynn Apelt is a student at the master's program of International Studies / Peace and Conflict Studies at the Goethe University Frankfurt and the Technical University of Darmstadt.

Max Jansen is a student at the master's program of International Studies / Peace and Conflict Studies at the Goethe University Frankfurt and the Technical University of Darmstadt. His research focuses on (post-) conflict dynamics, the role of civil society, as well as questions of cyber security and gender.

Christian Reuter is Full Professor for Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at the Technische Universität Darmstadt with a secondary appointment in the Department of History and Social Sciences. His research focuses on interactive and collaborative technologies in the context of crises, security, safety, and peace.

7. Bibliography

Altmann, Jürgen. (2019). Confidence and Security Building Measures for Cyber Forces. In *Information Technology for Peace and Security* (pp. 185–203). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4_9

Altmann, Jürgen, & Siroli, Gian Piero. (2018). Confidence and Security Building Measures for the Cyber Realm. In A. Masys (Ed.), *Handbook of Security Science*. London: Routledge.

BA. (2019). Bearded Avenger. Retrieved June 19, 2019, from https://github.com/csirtgadgets/bearded-avenger

Badsha, Shahriar, Vakilinia, Iman, & Sengupta, Shamik. (2019). Privacy preserving cyber threat information sharing and learning for cyber defense. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019* (pp. 708–714). IEEE. https://doi.org/10.1109/CCWC.2019.8666477

Barnum, Sean. (2014). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). *MITRE Corporation*, *July*, vol. *11*, , pp. 1–20. Retrieved from http://blackberry8520.b277.doihaveamobilestrategy.com/http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0_(Draft).pdf

Bodeau, Deborah J., Mccollum, Catherine D., & Fox, David B. (2018). "Cyber Threat Modeling: Survey, Assessment, and Representative Framework"," PR 18-1174. *HSSEDI, The Mitre Corporation*, iss. 18. Retrieved from https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyber-threat-modeling.pdf

Bourgue, Romain, Budd, Joshua, Homola, Jachym, Wlasenko, Michal, & Kulawik, Dariusz. (2013). Detect , SHARE , Protect Solutions for Improving Threat Data Exchange among CERTs. *European Network and Information Security Agency (ENISA)*, iss. October, pp. 51. Retrieved from https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs

Buchanan, Ben. (2016). *The Cybersecurity Dilemma*. London: C. Hurst & Co.

Buchanan, Ben. (2017). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. London: C. Hurst & Co. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001

CRITs. (2016). CRITs. Retrieved June 6, 2019, from https://crits.github.io

Dandurand, Luc, & Serrano, Oscar. (2013). Towards improved cyber security information sharing. In *International Conference on Cyber Conflict, CYCON* (pp. 1–16).

Davis, John S. II, Boudreaux, Benjamin, Welburn, Jonathan William, Ogletree, Cordaye, McGovern, Geoffrey, & Chase, Michael S. (2017). *Stateless Attribution: Toward International Accountability in Cyberspace*.

Dickow, Marcel, Hansel, Mischa, & Mutschler, Max M. (2015). Präventive Rüstungskontrolle – Möglichkeiten und Grenzen mit Blick auf die Digitalisierung und Automatisierung des Krieges. *Sicherheit & Frieden*, vol. *33*, iss. 2, pp. 67–73. https://doi.org/10.5771/0175-274x-2015-2-67

Dulaunoy, Alexandre, Iklody, Andras, Dereszowski, Andrzej, Studer, Christian, Vandeplas, Christophe, Andre, David, … Clement, Steve. (2019). *Malware Information Sharing Platform*.

Dunn Cavelty, Myriam. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, vol. *20*, iss. 3, pp. 701–715. https://doi.org/10.1007/s11948-014-9551-y

ENISA. (2015). *Actionable Information for Security Incident Response*. Retrieved from https://www.enisa.europa.eu/publications/actionable-information-for-security

ENISA. (2017). *Information Sharing and Analysis Centres (ISACs) Cooperative models*. https://doi.org/10.2824/549292

ENISA. (2019). *Incident Handling Automation*. *Community Projects*. Retrieved from https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation

EU. (2016). Directive (EU) 2016 / 1148. *Official Journal of the European Union*, vol. *6*, iss. 1, pp. 30. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Falliere, Nicolas, Murchu, Liam O., & Chien, Eric. (2011). W32. stuxnet dossier. *Symantec Security Response*, vol. *14*, iss. February, pp. 1–69. Retrieved from http://large.stanford.edu/courses/2011/ph241/grayson2/docs/w32_stuxnet_dossier.pdf

Hoepman, Jaap Henk, & Jacobs, Bart. (2007). Increased security through open source. *Communications of the ACM*, vol. *50*, iss. 1, pp. 79–83. https://doi.org/10.1145/1188913.1188921

Howard, John D., & Longstaff, Thomas A. (1998). *A common language for computer security incidents*. *Sandia National Laboratories*. https://doi.org/10.2172/751004

IntelMQ. (2019). IntelMQ – Data Harmonization. Retrieved June 26, 2019, from https://github.com/certtools/intelmq/blob/develop/docs/Data-Harmonization.md

Johnson, Christopher S., Badger, Mark Lee, Waltermire, David A., Snyder, Julie, & Skorupka, Clem. (2016). *Guide to Cyber Threat Information Sharing*. *Special Publication – Council for Agricultural Science and Technology*. Gaithersburg, MD. https://doi.org/10.6028/nist.sp.800-150

Kaiafas, Georgios (European Commission). (2017). *Horizon 2020. Threat Intelligence Sharing : State of the Art and Requirements*. Retrieved from https://protective-h2020.eu/wp-content/uploads/2017/07/PROTECTIVE-D5.1-E-0517-Threat-Intelligence-Sharing.pdf

Kaufhold, Marc-André, Rupp, Nicola, Reuter, Christian, & Habdank, Matthias. (2019). Mitigating Information Overload in Social Media during Conflicts and Crises: Design and Evaluation of a Cross-Platform Alerting System. *Behaviour & Information Technology (BIT)*.

Liptak, Andrew. (2019, May 25). Hackers reportedly used a tool developed by the NSA to attack Baltimore's computer systems. *The Verge*. Retrieved from https://www.theverge.com/2019/5/25/18639859/baltimore-city-computer-systems-cyberattack-nsa-eternalblue-wannacry-notpetya-cybersecurity

McQuade, Mike. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, pp. 1–6. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Meyer, Berthold, von Bredow, Wilfried, & Evers, Frank. (2015). 40 Jahre Schlussakte von Helsinki, 25 Jahre Pariser Charta: Rückblick und Ausblick auf die OSZE. *Sicherheit & Frieden*, vol. *33*, iss. 2, pp. 106–111. https://doi.org/10.5771/0175-274x-2015-2-106

MISP. (2018). *MISP – User Guide, A Threat Sharing Platform*. MISP Community. https://www.circle.lu/doc/misp/

Mitre Corporation. (2015). Collaborative Research Into Threats. *MITRE Corporation*. Retrieved from https://crits.github.io/.

Mohaisen, Aziz, Al-Ibrahim, Omar, Kamhoua, Charles, Kwiat, Kevin, & Njilla, Laurent. (2017). Rethinking information sharing for threat intelligence [Position Paper]. *HotWeb 2017 – Proceedings of the 5th ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies*, pp. 1–7. https://doi.org/10.1145/3132465.3132468

OSCE. (2013). Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. *DEC/1202*, vol. *10*, iss. December, pp. 4. Retrieved from http://www.osce.org/pc/109168?download=true

Páhi, Tímea, Leitner, Maria, & Skopik, Florian. (2017). Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy* (Vol. 2017, pp. 334–345). SCITEPRESS – Science and Technology Publications. https://doi.org/10.5220/0006149703340345

Pawlak, Patryk. (2016). Confidence-Building Measures in Cyberspace : Current Debates and Trends. *International Cyber Norms: Legal, Policy & Industry Perspectives*, vol. *20*, iss. April 2015, pp. 129–153.

Perlroth, N., & Sanger, D. E. (2019). U.S. Escalates Online Attacks on Russia's Power Grid – The New York Times. *New York Times*. The New York Times Company. Retrieved from https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html%0Ahttps://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?smid=nytcore-ios-share

Reinhold, Thomas, & Reuter, Christian. (2019). Arms Control and its Applicability to Cyber Space. In C. Reuter (Ed.), *Information Technology for Peace and Security* (pp. 207–233). Wiesbaden: Springer.

Reuter, Christian. (2019). Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. (C. Reuter, Ed.). Wiesbaden. Retrieved from https://doi.org/10.1007/978-3-658-25652-4

Reuter, Christian. (2020). Towards IT Peace Research: Challenges on the Interception of Peace and Conflict Research and Computer Science. *S+F Sicherheit Und Frieden / Peace and Security*, vol. *38*, iss. 1, pp. 1–15.

Sauerwein, Clemens, Sillaber, Christian, Mussmann, Andrea, & Breu, Ruth. (2017). Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In *Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017)* (pp. 837–851).

Serrano, Oscar, Dandurand, Luc, & Brown, Sarah. (2014). On the Design of a Cyber Security Data Sharing System. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security – WISCS '14* (Vol. 2014-Novem, pp. 61–69). New York, New York, USA: ACM Press. https://doi.org/10.1145/2663876.2663882

Skopik, Florian, Páhi, Tímea, & Leitner, Maria (Eds.). (2018). *Cyber Situational Awareness in Public-Private-Partnerships*. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-56084-6

Skopik, Florian, Settanni, Giuseppe, & Fiedler, Roman. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*, vol. *60*, , pp. 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Strobel, Warren. (2015, February 10). U.S. creates new agency to lead cyberthreat tracking – Reuters. *Reuters*. Retrieved from https://www.reuters.com/article/us-cybersecurity-agency/u-s-creates-new-agency-to-lead-cyberthreat-tracking-idUSKBN0LE1EX20150210

Strom, Blake E., Applebaum, Andy, Miller, Doug P., Nickels, Kathryn C., Pennington, Adam G., & Thomas, Cody B. (2018). MITRE ATT&CK – Design and Philosophy. *Technical Report*, iss. July, pp. 37.

Symantec Corporation. (2019). Symantec Internet Security Threat Report. *Network Security*, iss. 24, pp. 61. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Team CIRCL. (2017). MISP features and functionalities. Retrieved June 25, 2019, from https://www.misp-project.org/features.html

Ziolkowski, Katharina. (2013). Confidence Building Measures for Cyberspace–Legal Implications. *NATO CCD COE Publication*, pp. 1–88.

Towards a prospective assessment of the power and impact of Novel Invasive Environmental Biotechnologies*

Johannes L. Frieß, Bernd Giese, Anna Rößing, Gunnar Jeremias

Abstract: Novel environmental invasive biotechnologies, such as gene drives and Horizontal Environmental Genetic Alteration Agents exceed the classical applications of genetically modified organisms. The reason for this is that they are designed to transform wild organisms into genetically modified organisms which express desired traits. Instead of in a laboratory, this transformation takes place in the environment. The far-ranging effects that may be triggered by gene drive and Horizontal Environmental Genetic Alteration Agents require an extension of risk assessment to include socio-political consequences. The present article offers a first brief examination whether regulation is prepared for possible conflicts caused by benevolent or by hostile use of these novel technologies.

Keywords: Gene Drive, Horizontal Environmental Genetic Alteration Agents (HEGAA), Dual-Use, Novel Biotechnologies
Schlagwörter: Gene Drive, HEGAA, Dual-Use, neue Biotechnologien

1. Introduction

This study seeks to identify potential future areas of concern associated with the release of artificial genetic elements that have the capacity to self-propagate. This for instance includes application of gene drives (GD) (Oye et al., 2014) and Horizontal Environmental Genetic Alteration Agents (HEGAA) systems (Reeves et al., 2018), such as the Insect Allies project. Their potential to accelerate and induce social and political conflicts is worth an extensive investigation, given the highly increased range that both represent in comparison to previous releases of genetically modified organisms (GMO). Both technologies are rapidly developing novel invasive environmental biotechnologies (NIEB) with widely ranging applications. With only a few exceptions, the current focus of the risk assessment of GMO within the framework of authorisation procedures on environmental and health risks ignores a wide range of possible technological effects of the use and release of GMO on society and thereby social, economic, legal, ethical and cultural aspects. Most methods of technology assessment applied today investigate a much wider range of possible effects. This breadth has proved to be justified for two reasons: in addition to their direct interaction with the living or inanimate environment, technologies produce effects for the purpose for which they are intended. These include the measures and preconditions necessary for their use as well as side effects, failure or misuse.

NIEB technologies, such as GD or HEGAA, which aim at altering wild populations, may come with an extended spectrum of effects beyond the existing cultivated areas if they are to be used to intervene in ecosystems. Besides possible conflicts arising from the protection of the integrity of nature and ethical references, the use of GD to suppress species can give rise to political controversy, if their spread cannot be restricted and adverse ecological, social or economic effects are to be feared in other regions. For the same reasons, a potential misuse of these technologies for the development and production of bioweapons should be regarded as a very serious intervention. Not without reason did the US intelligence community group the act of genome editing in the category of weapons of mass destruction and proliferation concerns (Clapper, 2016).

To raise awareness, this article explores the currently envisioned environmental application fields for these technologies and characterizes their methods. The latter should help to investigate the potential range of impacts of an application of NIEB. Information about the dimensions and levels of the concerned environmental and societal areas may contribute to the exploration of putative socio-political consequences arising from such applications and the design of further approaches of prospective analysis.

2. GD and HEGAA as Novel Invasive Environmental Biotechnologies

GD, as well as HEGAA, in principle harness mechanisms that occur naturally. But their entanglement with new tools of molecular biology and the gain of a specific function justify their separation from naturally occurring mechanisms leading to biased inheritance (for GD) or lateral gene transfer (for HEGAA). In terms of genetic engineering, the introduction of a comparably simple approach for the targeted induction of genomic alterations by the 'gene scissors" CRISPR/Cas (Jinek et al., 2012) has opened up a variety of new approaches and boosted the development of already existing technologies like GD. The design of synthetic GD has been motivated by naturally occurring selfish genetic elements that have been shown for several plant and animal species. GD serve to accelerate the spread of genes in wild populations and are now intended for a range of applications, further explained below. It is unknown whether natural GD have caused extinctions of species in the past. We can only assume that existing species seem to have evolved mechanisms to get along with this type of genetic elements (cf. Nick Barton in Giese et al., 2019). Synthetic GD, however, have so far not been tested in the wild. Predictions on their dynamics of spread in wild populations and potential ecological effects, therefore, rely on models and laboratory experiments using caged populations. Depending on their

* This article has been double blind peer reviewed.
The authors express their thanks to the reviewers.

intended applications, some suggested to distinguish between local and rather globally acting GD ("standard gene drives", cf. Min et al., 2018). Global GD are supposed to suppress or even eradicate pathogens or disease vectors for animals and humans, whereas local drives should be designed to suppress agricultural pests and invasive species or protecting threatened species in a certain region (Min et al., 2018). Although several applications for GD have been put forward in recent years, it is still uncertain whether the results of modelling approaches and lab experiments provide reliable information on what to expect in the event of a release. On the one hand, the genetic variability of natural populations in comparison to laboratory strains gives rise to the assumption that GD might partially be less effective in the wild (Buchman et al., 2018). On the other hand, there is reason to believe that local drives will not stay confined to a certain population (Noble et al., 2018). In particular, when GD are applied to eradicate invasive species, loss of control over GD organisms and a potential dispersal into their native habitat may represent a serious hazard. Due to such concerns, intricate mechanisms have been proposed to either "overwrite" a released drive by a second GD or to achieve a transient drive whose activity comes to a hold after a certain number of generations (DiCarlo et al., 2015; Esvelt et al., 2014; Noble et al., 2016). But as they are synthetic GD themselves, there is so far no proof for such control mechanisms under the conditions of an application (Giese et al., 2020). Accordingly, the EU-Parliament recently decided to request *"the Commission and the Member States to call for a global moratorium at the COP15 on releases of gene drive organisms into nature, including field trials, in order to prevent these new technologies from being released prematurely and to uphold the precautionary principle, which is enshrined in the Treaty on the Functioning of the European Union as well as the CBD"*.[1]

For the HEGAA approach, it is planned to use GM insects as vectors for GM plant viruses which will then carry out genetic modifications on crops (Reeves et al., 2018). HEGAA should serve to rapidly enhance crop plants with benefical traits to reduce crop loss due to environmental stressors (Bextine in response to Kupferschmidt, 2018). Some, however, pointed out that HEGAA would be more readily applicable as a bioweapon instead (WCAI, Partan and Goldstone, 2018; Reeves et al., 2018). In contrast to the vertical transfer of transgenes from a parental generation to the offspring in the case of GD, HEGAA make use of a lateral transfer of transgenes. If the density of appropriate insect species as vectors is high enough, several transfer events may occur within one plant generation. Therefore, the spread of transgenes by HEGAA must be assumed as potentially being much faster than by GD. However, according to the available official statements of the funding programme (DARPA), the spectrum of target species of HEGAA is rather limited to crop plants and not projected to transform wild species as in the case of GD (Bextine, 2018).

These NIEB indicate a change in principles in areas in which methods have hitherto been either more natural or did not intervene into the genomic setup of organisms (e.g. as pesticides). The new methods favour powerful strategies at the molecular level. In addition, the process of genetic manipulation is increasingly shifted out of the laboratory into the field (Simon et al., 2018). In that regard, besides concerns related to unintended consequences, the self-sustaining nature of GD was already considered as a new opportunity for its use as a weapon by the US-National Academies of Sciences (National Academies of Sciences, 2016, p. 160f).

2.1 Potential Application Fields for Gene Drives

There are multiple potential applications for the two NIEB which this article focuses on. For the potential application fields, we will, however, only list those applications as examples which we deem the most likely to be released, either due to their funding, their level of development or the sheer willingness of actors to put the technology to use. We thereby want to make the distinction in scale of the releases between local and potentially global applications. Two application fields of GD fit into the local scale.

A great number of target organisms could be listed for the application field of bio-conservation. Therein, endangered species that often live on isolated islands ought to be protected from extinction. In all proposed cases an invasive species that threatens indigenous species is considered for suppression drive application. Although transboundary escapees in many cases cannot be excluded, these applications may still be considered local, since suppression drives generally require a high threshold (ratio of GD organisms to wild types in a population) in order to spread. Probably the most prominent examples for efforts in bio-conservation are Australia and especially New Zealand, which both suffer from a large number of invasive species threatening the indigenous fauna and flora. The Australian Academy of Sciences explored the potential of GD in a report from 2017 and concluded that mosquitoes, black rats, mice, carps and agricultural pest insects might be suitable candidates for suppression drives (Australian Academy of Science, 2017, p. 15). In New Zealand on the other hand, foremost represented by the Predator Free 2050 initiative[2], GD may be considered to eradicate invasive rodents. Their risks, as well as legal and regulatory implications, are currently discussed in scenarios for pest control (Royal Society of New Zealand, 2019). Stoats, possums and rats are especially dangerous to native birds and plants. Rats are reported to even feed on the eggs of the kiwi, New Zealand's national animal. Currently, mass trappings and mass poisonings are conducted on the small and main islands of New Zealand. The latter causing painful deaths, making an eradication by suppression drive seem more humane. Furthermore, it proves difficult to completely eradicate and kill the last rodents on an island with poison alone (Owens, 2017). Other potential target organisms are two wasp species *Vespula germanica* and *Vespula vulgaris* (Dearden et al., 2018; Royal Society of New Zealand, 2019, p. 10). Although suppression drives are considered to remain local with only a low likelihood to spread beyond the isolated release areas, a re-immigration into continental areas, aside from grave ecological impacts, given enough time, would constitute high conflict potential.

1 European Parliament resolution of 16 January 2020 on the 15th meeting of the Conference of Parties (COP15) to the Convention on Biological Diversity (2019/2824(RSP); https://www.europarl.europa.eu/doceo/document/TA-9-2020-0015_EN.html

2 https://predatorfreenz.org/about-us/pf-2050/

The other application field for GD that may be considered local is agriculture. Here as well, a panoply of different pest organisms or weeds have already been considered as potential target organisms, such as Palmer's amaranth, mice, mostly insects that either feed or oviposit on crop plants and even nematodes (ETC Group and Heinrich-Böll-Stiftung, 2018; National Academies of Sciences, 2016). The probably most advanced endeavour in the agricultural sector is developed against the invasive fruit fly species *Drosophila suzukii*. The GD is developed by the MIT-based Akbari Lab (Buchman et al., 2018) and financed by the California Cherry Board since 2013, as the fly is a major crop pest on cherry creeks (Regalado, 2017). Issues of conflict potential again may arise due to lack of confinability from farm to farm, and from farm to wild habitat, but also due to international trade on regulatory, legislative and, by extension, even on political stages.

GD applications on a non-local and possibly even global scale are situated in the field of combatting diseases. Thereby, the distinction can be made between public (human) health and animal health. Plausible applications concern the population control or the modification of vector species for pathogens. Target organisms are mosquito species that transmit diseases such as malaria or dengue (Gantz et al., 2015; Hammond et al., 2016; Li et al., 2019). The National Academies of Sciences (2016, p. 53) in their case study consider avian malaria as a possible target to control animal pathogens. For human health, the population control of malaria vector species is a prominent example for GD applications not only in the health sector but for GD in general. The international research consortium Target Malaria (TM), funded by the TATA Group, the Bill and Melinda Gates Foundation, Open Philanthropy Project and supported by the World Health Organisation, pursues the best-funded GD research project worldwide. Currently, TM is in the first of three phases of test releases. Therein, sterile males are released and recaptured to monitor the dispersal of the mosquitoes. In these unprecedented efforts to promote public health on a transnational scale, as releases will ultimately not be confined to single countries, TM is facing opposition by Civil Society Organisations. For example, Friends of the Earth International, ETC Group (2018) and the African Centre for Biodiversity (2019), among others, criticize the practices of TM concerning the lack of environmental risk assessments, public consultation and prior informed consent. They further claim that TM has thereby created social strife in the communities concerned. Moreover, according to critics, releases may cause unintended transboundary spread and present a risk to biodiversity since the releases will not be contained (African Centre for Biodiversity, 2019). Thus, this novel and far-ranging effort in public health – not least because of its grand transnational scale – already causes conflict although the definite releases have not yet begun.

2.2 Potential Application Fields for HEGAA

The US Advanced Research Project Agency (DARPA) funds the Insect Allies research project (DARPA, 2016). This project aims to develop application-ready genetically modified insects which are infected with genetically engineered viruses. The application field for this fast-propagating technology is meant to be agricultural. Should the need arise, HEGAA would be released onto crop fields. The GM insects would transfer the GM-viruses onto the crop plants, which then confer desired traits onto the plants. The technology is envisioned to provide the crop plants with various resistances to different stressors, such as heat, drought, cold, moisture or salinity. HEGAA are supposed to be a contingency plan in case of a foreseeable bad crop harvest, be it as a result of an attack with a bioweapon or due to adverse weather conditions. To quickly induce the desired changes, this technology relies on the rapid horizontal spread of viruses which may only take days instead of the slow vertical spread of GD that requires generations. Currently, research on the project is financed for three working groups in the US (Boyce Thompson Institute, 2017; Harter, 2017; Horetsky, 2017). Although a last resort technique to evade food shortage may seem meaningful, it was pointed out that the development of this technique inevitably also leads to the potential to develop HEGAA as a bioweapon. The realisation as such would be much easier to construct than the planned peacefully applicable variant. Arguably, the disruption of gene function is much simpler to engineer than their enhancement (Reeves et al., 2018).

However, even considering only peaceful applications of HEGAA, multiple potential conflict sources not unlike those for some GD applications become apparent. These include the spread of GM-organisms or GM-viruses in space (beyond their intended release sites, potentially crossing international borders), time and possibly even between different species of plants. Thus, regulatory, legislative and political conflicts may arise in (international) trade of crop produce modified by GM viruses outside the controlled confines of a laboratory.

3. Consequences, Governance, and Regulation

Regardless of hostile or peaceful intent, these technologies have the potential to cause conflict due to socio-economic disturbances on different levels. Only some of these conflict sources are regulated by national or international law. We first concentrate on the international legislation regulating release for hostile and non-hostile purposes and then briefly mention consequences that require non-legislative governance activities. We will show that existing legislation regulating the release of NIEB was at least not developed for these technological developments and might thus not be adequate and require adaptations.

3.1 International Legislation Regulating Hostile Use of NIEB

Hostile use of biological systems might historically be associated with large-scale programs to weaponise human pathogens for use as Weapons of Mass Destruction. But the unwanted spread of NIEB could also be considered hostile when changes to genomes in natural or agricultural populations are induced which may impair interests or protected commodities of a third country not involved in the licensing of the release. For instance, uncontrolled cross-border spread of a NIEB that

is considered helpful in the country of release but induces interference of agricultural production in a neighbouring country could either be considered a liability issue to be treated under international private law or as a hostile act to be reviewed under the provisions of multilateral arms control treaties. Two multilateral treaty regimes may be relevant, namely the Biological and Toxin Weapons Convention (BTWC) and the convention on environmental warfare (ENMOD). Lastly, relevance to international export control regulations is briefly addressed by the identification of open questions.

3.1.1 Biological and Toxin Weapons Convention (BTWC)

Biological warfare is almost globally prohibited by the BTWC of 1975. Only ten states have neither signed nor ratified this arms control treaty, which without exception prohibits offensive bioweapons related activities. However, it might be questionable if NIEB fall under the regulation of the BTWC when being used in the development and production of weapons (or release being interpreted as a hostile act) since technologies are not biowarfare agents in the established understanding. Article I of the treaty obliges its State Parties to *"never in any circumstances develop, produce, stockpile or otherwise acquire or retain: (1) Microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes; (2) Weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict."* Phrasing and the historical context of the early 1970s, when the treaty was negotiated, point to viruses, bacteria and other pathogens being released as weapons of war. Until recently, aerosols and bomblets would have been considered as the main means for delivery. NIEB changed this view and gave insects and viruses a much more central role as possible vectors. As stated above, at least HEGAA do have the potential to be used in a bioweapon context. Should mosquitoes become adapted to serve as vectors for specific pathogens, or if HEGAA was used to induce damaging genome editing in plant populations, the insect and virus would serve as means of delivery and would hence fall under the obligations of the BTWC.

But could animal populations that are equipped with a GD also be considered a biological weapon as they do not serve as a vector? Could the mere presence and spread of a GD population in a wild ecosystem or an agricultural area be considered a hostile act? States Parties of the BTWC have at the second Review Conference in 1986 agreed that *"the scope of article I covers scientific and technological developments relevant to the Convention […]. It was agreed that the obligations assumed under Article I applied to all such developments without reservation"* (BWC/CONF.II/9). This interpretation was repeatedly confirmed at subsequent Review Conferences, bringing NIEB-based developments within the scope of the BTWC, if they are produced or used for hostile purposes.[3]

3 The BTWC does not directly address bioterrorism, but activities of states. Though, it might become relevant indirectly, e.g. through ineffective implementation of the convention into national law. Primarily all UN members are obliged to take action against WMD-terrorism by UNSC Resolution 1540/2004.

3.1.2 ENMOD

Another international arms control treaty that may be relevant for hostile use of the technologies in question is the ENMOD treaty (Convention on the Prohibition of Military or Any Other Hostile Use of **En**vironmental **Mod**ification Techniques) from 1976. In its first article, it prohibits the Contracting Parties from engaging *"military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party"*. Subjects of protection as defined in Article 2 are *"natural processes – the dynamics, composition or structure of the Earth, […] including its biota […]"*.[4] ENMOD membership is by far not as widespread as that of the BTWC, but most countries with the technological capacities to create NIEB are ENMOD members. There is neither experience with the activation of the convention (via the complaint of a member at the UN-Security Council), nor is there consensus concerning the scope of the treaty (Lohbeck, 2004). Furthermore, no ENMOD meetings took place after the second Review Conference in 1992. This does not render the treaty ineffective but also does not evidence its wide acceptance as a means of international conflict prevention or resolution. With these limitations, it is, however, plausible that the eradication of a plant or animal population or the unwanted editing of genomes in a population could be interpreted as a hostile act if effects occur that are interpreted as damages.

A problem for both treaties is that there are many conceivable scenarios involving the release of NIEB that result in consequences considered as damage or harm by another state into whose territory the technologies have autonomously spread. However, hostility is usually interpreted as an activity with the intention to harm. Intent is already hard to prove when the action in question does not take place in a war situation, but in contrast, may even be a licensed activity by a private stakeholder for commercial or public health issues. Hence, the question is, if activities whose effects on natural resources were not intended to be destructive, but which were not assessed in advance (on purpose or by omission), could be judged as hostile. A multitude of views on how this should be treated under international law might arise after release, although it would help prevent conflicts if there would be widespread awareness on these issues.

3.1.3 Export Control Law (Dual-Use Items and Weapons of War)

Export restrictions of specified items become only relevant if NIEB technologies would be recognized as having a dual-use potential by a state or in one of the relevant (informal) export control regimes (Australia Group and Wassenaar Arrangement). Export restrictions under the Australia Group (AG) control list include dual-use biological equipment and related technology and software.[5] There is hardly any equipment that is specific to NIEB. But *'Related Technologies'* have to be *"directly associated with: AG-controlled pathogens and toxin or AG-controlled dual-use biological equipment items"*. On the other hand, the *'transfer*

4 https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/460
5 https://australiagroup.net/en/controllists.html

of technology' such as *'technical assistance'* is also included. If these requirements were met by a specific NIEB-application, it would fall within the scope of the AG control list. However, *"controls on 'technology' do not apply to information 'in the public domain' or to 'basic scientific research' or the minimum necessary information for patent application."* Despite the research and funding environment for the development of HEGAA, together with the finding that misuse could technically be easier than the prospected civil applications (Reeves et al. 2018), it cannot be assessed here whether or not any of the requirements for export controls would be met by the direct export of ready-made HEGAA insects (not to mention GD organisms).

3.2 Non-Hostile Use

The regular case will likely be a release for non-hostile applications as characterized above. On the international level, the Convention on Biodiversity (CBD) could contribute to the regulatory framework since the protection of genetic resources is within the scope of the treaty (articles 1 and 2). CBD States Parties discuss the issues, for example in consideration of a moratorium for GD, but have not made a decision. On the national level, the release of GD or HEGAA would fall in the category of the release of GMO, for which many countries since the early 1990s have enacted and further developed legislations. We cannot go into details on more or less restrictive laws, but would state that these different laws have in common that GMO releases are in principle licensable after a risk assessment procedure.[6] In all examined cases, it is possible to bring transgenes into circulation, but only after a risk assessment. This, among other specifications, usually requires the prevention of uncontrolled spread of the released GMO into the wild. The motives for the development of such regulatory institutions were environmental protection and the associated protection against critical changes in the environment, particularly of agricultural land against undesirable influences. Concerning the political circumstances in which the legislations have been developed, this doubtlessly happened with regard to the potential of uncontrolled GMO to cause social conflict. As a general rule, if at all, GMO release was only licensed for self-restricting GMO. In contrast, self-sustainability is the main feature of any NIEB, at least for a certain period. Of course, these technologies were not foreseen when the regulations were designed. It is therefore questionable how developers can expect to license under these circumstances – possibly in the hope of risk-benefit assessments, where the benefits of release outweigh the risks of uncontrolled spread.[7] Under the current EU regulations on the deliberate release of GMO (Directive 2001/18/EC, Annex III A), there are some aspects to an environmental risk assessment that can hardly be answered for NIEB at the current stage of development, as proven measures for control are lacking. This for instance concerns the duration of the release, the size of the release site and all aspects concerning control of the release. A case in Brazil may be employed as a cautionary tale: although the involved company denies this, scientists claim to have found evidence for the establishment and spread of so-called "self-limiting genes" in mosquito populations in Brazil. These mosquitoes were released between 2013 and 2015 by the hundreds of thousands and were expected to suppress mosquito populations and then disappear – but they instead led to a small but significant introgression of their genome to the natural mosquito population (Evans et al., 2019; Grens, 2019). Target Malaria researchers are emphasising that they will ensure safety, but licensing authorities (should there be any) and stakeholders should take the case above into account. It is not clear whether or not the people of an affected country will agree to a release, and it is even more uncertain whether or not the authorities will do so.

This stresses that there is a large grey area between damages from hostile use and use that induces damages through negligence. It would then not only be enlightening to explore possible consequences, e.g. by scenario-building on how unintended consequences might lead to legal and societal conflicts. Scenarios should examine local retention and cross-border spread of GD populations.

3.3 Release in or Spread to Third Countries

Peaceful applications of environmental biotechnology may cause conflict, if either accidental spread occurs, or if there is negligence of other notions of what is perceived as unwanted consequences. If we take the example of the impacts of unwanted technology on farming, the introduction of technologies which are not accepted or even cause a fitness loss, may lead to major social upheavals in agricultural economies.

Situations might be aggravated if the real or perceived threat comes from another country. In many historic cases, the accidents in nuclear or chemical facilities led to contaminations or physical destructions. Such consequences could theoretically be resolved through international liability agreements. However, bi- or multilateral mechanisms, such as the EU safety, liability and cooperation framework for the nuclear area are rare (EU Parliament, 2019). In the event of an incident, this will, in any case, entail years of complicated court hearings. Other examples are the complicated litigations after accidents in chemical production facilities that have contaminated downstream river systems in neighbouring states.[8] Most fields and cases, among them the unintended spread of GMO, remain unregulated. Private persons, including farmers, would most likely not be able to take appropriate actions in such lawsuits – and even less so, if there is no precedence, as it would be the case with NIEB crossing borders.

Generally, the "the polluter-pays-principle" would have to be applied (as implemented in different legal and other frameworks such as the Rio Declaration, OECD rules, EU law, and many national legislations). But this principle is already difficult to enforce when a polluter and the injured party come from the same country; it would be much more complicated or almost impossible if the plaintiff is based in another country, beginning with the issue whether or not self-sustaining, spreading GMO should be considered pollution at all.

6 In the EU a regulation (EC guideline 2001/18) sets the framework for the member countries.

7 In a recent case, US-authorities in their risk-benefit assessment might value the importance of saving "a billion-dollar industry" from the bacterial Huanglongbing disease through "vaccination" by spreading CRISPR-mutations with Asian citrus psyllid (Chow et al., 2019).

8 https://www.umweltbundesamt.de/en/press/pressinformation/sandoz-chemical-spill-25-years-on

Hence, before the question is raised whether or not an injuring party is obliged to eventually provide compensation, the principal difficulty is to assess and quantify the volume of compensation in dispute. Even if a country (or company) would concede that effects deemed positive, and being licensed in that country, would be assessed as damage or harm in another country (e.g. the GD induced collapse of a mosquito population, or genome edits following a HEGAA infection), there is no comparable case that could be used for the estimation of the financial damage, not to mention more complex damages.

It is easy to imagine that with growing interferences of the "target country" also intentions become an issue, as hostile intentions by the "source country" can be claimed. It would not be the first time that countries hold other countries responsible for biological damages, even if they had natural origins (e.g. "The great Cold War potato beetle battle" [9]).

In conclusion, both legislations for hostile and for non-hostile use of the technologies in question are either not developed or poorly adapted to these new biotechnologies. Due to the General-purpose criterion (Article I of the BTWC), the bioweapons ban might be the best framework to regulate them.

Here, we did not even include consequences that do not directly lead to measurable effects, such as dissatisfaction, fear for poverty, the feeling of being dominated by foreign countries, companies or other institutions, or the danger that attempted techno-fixes by GD might endanger conventional efforts in public health and mosquito control. This would require another study. However, we do want to stress that the governance of socio-economic effects of technology use in a country (and beyond) ideally exceeds pure legislation. It should also include risk-communication with the aim of achieving societal (cross-border) consensus on the use of a technology – ideally in coordination with societal debates in countries that might (unintentionally) be affected.

4. Conclusion

Novel invasive environmental biotechnologies such as GD and HEGAA represent a new quality of GMO-release in their potentially far-ranging activity on the genomic level of wild organisms or crop plants. Depending on their impact on respective populations and the specific trait, effects may substantiate on different levels from populations to ecosystems up to the socio-economic sphere. The necessity to address aspects beyond health and environmental hazards was already brought forward (National Academies of Sciences, 2016, p. 179). Moreover, Kuzma and Rawls (2016) highlight the fact that although an application of GD might be beneficial for the current generation, future generations may be deprived by the consequences of its application. Wintle et al. (2017) even point out that weighing benefits against risks might be very unattractive given the potential extent of the latter. As we have shown, governance and regulation for benevolent as well as potential hostile applications of these new biotechnologies may be unable to cope with some of the outcomes and ramifications of the release of GD and HEGAA. In particular, the potentially high rate of intentional gene flow makes them a 'common good' instead of a technology for private use like previous GMOs (cf. Simon et al., 2018) and generates a higher risk of transboundary movements. As the NAS report for GD already mentioned, this deficit is in part due to the present regulatory logic of confinement and containment, which becomes problematic given the invasive nature of the new technologies (National Academies of Sciences, 2016, p. 178). With regard to hostile use of GD, the prevention of disclosure of instructions for synthesis of GD in analogy to nuclear weapons was already claimed (Gurwitz, 2014).

To further investigate the deficiencies of the current regulatory framework, and to prepare a base for an adaptive amendment, we propose to analyse potential effects of these new and comparably invasive techniques for genetic engineering in a comprehensive examination. Due to the lack of experience from first releases, investigations have to cope with a lack of empirical data and rather rely on *a priori* analysis. Here, scenario-building could serve as an appropriate approach to cover a wide range of potential application cases. Scenario exercises do not claim to make accurate predictions, but rather aim to develop multiple and comparable plausible versions of the contingent future to inform and direct research roadmaps that improve long-term policy planning, and policy implementation.

9 https://www.bbc.com/news/magazine-23929124

Dr. rer. nat. **Johann L. Frieß** is employed as a senior scientist at the University of Natural Resources and Life Sciences, Vienna (BOKU) at the Institute of Safety/Security and Risk Sciences. He has expertise in molecular biology and works on multiple projects on the technology assessment of novel invasive environmental biotechnologies.

Dr. rer. nat. **Bernd Giese** leads the Bio- and Nanotechnology branch of the Institute of Safety/Security and Risk Sciences (ISR) at the University of Natural Resources and Life Sciences, Vienna (BOKU). His work is dedicated to technology assessment of emerging technologies and their governance in accordance with the precautionary principle.

Ms. **Anna Rößing** M.A. is a Doctoral Researcher at the University of Bath. She has worked as a research associate at the Carl Friedrich von Weizsäcker Centre for Science and Peace Research at the University of Hamburg. She researches the political drivers of military innovation, and broader changes in Technology.

Dr. phil. **Gunnar Jeremias** is the head of the BMBF Junior Research Group BIGAUGE and Interdisciplinary Research Unit for the Analysis of Biological Risks at the Carl Friedrich von Weizsäcker Centre for Science and Peace Research at the Universität Hamburg. His expertise is in Biological Arms Control, Biological Security and Ethics in Science.

5. Bibliography

African Centre for Biodiversity, 2019. Stop risky GM Mosquito releases – We have the right to say no. https://www.acbio.org.za/sites/default/files/documents/OPEN_LETTER_TO_THE_TARGET_MALARIA_PROJECT_FROM_AFRICAN_CIVIL_SOCIETY_%20Stop%20risky_GM_mosquito_releases_we_have_the_right_to_say_no.pdf

Australian Academy of Science, 2017. Synthetic gene drives in Australia: implications of emerging technologies. https://www.science.org.au/support/analysis/reports/synthetic-gene-drives-australia-implications-emerging-technologies

Bextine, B., 2018. DARPA Response to Science Opinion Piece (published Oct 4, 2018). https://www.darpa.mil/attachments/DARPA%20Response%20to%20Science%20Opinion%20Piece%20-%20Oct%204%202018.pdf

Boyce Thompson Institute, 2017. BTI receives DARPA "Insect Allies" Award – Developing viruses and insects for maize improvement. Eureka Alert. https://www.eurekalert.org/pub_releases/2017-07/bti-brd072717.php

Buchman, A., Marshall, J.M., Ostrovski, D., Yang, T., Akbari, O.S., 2018. Synthetically engineered *Medea* gene drive system in the worldwide crop pest *Drosophila suzukii*. Proceedings of the National Academy of Sciences 201713139. https://doi.org/10.1073/pnas.1713139115

Chow, A., Czokajlo, D., Patt, J.M., Sétamou, M., 2019. Development and Field Validation of a Beta-cyfluthrin-Based 'Attract-and-Kill' Device for Suppression of Asian Citrus Psyllid (Hemiptera: Liviidae) on Residential Citrus. Journal of Economic Entomology toz221. https://doi.org/10.1093/jee/toz221

Clapper, J.R., 2016. Worldwide threat assessment of the US intelligence community. Office of the Director of National Intelligence Washington DC.

DARPA, 2016. Insect Allies. https://www.darpa.mil/program/insect-allies

Dearden, P.K., Gemmell, N.J., Mercier, O.R., Lester, P.J., Scott, M.J., Newcomb, R.D., Buckley, T.R., Jacobs, J.M.E., Goldson, S.G., Penman, D.R., 2018. The potential for the use of gene drives for pest control in New Zealand: a perspective. Journal of the Royal Society of New Zealand 48, 225–244. https://doi.org/10.1080/03036758.2017.1385030

DiCarlo, J.E., Chavez, A., Dietz, S.L., Esvelt, K.M., Church, G.M., 2015. Safeguarding CRISPR-Cas9 gene drives in yeast. Nature biotechnology 33, 1250–1255. https://doi.org/10.1038/nbt.3412

Esvelt, K.M., Smidler, A.L., Catteruccia, F., Church, G.M., 2014. Concerning RNA-guided gene drives for the alteration of wild populations. eLife 3. https://doi.org/10.7554/eLife.03401

ETC Group, Heinrich-Böll-Stiftung, 2018. Forcing the Farm – How Gene Drive Organisms could entrench industrial Agriculture and threaten Food Sovereignty.

Evans, B.R., Kotsakiozi, P., Costa-da-Silva, A.L., Ioshino, R.S., Garziera, L., Pedrosa, M.C., Malavasi, A., Virginio, J.F., Capurro, M.L., Powell, J.R., 2019. Transgenic Aedes aegypti Mosquitoes Transfer Genes into a Natural Population. Scientific Reports 9, 13047. https://doi.org/10.1038/s41598-019-49660-6

Friends of the Earth International, ETC Group, 2018. United Nations hits the brakes on Gene Drives. ETC Group. https://www.etcgroup.org/content/united-nations-hits-brakes-gene-drives

Gantz, V.M., Jasinskiene, N., Tatarenkova, O., Fazekas, A., Macias, V.M., Bier, E., James, A.A., 2015. Highly efficient Cas9-mediated gene drive for population modification of the malaria vector mosquito Anopheles stephensi. Proceedings of the National Academy of Sciences of the United States of America 112, E6736–E6743. https://doi.org/10.1073/pnas.1521077112

Giese, B., Frieß, J.L., Barton, N.H., Messer, P.W., Débarre, F., Schetelig, M.F., Windbichler, N., Meimberg, H., Boëte, C., 2019. Gene Drives: Dynamics and Regulatory Matters—A Report from the Workshop "Evaluation of Spatial and Temporal Control of Gene Drives," April 4–5, 2019, Vienna. BioEssays 41, 1900151. https://doi.org/10.1002/bies.201900151

Giese, B., von Gleich, A., Frieß, J.L., 2020. Alternative Techniques and Options for Risk Reduction of Gene Drives. In: Gene Drives at Tipping Points. von Gleich, A., Schröder, W. (Eds.), Springer (in Press).

Grens, K., 2019. GM Mosquito Progeny Not Dying in Brazil: Study. The Scientist. https://www.the-scientist.com/news-opinion/gm-mosquito-progeny-not-dying-in-brazil--study-66434

Gurwitz, D., 2014. Gene drives raise dual-use concerns. Science 345, 1010–1010. https://doi.org/10/ggh48v

Hammond, A., Galizi, R., Kyrou, K., Simoni, A., Sinicalchi, C., Katsanos, D., Gribble, M., Baker, D., Marois, E., Russell, S., Burt, A., Windbichler, N., Crisanti, A., Nolan, T., 2016. A CRISPR-Cas9 gene drive system targeting female reproduction in the malaria mosquito vector Anopheles gambiae. Nature Biotechnology 34, 78–85. https://doi.org/10.1038/nbt.3439

Harter, K., 2017. Ohio State scientists to make plant virus system "turn on its head" with insect research. The Lantern. https://www.thelantern.com/2017/12/ohio-state-scientists-to-make-plant-virus-system-turn-on-its-head-with-insect-research/

Horetsky, J., 2017. Penn State team receives $7M award to enlist insects as allies for food security. Penn State University. https://news.psu.edu/story/495037/2017/11/20/research/penn-state-team-receives-7m-award-enlist-insects-allies-food

Jinek, M., Chylinski, K., Fonfara, I., Hauer, M., Doudna, J.A., Charpentier, E., 2012. A programmable dual-RNA-guided DNA endonuclease in adaptive bacterial immunity. Science (New York, N.Y.) 337, 816–21. https://doi.org/10.1126/science.1225829

Kupferschmidt, K., 2018. Crop-protecting insects could be turned into bioweapons, critics warn. Science. https://doi.org/10.1126/science.aav6274

Kuzma, J., Rawls, L., 2016. Engineering the Wild: Gene Drives and Intergenerational Equity. Jurimetrics 279–296.

Li, M., Yang, T., Kandul, N.P., Bui, M., Gamez, S., Raban, R., Bennett, J., Sánchez C., H.M., Lanzaro, G.C., Schmidt, H., Lee, Y., Marshall, J.M., Akbari, O.S., 2019. Development of a Confinable Gene-Drive System in the Human Disease Vector, *Aedes aegypti* (preprint). Bioengineering. https://doi.org/10.1101/645440

Lohbeck, W., 2004. Umwelt und bewaffneter Konflikt: Dilemma ohne Ausweg (No. 137). Hamburg.

Min, J., Smidler, A.L., Najjar, D., Esvelt, K.M., 2018. Harnessing gene drive. Journal of Responsible Innovation 5, S40–S65. https://doi.org/10.1080/23299460.2017.1415586

National Academies of Sciences, 2016. Gene Drives on the Horizon: Advancing Science, Navigating Uncertainty, and Aligning Research with Public Values. The National Academies Press, Washington, DC. https://doi.org/10.17226/23405

Noble, C., Adlam, B., Church, G.M., Esvelt, K.M., Nowak, M.A., 2018. Current CRISPR gene drive systems are likely to be highly invasive in wild populations. eLife 7, e33423. https://doi.org/10.7554/eLife.33423

Noble, C., Min, J., Olejarz, J., Buchthal, J., Chavez, A., Smidler, A.L., DeBenedictis, E.A., Church, G.M., Nowak, M.A., Esvelt, K.M., 2016. Daisy-Chain Gene Drives for the Alteration of Local Populations. https://doi.org/10.1101/057307

Owens, B., 2017. Das große Keulen. Spektrum.de. https://www.spektrum.de/news/neuseeland-will-invasive-arten-ausrotten/1436198

Oye, K.A., Esvelt, K., Appleton, E., Catteruccia, F., Church, G., Kuiken, T., Lightfoot, S.B.-Y., McNamara, J., Smidler, A., Collins, J.P., 2014. Regulating gene drives. Science 345, 626–628. https://doi.org/10.1126/science.1254287

Partan, E., Goldstone, H., 2018. "Insect Allies" Program Draws Criticism. WCAI. https://www.capeandislands.org/post/insect-allies-program-draws-criticism#stream/0

Reeves, R.G., Voeneky, S., Caetano-Anollés, D., Beck, F., Boëte, C., 2018. Agricultural research, or a new bioweapon system? Science 362, 35–37. https://doi.org/10.1126/science.aat7664

Regalado, A., 2017. Farmers seek to deploy powerful gene drive. MIT Technology Review.

Royal Society, 2019. Gene Editing. Scenarios in Pest Control. Royal Society Te Aparangi.

Simon, S., Otto, M., Engelhard, M., 2018. Synthetic gene drive: between continuity and novelty. EMBO reports 19, e45760. https://doi.org/10.15252/embr.201845760

Wintle, B.C., Boehm, C.R., Rhodes, C., Molloy, J.C., Millett, P., Adam, L., Breitling, R., Carlson, R., Casagrande, R., Dando, M., 2017. Point of View: A transatlantic perspective on 20 emerging issues in biological engineering. Elife 6, e30247.

New Military Technologies: Dangers for International Security and Peace*

Jürgen Altmann

Abstract: New military technologies are being developed at a high pace, with the USA in the lead. Intended application areas are space weapons and ballistic missile defence, hypersonic missiles, autonomous weapon systems, and cyber war. Generic technologies include artificial intelligence, additive manufacturing, synthetic biology and gene editing, and soldier enhancement. Problems for international security and peace – arms races and destabilisation – will likely result from properties shared by several technologies: wider availability, easier access, smaller systems; shorter times for attack, warning and decisions; and conventional-nuclear entanglement. Preventive arms control is urgently needed.

Keywords: Research, Development, Technology, Preventive Arms Control
Stichwörter: Forschung, Entwicklung, Technologie, präventive Rüstungskontrolle

1. Introduction

Throughout history new technology has enabled new kinds of weapons (Brodie and Brodie 1973). A technology edge of one side provided an advantage in war, but did not always guarantee victory. With the rise of science new technologies were developed ever more systematically. Systematic, large-scale, organised use of science for warfare started in the Second World War and was scaled up drastically in the Cold War, mainly in the USA and the USSR (Thee 1988). Important milestones of new military technologies with marked effects on the international situation were: in the 1950s the hydrogen bomb, in the 1960s ballistic long-range missiles, in the 1970s multiple independently targetable reentry vehicles, in the 1980s precision guidance, in the 1990s net-centric warfare and in the 2000s uninhabited vehicles. In many cases, such innovations increased threats and reduced warning and reaction times, deteriorating international security and endangering peace (Müller and Neuneck 1991/92).

The dangers associated with nuclear weapons motivated peace movements, and concerned scientists warned against the nuclear threat (Evangelista 1999). Over time – and with the experience of crises, in particular the Cuban missile crisis 1962 – in both governments the insight grew that an unconstrained quantitative and qualitative arms race was too dangerous, and arms-control treaties became possible. Their negotiation and conclusion depended on the respective political situation. The end of the Cold War brought a wave of important arms-limitation treaties (Goldblat 2002). Despite impressive successes, arms control did not block further military-technological innovation; a qualitative arms race continued, with an increasing number of participating countries. Presently this arms race is accelerating, aggravated by the addition of strategic actors.

This article intends to warn against the consequences of the new technological arms race, primarily among the major powers, but possibly also involving other countries. It takes a rather fundamental approach, emphasising arms control over export control.[1] After a look at the scale of military research and development, a brief explanation of preventive arms control is given. Then, short overviews of the new military technologies are presented that are or will become relevant for international security, with exemplary references, from space weapons via artificial intelligence to enhanced soldiers. Finally, common traits are highlighted that will likely bring negative effects for international security and peace, and thus require preventive arms control.

2. Scale of Military Research and Development, and Predominance of the USA

The USA is the global leader in military research and development (R&D). While the USA with around $700 billion per year covers around 40 per cent of the global total military expenditure, its share in military R&D is nearly two thirds, around $70 billion per year. The other official nuclear-weapon states Russia, UK and France each spend less than one tenth of that (Altmann 2017).

The unrivalled US expenditure derives to a significant part from the motive to maintain military-technological superiority. While a long-time, general policy,[2] it has been re-emphasised recently with the argument that China and Russia are catching up in high technologies (e.g. Work 2015). As a consequence, the USA is the forerunner in new military technologies; to know the trends, it is generally sufficient to look at the USA. This is alleviated by the unequalled openness of the USA about its military R&D.[3]

3. Military-Technology Assessment and Preventive Arms Control[4]

Will new military technology be good or bad for world peace? This question and others are investigated systematically in military-technology assessment. It does a prospective analysis

* This article has been double blind peer reviewed.
1 For export control of new technologies see e.g. Brockmann and Kelley (2018), Bromley and Maletta (2018).
2 E.g. "The DoD R&E [Department of Defense Research & Engineering] program needs to create, demonstrate, apply, and partner in the transition to operational use of technologies to enable affordable and decisive military superiority to defeat any adversary on any battlefield." (US DoD 2007).
3 See e.g. the hundreds of pages of budget-request justifications for research, development, testing and evaluation for the armed services and defence-wide R&D institutions (e.g. US DoD 2019a).
4 Smit et al. 1992, Neuneck and Mutz 2000, Altmann 2006: ch. 5, 2008.

DOI: 10.5771/0175-274X-2019-4-36

of a potential new military technology or application. What could be military uses? How could operations look like? With answers to such questions, one then checks whether or not the potential new technology or application would fall under the criteria of preventive arms control. These can be classed into three groups:

1. Could the new technology create problems for arms control, for disarmament, or for international (humanitarian) law?
2. Could the new weapons or applications cause an arms race? Could they destabilise the situation between potential adversaries?
3. Could they cause problems for humans, the environment or society already in peace time?

If an important concern shows up in one of the issue areas, considerations about preventive limits are in order. Preventive arms control limits or prohibits certain military systems or certain uses of technology before they are deployed. Legally, it can work at different phases: it can set rules for use, for deployment or for the prior stages of testing or of development (research mostly is not included because the results are unknown or could be used for many purposes).

Many arms-control treaties contain preventive elements. Prohibitions on use are contained in the Geneva Protocol on gas warfare (Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare), the Environmental Modification Convention and the Blinding Laser Weapons Protocol. Deployment is banned in the Outer Space Treaty and was limited in the Anti-Ballistic Missile (ABM) Treaty. Development is included in the prohibitions of the Biological and the Chemical Weapons Conventions and, for the non-nuclear-weapon states, in the Nuclear Non-Proliferation Treaty. The Partial and the Comprehensive Nuclear Test Ban Treaties explicitly focus on testing, but thereby they prevent research with actual nuclear explosions and hinder the development of new types of nuclear weapons.

Despite such successes, most military-technological advances went unimpeded. In many cases science has provided concepts for preventive limits and for verification, e.g. for space weapons or weapons-usable fissile materials,[5] but the relevant states considered their own military strength as more important, or there were other reasons that prevented cooperation, e.g. in the Conference on Disarmament (Caughley 2011). Convincing states that mutual limitation is in their own interest in an enlightened concept of national security – i.e. embedded in international security – continues to be a difficult but important task of scientists and other citizens who care for peace.

Generally, preventive arms control focuses on (potential) military systems, not on generic technologies that can have different uses. Many dual-use technologies are subject to export controls in order to prevent or slow down proliferation and military uses by other countries or non-state groups. Except in the areas of chemical and biological weapons, export controls are asymmetric. In the interest of international security and peace, it would be better to exclude military uses of problematic technologies (old: e.g. nuclear, new: the ones discussed here) globally.

5 Fischer et al. 1984, Feiveson et al. 2014.

4. Areas of Present Military Research and Development

Following the motive to increase military effectiveness by new technology, the important actors, above all the USA, are doing R&D in various fields. Several of the activities (4.1 to 4.3) date back to precursors of the Cold War. Others have come up in the last two decades. In most cases the work is directed toward concrete military systems (4.1 to 4.4), here preventive arms control would be applicable directly. But there are also generic technologies that may enable many different military applications (4.5 to 4.8), here preventive limitations would present much higher difficulties, not the least because of dual use that may require inclusion of civilian applications.[6]

There are also synergies between the technologies. E.g. additive manufacturing can contribute to space weapons, missiles, autonomous weapon systems, and biological weapons. Artificial intelligence can support advances in most other areas.

4.1 Space Weapons[7] and Ballistic Missile Defence[8]

Space weapons were curtailed to some extent by the Outer Space Treaty of 1967 that prohibited weapons of mass destruction in outer space. Non-nuclear anti-satellite (ASAT) weapons were developed and tested, in the 1960s and 1970s in the form of rendezvous/follower satellites by the USSR. In the USA, with the Strategic Defense Initiative (SDI) of the 1980s, interest focused first on beam weapons. However, they were shown later to have little chance of providing protection from a nuclear attack. Direct-ascent ASAT systems were developed and tested by the USA in the 1980s. In recent years, China as well as India additionally have demonstrated an ASAT capability. Very recently, the USA has decided to build up a space force with the intent to expand "American superiority in space" since "[s]pace is the world's newest warfighting domain" (US DoD 2019b). Which types of weapons and forces will be developed, remains to be seen. Since satellites fulfil central roles in warfare, ASAT weapons appear militarily attractive. Depending on deployment mode and target altitude, the travel time can be minutes to hours.

In the 1990s, the USA brought ballistic missile defence (BMD) to the fore, with an extensive development and testing program. After abrogation of the ABM Treaty (2001/2002), it deployed BMD systems in several regions at sea and on land in Alaska and Romania. While the Russian ABM system has used nuclear-armed interceptors, the US BMD interceptors rely on actually hitting the incoming reentry vehicles in midcourse while they fall along the gravity-caused ellipse, using an infrared seeker and trajectory correction over some final 20 seconds before collision. For slower ballistic missiles of shorter ranges, terminal-phase interceptors exist. Even though midcourse discrimination of the real warhead from a multitude of light-weight decoys is not guaranteed, Russia and China are working on hypersonic glide vehicles in order to circumvent US BMD sites.

6 For a concrete example how this might be done see the recommendations for nanotechnology in Altmann (2006: ch. 7).
7 Pelton 2019, Bulletin 2019.
8 Korda and Kristensen 2019.

The Trump administration has changed the goal of BMD from limited attacks from countries such as North Korea to any missile launched against the USA, including from Russia and China. If this goal will persist, R&D for defence in all flight phases will have to be intensified, including for defence against hypersonic missiles.

4.2 Hypersonic Missiles[9]

While supersonic flight refers to a velocity above the speed of sound (about 0.34 km/s at normal temperatures), the term hypersonic describes above five times the speed of sound (Mach 5). Hypersonic missiles were developed and tested in the USA after 2003 for the so-called conventional prompt global strike. After tests in 2010 and 2011, the programmes were stopped. Russia had intensified its R&D already after the US SDI of the 1980s and has announced in 2018 that it has developed hypersonic missiles of both kinds: hypersonic glide vehicles (HGVs) and hypersonic cruise missiles. China is active in research and has tested HGVs from 2014 on. The USA has started new programmes for both kinds in 2016.

A *hypersonic glide vehicle* (HGV, also called boost-glide vehicle) is accelerated by a rocket and falls along an elliptical trajectory through outer space. It reenters the atmosphere far in front of the target. Rather than falling down on a slant trajectory, the vehicle turns to horizontal in about 100 km altitude and glides through the atmosphere. The speed falls from about 6 km/s to about 2 km/s speed (Mach 20 to 6) while it slowly descends to about 30 km. A steep, guided descent toward the target follows. Alternatively, the vehicle stays below 100 – 200 km altitude all the time. In the gliding phase it can change its course by control flaps, covering many times 1,000 km. Total ranges far above the maximum ICBM range of 10,000 – 13,000 km are possible.

HGVs make missile defence much more difficult: The ballistic phase is shorter and occurs at lower altitudes so that they rise above the horizon of ground-based radars in the target region later – or only on final approach. The rocket-launch flame can be seen by space-based early warning systems. But even if the trajectory after burnout could be measured, only the reentry site could be predicted, no longer the target location itself. By flying curves in the second phase, an HGV can circumvent BMD sites and thwart prediction of the trajectory. The times for detection and for reaction are reduced markedly.

Hypersonic missiles of the second kind, *hypersonic cruise missiles* (HCM), do not leave the atmosphere. Their supersonic combustion ramjet (scramjet) engines take in air, limiting the altitude to 30 km, and require initial acceleration, e.g. by air launch or booster rocket. With Mach 5 to 8 (1.7 to 2.7 km/s) they are 6 to 10 times as fast as traditional, subsonic cruise missiles, and 2 to 5 times as fast as supersonic combat aircraft. The range can be up to a few times 1,000 km. For attack over 1,500 km, e.g. from surface ships or submarines, HCMs take 9 to 15 minutes, leading to markedly shorter times for detection and reaction than with the 80 minutes flight time of subsonic cruise missiles.

Both types of hypersonic missiles, HGV and HCM, principally can be equipped with conventional as well as nuclear warheads. They increase possibilities for surprise attack, in particular against nuclear-strategic weapons and command-and-control systems.

4.3 Autonomous Weapon Systems[10]

In the last two decades, armed uninhabited air vehicles (UAVs) have proliferated widely; more than 30 countries have added them to their arsenals. Many have automatic functions, but the weapons are released under remote control by a human operator, requiring a communication link. Based on fast advances in sensors, computers and software, armed forces plan for the next step: autonomous weapon systems (AWS). AWS would – after activation – select and engage targets without further interaction with a human. An algorithm would search in sensor data for potential targets, classify them, select appropriate ones and attack them. Such AWS for complex environments do not yet exist, but there are precursors in close-range weapon systems with an automatic mode and longer-range missiles with target-recognition systems.

AWS would come in various sizes and forms, moving in air, on land, on or under water. Military advantages are obvious. Already remote-control weapon systems remove the operator from the scene and thus from danger. Without a remote-control link, AWS would be harder to detect, the link could not be jammed, and AWS could react markedly faster. Military disadvantages exist, too: control of events on the battlefield would suffer, and the systems could be hacked, but militarily, the advantages outweigh the problems. Once deployment of AWS would begin, an accelerating arms race can be expected, much faster than what can be observed with remote-control armed UAVs at present. The main reason is that AWS are intended for combat against a competent adversary, not for very asymmetric scenarios.

Significant doubts exist whether an algorithm will be able to comply with international humanitarian law. At least as problematic is the escalation dynamic that can ensue from the interaction between two fleets of AWS at short mutual distance, with only seconds of missile flight time between them. In a severe crisis both sides would intensely observe each other for indications of attack. In order not to lose one's systems they would have to be programmed to shoot back fast – which in case of a false alarm could start a "flash war" by mistake. AWS would bring new possibilities for surprise attack, raising nervousness and the need to react faster.

Armed uninhabited vehicles can form swarms. Attacking simultaneously or in waves from many sides, they promise higher probability of destruction and saturation of defences. While a swarm acting as a whole against a single target could be controlled by a human, the full advantage of swarm attack – with self-coordination, adaptive assignment to different targets, and maybe emergent behavior – would only accrue if the swarm consisted of AWS. Swarm and swarm defence would thus constitute a subarea of an AWS arms race.

Expert discussions about a prohibition or limitation of AWS in the context of the UN Convention on Certain Conventional Weapons have not led to a mandate for negotiations because militarily important states are opposed.

9 Acton 2013, 2015, Speier et al. 2017, Lele 2019.

10 Bhuta et al. 2016, Altmann and Sauer 2017, Scharre 2018.

4.4 Cyber-War Preparations[11]

With the increasing use of information and communication technology (ICT) in the armed forces and the rise of the internet, the cyber realm has become a fifth area of warfare. Many states have founded cyber forces that not only act defensively, but also prepare offensive action. Attacking the information systems of enemy forces has become an integral part of war plans, to be used in conjunction with physical attacks. But cyber attacks can also be used on their own, outside of traditional armed conflict, opening a grey area between espionage and armed attack. Cyber attacks range from simple intrusion into the military or civilian computer systems of an adversary for gaining information to the destruction of the military or civilian infrastructure, with consequences far beyond the ICT systems. Indirect effects could strongly reduce the fighting capability or devastate the functioning of a society, with damages comparable to the effects of massive attacks using physical weapons. To deter such cyber attacks, military responses in the physical world have been threatened. International law manuals have been developed providing guidelines for when such reaction can be justified and how cyber operations in war should be conducted.

Cyber-war preparations increase mutual threats. Fear and mistrust are aggravated by secrecy. If prepared in advance by planting malware, cyber attacks could occur in seconds. This increases motives to respond equally fast, that is by automating the reaction, maybe including AI and learning. Thus, also here the possibility exists for fast escalation by interaction between two automatic/autonomous systems of attack and counter-attack.

Containing the cyber arms race and the associated destabilisation by arms control meets specific difficulties. Non-state actors could use the same cyber weapons as armed forces, even though those of the latter will be much more sophisticated generally. However, once developed and known they can be used by nearly anyone without special training or infrastructure. Different from tanks or aircraft, cyber weapons can be multiplied easily, thus numerical limits cannot work. Their capabilities can be kept secret before they are used. Turning from espionage to attack is easy. Attribution to the real originator is difficult. Devising limits on cyber forces and methods for verification thus needs creativity.

4.5 Artificial Intelligence, Big-Data Analysis, and Machine Learning[12]

The field of artificial intelligence (AI) with its sub-fields of big-data analysis and machine learning has shown impressive progress in recent years, in games such as chess and go as well as in object recognition in images. At the same time, spectacular classification errors have been found as well as produced intentionally. The opacity of machine learning, in particular with deep neural networks, has led to calls for explainable AI.

The USA, Russia and China see AI as a major component of their future military strength, by incorporating more information and enabling faster action. Future AI may be transformative "on a par with nuclear weapons, aircraft, computers, and biotech" (Allen and Chan 2017). Armed forces could apply AI in many areas: in logistics for supplies or maintenance, and in AWS for recognising targets and for classifying scenarios. Situation awareness from tactical to strategic levels would profit from finding patterns in data from many sensors and other sources. In battle management, AI could be used at least for decision support, later maybe for decision making. Enemy actions could be assessed and modelled.

There is a big difference to machine learning in games: with fixed rules in a very restricted space, computers can easily generate millions of valid chess or go games to train the algorithms. In preparation for combat on the other hand, there will not be many actual high-technology battles to learn from. Thus, simulation will have to play a big role. Whether the results will be similar to events in actual war is questionable at least. Making weapons and forces more dependent on AI opens possibilities for hacking and deception. More problematic would be the reduction of human control, in particular due to a much higher speed of decisions and actions.

With respect to nuclear weapons, AI could be used for early warning, attack characterisation and preparation of a counterattack, principally also for the launch decision itself, e.g. to ensure a second strike even if human control is no longer possible. Including more information in situation assessment could improve human decision making and reduce the risk of accidental nuclear war, but a greater role of AI could also increase it. A special problem would ensue if, by big-data analysis, nuclear submarines or mobile intercontinental ballistic missiles could be located and destroyed in a first strike. Both systems are seen as guaranteeing a secure second-strike capability. The fear that these deterrents are endangered would create strong crisis instability. Arms race instability could ensue from the intentions to prevent such a situation.

4.6 Additive Manufacturing[13]

In additive manufacturing (AM, often also called 3-D printing), solid parts are built up layer by layer from a material that can be in liquid or powder form and then solidifies by various mechanisms, e.g. cooling from a melt, light-induced polymerisation or sintering. Inner cavities can be created easily. The materials include plastic, metals and ceramics, the strength approaches that achieved by traditional production technologies such as casting, forging and hardening. The process is slower, thus not well suited to mass production, but finds increasing use for low numbers of special components and prototypes or for casting or pressing moulds. In this way, together with computer modelling, development cycles can be shortened drastically. What can be produced depends firstly on the machine and the available material. Since the machines provide near-universal capability, the product is defined secondly by the control code, the so-called build file. Prohibited or limited products could be made if the software can be accessed, maybe illegally. Crude firearms have already been made by AM. Work is being done on ammunition and smaller missiles.

11 Lewis and Neuneck 2013, Schmitt 2017, Reuter 2019: chs. 4-7, 9-10, 12-13.
12 Geist and Lohn 2018, Horowitz 2018, Boulanin 2019.
13 Fey 2017, Johnston et al. 2018, Brockmann/Kelley 2018, Brockmann 2019, Christopher 2019.

For armed forces, several applications are foreseen: Replacement parts could be produced in the field, reducing logistics and allowing faster repairs. More relevant for international security could be mass production of small uninhabited weapon systems. Principally, missile bodies as well as energetic materials can be made. Uranium enrichment could profit from 3-D-printed parts for centrifuges. AM could support a biological weapons programme.

4.7 Synthetic Biology and Gene Editing[14]

Genetic engineering started in the 1970s with very complex and expensive laboratory equipment but got increasingly accessible with ever faster and cheaper methods of DNA sequencing and then DNA synthesis, leading to biotechnology as a routine method of production. Synthetic biology, the fabrication of complex, artificial biological systems that fulfil certain tasks, maybe with non-natural biochemical structures, was the next major innovation. Several methods and tools have become cheap and widely accessible so that hobby groups and students can do significant work. Relevant concern exists that individuals or small groups by chance or by bad intent could produce new harmful biological agents for which no antidote is known.

Since 2012 genetic engineering has become drastically easier with the CRISPR/Cas9[15] method. This tool allows one to modify the genetic code in DNA molecules nearly arbitrarily ("gene editing"). This technology promises curing genetic and other diseases and faster advance in basic and applied research. However, as other fundamental technologies, it has a dual-use character. One obvious military application would be the creation of new biological-warfare agents, maybe causing diseases or modifying behaviour by acting on the brain. Such activity is prohibited by the Biological Weapons Convention (BWC) with its nearly universal adherence, however, the Convention still lacks a compliance and verification scheme. Non-state actors, on the other hand, could act outside of the BWC and against its bounds. Another potentially hostile application is possible with so-called gene drives aimed at changing or even eradicating animal or plant populations in the wild.

4.8 Enhanced Soldiers and Body Manipulation[16]

Even if they are relatively far from being implemented, concepts of future soldier enhancement have gotten enough credibility that detailed discussions about conditions, consequences and ethical issues have begun (however, international security and preventive arms control are not yet on the agenda). Various possibilities are conceived of, from exoskeletons via changes of the biochemistry to brain implants. "Supersoldiers" by genetic modification and fully fledged cyborgs are being envisioned. Changes could affect body, mind and mood, possibly switched on or off, reversible or irreversible. Since such enhancements pose many fundamental questions, involving the societies at large, it is unclear if they will be introduced at all, and if so, in which of the possible forms. But insofar as they will promise increased combat power, there will be strong military motives, and restraint may wane for fear of adversaries proceeding faster. Consequences for international security will depend on the extent and degree of enhancement, but because soldier enhancement would come in synergy with combat robots and AI, acceleration of battle tempo and shortening of decision times would be a probable outcome.

5. Problematic Traits of Coming Military Technologies

Many of the military technologies described share properties that are likely to produce negative effects for international security and peace. Synergies between them will aggravate the problems.

Wider Availability, Easier Access, Smaller Systems

General-purpose technologies such as information and communication technology, artificial intelligence, additive manufacturing and synthetic biology/gene editing are becoming cheaper, more widely distributed, and accessible for actors with fewer skills. Expensive state-funded R&D institutions may be unnecessary for production of items for nefarious or hostile uses. Product properties in many cases depend on control software, software proliferation is inherently difficult to prevent. Dangerous goods or materials could be very small and hidden easily. They could be produced in small facilities by states as well as non-state actors. International limitations on military uses of such technologies would need verification by on-site inspections at any site at any time, and large-scale monitoring of data traffic. Accepting such intrusiveness will probably be very difficult not only for armed forces, but also for enterprises and civil society at large.

Shorter Times for Attack, Warning, and Decisions

For weapons that need physical transport to a target, the time between launch and arrival depends on the speed of propagation and the distance. This time can be from seconds to hours (Table 1). Faster carriers shorten this time, e.g. hypersonic versus subsonic cruise missiles. The time for warning and reaction is shorter if detection and determination of the intended target region do not occur at launch. For example, the trajectory of a traditional ballistic reentry vehicle can be determined by radars looking into space. Predicting the target of a hypersonic glide vehicle, with about the same flight time, may only be possible late in the second flight phase. Remotely controlled uninhabited weapon systems may be close to potential targets with missile flight times of seconds only. The two-way communication delay between a sensed event and the execution of the commanded action typically is a few seconds. Autonomous weapon systems, where the processing of sensor data as well as the selection and engagement of a target is done on board, would react without such delay, that is, much faster. Electronic transmission times over the internet range from fractions of a second to a few seconds. Thus, if a target computer has already been infected before, a

14 Nixdorff 2017, Himmel 2019, Frieß et al. 2020.
15 Clustered Regularly Interspaced Repeats/CRISPR-associated protein 9.
16 Kott et al. 2015, Wigan 2017, Matthews and Schnyer 2019.

cyber attack could be started in seconds time. Depending on the kind of attack, the effects may become visible only after some time; in this respect, biological weapons are similar where some diseases need time to break out. Artificial-intelligence-augmented battle management would increase the tempo of combat.

Overall, the new military technologies would markedly accelerate events in war, reducing the time for decisions. In particular in a crisis there would be less time to double-check whether an alarm is due to a real attack, was caused by a sensor, computer or algorithm malfunction, or was the result of an erroneous classification of data. Table 1 summarises the travel/propagation times for various weapon types; detection, warning and decision times are shorter.

Table 1: Times from launch to arrival at target, or from start of attack to effects for various weapon types and typical distances.[17]

Weapon Type	Distance/ km	Speed/ km/s	Time to Arrival/Effect	Nuclear	Conventional
Subsonic long-range bomber	5,000	0.3	6 h	X	X
Supersonic fighter-bomber	1,500	0.5-0.9	50-30 min	X	X
Subsonic cruise missile	1,500	0.3	80 min	X	X
Supersonic missile	10	0.5-1.5	20-7 s	X	X
HCM	1,500	1.7-2.7	15-9 min	X	X
ICBM	10,000	7	33 min	X	-
HGV	5,000 + 7,000	6	24 + 24 min	X	X
SLBM	3,000	4.4	17 min	X	X
Cyber attack (prepared)	arbitrary	-	seconds	-	-

Conventional-Nuclear Entanglement

Faster missiles with higher precision raise the chance and thus the motive to take out strategic nuclear weapons as well as command-and-control systems with conventional weapons. The same carriers could also carry nuclear weapons. Smaller nuclear weapons (though still in the Hiroshima class) are envisioned as means of threatening fast escalation to deter conventional attacks. As a consequence, for war among nuclear-weapon states, there will be an increasing risk of escalation from conventional to nuclear weapons, as well as of understanding a conventional attack as nuclear-relevant. In a severe crisis, launch on warning and pre-emptive attack will become more probable.

17 These times are upper limits for detection and warning of attack. Entries are typical or average values, for ballistic missiles for trajectories with minimum energy. The sound speed in air at 20 °C is 0.34 km/s, at -50 °C (10 km altitude) 0.30 km/s. For ballistic missiles and HGV, the speed at burnout is given; due to the elliptical flight path the speed decreases up to the peak altitude, and the path is longer than the distance along the ground. For anti-satellite weapons, the time varies between minutes and hours depending on the altitude and weapon type and deployment. HCM: Hypersonic Cruise Missile, ICBM: Intercontinental Ballistic Missile, HGV: Hypersonic Glide Vehicle, SLBM: Submarine-Launched Ballistic Missile.

6. Conclusion

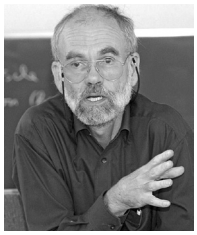
Each of the the new military technologies that are in the making would reduce warning and decision times, increase possibilities for surprise attack and create corresponding fears and nervousness, with the associated risks of misperceptions, worst-case assumptions and false alarms, not only by human decision makers, but also by algorithms. In synergy, these dangers would be multiplied. Preventive arms control is needed urgently; export control could limit proliferation to some countries and non-state actors but would not solve the destabilisation problem between producer states. Limitations and their verification in space weapons, ballistic missile defence and hypersonic missiles can follow established arms-control concepts. For autonomous weapon systems and cyber-war preparations, innovative approaches are required that should be investigated in interdisciplinary research.

Even though the present political situation does not bode well for it: Preventing the dangers may need nothing less than a comprehensive approach with a return to fundamental insights:

A nuclear war cannot be won and must never be fought.

Conventional war between major powers carries a strong risk of escalation to nuclear war.

Sustainable national security is possible only in the context of international security.



Jürgen Altmann, PhD, senior researcher and lecturer, head of Physics and Disarmament Group, Experimental Physics III, TU Dortmund, Germany. Expertise: acoustic-seismic detection, military-technology assessment, preventive arms control. Recent projects on uninhabited and autonomous weapon systems.

Bibliography

Acton, James M. (2013). *Silver Bullet? Asking the Right Questions About Conventional Prompt Global Strike*. Washington, D.C.: Carnegie Endowment for International Peace.

Acton, James M. (2015). Hypersonic Boost-Glide Weapons. *Science & Global Security* 23 (3), 191-219.

Allen, Greg and Taniel, Chan (2017). *Artificial Intelligence and National Security*. Cambridge MA: Belfer Center, Harvard University. http://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf (16 Febr. 2020).

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). Militärische Forschung und Entwicklung. In Jürgen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann und Dieter Wöhrle. *Naturwissenschaft – Rüstung – Frieden – Basiswissen für die Friedensforschung*. 2nd edition. Wiesbaden: Springer VS.

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

Bhuta, Nehal, Susanne Beck, Robin Geiß, Hin-Yan Liu and Claus Kreß (eds.) (2016). *Autonomous Weapon Systems – Law, Ethics, Policy*. Cambridge: Cambridge University Press.

Boulanin, Vincent (2019). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Volume I Euro-Atlantic Perspectives*. Solna: SIPRI. https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk (11 Febr. 2020).

Brockmann, Kolja (2019). Additive Manufacturing and Biological Weapons: Assessing Proliferation Risks and Challenges to Export Control. In Christian Reuter, Jürgen Altmann,

Malte Göttsche, Mirko Himmel (eds.). *SCIENCE PEACE SECURITY '19 – Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research*. Darmstadt: TUprints. https://tuprints.ulb.tu-darmstadt.de/id/eprint/9164 (11 Febr. 2020).

Brockmann, Kolja and Robert Kelley (2018). *The Challenge of Emerging Technologies to Non-Proliferation Efforts – Controlling Additive Manufacturing and Intangible Transfers of Technology*. Solna: SIPRI, April 2018. https://www.sipri.org/sites/default/files/2018-04/sipri1804_3d_printing_brockmann.pdf (18 Febr. 2020).

Brodie, Bernard and Fawn M. Brodie (1973). *From Crossbow to H-Bomb*. Bloomington, IN: Indiana University Press.

Bromley, Mark and Giovanna Maletta (2018). *The Challenge Of Software and Technology Transfers to Non-Proliferation Efforts – Implementing and Complying with Export Controls*. Solna: SIPRI. https://www.sipri.org/sites/default/files/2018-04/sipri1804_itt_software_bromley_et_al.pdf (18 Febr. 2020).

Bulletin of the Atomic Scientists (2019), Special Issue Space, 75 (4).

Caughley, Tim (2011). The Conference on Disarmament – Breaking the Ice. Geneva: UNIDIR. https://unidir.org/files/publications/pdfs/breaking-the-ice-in-the-conference-on-disarmament-a-wrap-up-376.pdf (13 Febr. 2020).

Christopher, Grant (2019). Additive Manufacturing and the Military: Applications and Implications. In: Christian Reuter, Jürgen Altmann, Malte Göttsche, Mirko Himmel (eds.). *SCIENCE PEACE SECURITY '19 – Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research*. Darmstadt: TUprints. https://tuprints.ulb.tu-darmstadt.de/id/eprint/9164 (11 Febr. 2020).

Evangelista, Matthews (1999). *Unarmed Forces – The Transnational Movement to End the Cold War*. Ithaca NY/London: Cornell University Press.

Feiveson, Harold A., Alexander Glaser, Zia Mian and Frank von Hippel (2014). *Unmaking the Bomb: A Fissile Material Approach to Nuclear Disarmament and Nonproliferation*. Cambridge MA: MIT Press.

Fey, Marco (2017). *3D Printing and International Security – Risks and Challenges of an Emerging Technology*. Frankfurt/M.: Peace Research Institute Frankfurt. https://www.hsfk.de/fileadmin/HSFK/hsfk_publikationen/prif144.pdf (11 Febr. 2020).

Fischer, Horst, Reiner Labusch, Eckart Maus und Jürgen Scheffran (1984). Entwurf eines Vertrages zur Begrenzung der militärischen Nutzung des Weltraums. In Reiner Labusch, Eckart Maus und Wolfgang Send (Hg.). *Weltraum ohne Waffen – Naturwissenschaftler warnen vor der Militarisierung des Weltraums*. München: Bertelsmann.

Frieß, Johannes L., Anna Rössing, Gunnar Jeremias and Bernd Giese (2020). Application Scenarios for Gene Drives and new Biotechnology? *Sicherheit + Frieden* 38 (this issue).

Geist, Edward and Andrew J. Lohn (2018). *How Might Artificial Intelligence Affect the Risk of Nuclear War?* Santa Monica CA: RAND. https://www.rand.org/pubs/perspectives/PE296.html (11 Febr. 2020).

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

Himmel, Mirko (2019). Emerging Dual-Use Technologies in the life sciences: challenges and policy recommendations on export control. *EU Non-Proliferation and Disarmament Papers* 64, Stockholm: SIPRI. https://www.nonproliferation.eu/emerging-dual-use-technologies-in-the-life-sciences/ (11 Febr. 2020).

Horowitz, Michael C. (2018). Artificial Intelligence, International Competition, and the Balance of Power. *Texas National Security Review* 1 (3), 37-57.

Johnston, Trevor, Troy D. Smith, J. Luke Irwin (2018). *Additive Manufacturing in 2040 – Powerful Enabler, Disruptive Threat*. Santa Monica CA: RAND. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE283/RAND_PE283.pdf (11 Febr. 2020).

Korda, Matt and Hans M. Kristensen (2019). US ballistic missile defenses. *Bulletin of the Atomic Scientists*, 75:6, 295-306, DOI: 10.1080/00963402.2019.1680055.

Kott, Alexander, David Alberts, Amy Zalman, Paulo Shakarian, Fernando Maymi, Cliff Wang and Gang Qu (2015). *Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report*. ARL-SR-0327, Adelphi, MD: US Army Research Laboratory. http://www.arl.army.mil/arlreports/2015/ARL-SR-0327.pdf (11 Febr. 2020).

Lele, Ajey (2019). Hypersonic Weapons. In Ajey Lele. *Disruptive Technologies for the Militaries and Security,* Singapore: Springer Nature.

Lewis, James A. and Götz Neuneck (2013). *The Cyber Index – International Security Trends and Realities*. Geneva: UN Institute for Disarmament Research. http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (11 Febr. 2020).

Matthews, Michael D. and David M. Schnyer (eds.) (2019). *Human Performance Optimization: The Science and Ethics of Enhancing Human Capabilities*. Oxford: Oxford University Press.

Müller, Erwin and Götz Neuneck (eds.) (1991/1992). *Rüstungsmodernisierung und Rüstungskontrolle – Neue Technologien, Rüstungsdynamik und Stabilität*. Baden-Baden: Nomos.

Neuneck, Götz und Reinhard Mutz (Hg.) (2000). *Vorbeugende Rüstungskontrolle – Ziele und Aufgaben unter besonderer Berücksichtigung verfahrensmäßiger und institutioneller Umsetzung im Rahmen internationaler Rüstungsregime*. Baden-Baden: Nomos.

Nixdorff, Kathryn (2017). Biologie. In Jürgen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann und Dieter Wöhrle. *Naturwissenschaft – Rüstung – Frieden – Basiswissen für die Friedensforschung*. 2nd edition. Wiesbaden: Springer VS.

Pelton, Joseph N. (2019). Space Weapons, the Threat of War in Space and Planetary Defense. In Joseph N. Pelton. *Space 2.0 – Revolutionary Advances in the Space Industry*. Cham: Springer Nature.

Reinhold, Thomas and Christian Reuter (2019). Arms Control and its Applicability to Cyberspace. In Christian Reuter (ed.). *Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War and Peace*. Wiesbaden: Springer Vieweg.

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

Scharre, Paul (2018). *Army of None*. New York/London: Norton.

Schmitt, Michael N. (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2017.

Smit, Wim, John Grin and Lev Voronkov (eds.) (1992). *Military Technological Innovation and Stability in a and Changing World – Politically assessing and influencing weapon innovation and military research and development*. Amsterdam: VU University Press.

Speier, Richard H., George Nacouzi, Carrie Lee und Richard M. Moore (2017). *Hypersonic Missile Nonproliferation – Hindering the Spread of a New Class of Weapons*. Santa Monica CA: RAND. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2100/RR2137/RAND_RR2137.pdf (11 Febr. 2020).

Thee, Marek (1988). Science and Technology for War and Peace. *Bulletin of Peace Proposals* 19 (3/4), 261-292.

US DoD (Department of Defense) (2007). *Department of Defense Research & Engineering Strategic Plan*. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA472100 (11 Febr. 2020).

US DoD (Department of Defense) (2019a). *Fiscal Year (FY) 2020 Budget Estimates – Defense Advanced Research Projects Agency – Defense-Wide Justification Book Volume 1 of 5 – Research, Development, Test & Evaluation, Defense-Wide*. https://www.darpa.mil/attachments/DARPA_FY20_Presidents_Budget_Request.pdf (11 Febr. 2020).

US DoD (Department of Defense) (2019b). *Trump Signs Law Establishing U.S. Space Force*. By Jim Garamone, DOD News, Dec. 20. https://www.defense.gov/Explore/News/Article/Article/2046035/trump-signs-law-establishing-us-space-force/ (13 Febr. 2020).

Wigan, Marcus (2017). Ethics and Brain Implants in the Military. *IEEE Technology and Society Magazine* 36 (1), 65-68.

Work, Robert (2015). *Deputy Secretary of Defense Speech, 14 December*. https://www.defense.gov/News/Speeches/Speech-View/Article/634214/cnas-defense-forum.

Verhältnismäßigkeit im Humanitären Völkerrecht: Gewissensentscheidungen aus dem Blickwinkel des militärisch operativen Planungsprozesses*

Sophie Scheidt

English title: Proportionality in Humanitarian Law: Decisions of Conscience from the Perspective of the Military Operative Planning Process

Abstract: According to international humanitarian law, military decision makers must balance military necessity and humanitarian considerations when using military force against an adversary on a case-by-case basis. Determining whether or not, from a normative point of view, there is proportionality between the values weighed against each other, this article examines how these criteria are applied in the military planning and decision-making process. It discusses how the subjective element of the principle of proportionality is influenced by current technological developments in the field of artificial intelligence and what implications this might have for the legal and ethical responsibilities of military decision makers.

Keywords: Humanitarian Law, Proportionality, Targeting, Artificial Intelligence
Schlagwörter: Humanitäres Völkerrecht, Verhältnismäßigkeit, Targeting, Künstliche Intelligenz

1. Einleitung

Militärische Entscheider befinden sich bei der Anwendung militärischer Gewalt regelmäßig in dem ethischen Dilemma zwischen militärischer Notwendigkeit und Humanitätsgebot. Die Frage, in welchem Ausmaß die Akzeptanz ziviler Schäden zur Erfüllung eines militärischen Auftrags zulässig und ethisch vertretbar ist, stellt eine besondere Zuspitzung dieses Dilemmas dar. Den völkerrechtlichen Regelungsrahmen für diese Entscheidung setzt insbesondere das Prinzip der Verhältnismäßigkeit, geregelt in Art. 51 Abs. 5 b) i.V.m. Abs. 4 und Art. 57 Abs. 2 a) iii) ZP I[1], das auf dem Unterscheidungsprinzip basiert und Aussagen zum Abwägungsverhältnis der gegenüberstehenden Werte trifft. Der sehr allgemeine Wortlaut der einschlägigen Normen lässt erheblichen Auslegungsspielraum zu. Der konkrete individuelle Entscheidungsspielraum eines militärischen Entscheiders kann jedoch durch Vorgaben innerhalb des militärischen Planungs- und Führungsprozesses und die jeweils zur Verfügung stehenden Technologien erheblich begrenzt werden.

Dieser Artikel untersucht die Rahmenbedingungen, unter denen individuelle Gewissensentscheidungen mit Blick auf die Akzeptanz ziviler Schäden bei militärischer Gewaltanwendung zu betrachten sind. Hierfür werden im ersten Schritt die rechtlichen Anforderungen und Unschärfen diskutiert, die sich aus dem Prinzip der Verhältnismäßigkeit ergeben. Neben der Erfassung der abzuwägenden Werte liegt der Schwerpunkt der Untersuchung auf dem zugrunde zu legenden Abwägungsmaßstab. Zweitens wird der militärische Planungs- und Führungsprozess für multinationale Einsätze der NATO betrachtet. Hierzu wird der Prozess des *Targetings* als Kernstück dieses Planungs- und Führungsprozesses dargestellt und es wird auf die im Wesentlichen relevanten Arbeitsschritte bei der Umsetzung von Vorgaben der strategischen Ebene über die operative auf der taktischen Ebene eingegangen. Diese doktrinenbasierte Prozessbetrachtung ermöglicht eine kursorische Abbildung der Eingrenzung des rechtlich zulässigen Handlungsspielraums im militärischen Prozess für den individuellen Entscheider. Abgerundet wird die Analyse durch die Diskussion der Implikationen der zukünftigen Anwendung aktueller technologischer Entwicklungen im Bereich der Künstlichen Intelligenz und der möglichen Auswirkungen auf die Qualität der Verhältnismäßigkeitsabwägung als menschliche Gewissensentscheidung.

Dieser Artikel soll nicht zuletzt als friedenspolitischer Beitrag zu den gegenwärtigen Diskussionen im Zusammenhang mit den Regulierungsbemühungen für den Einsatz von letalen autonomen Waffensystemen (LAWS) verstanden werden, in denen gerade das Verhältnismäßigkeitsprinzip oftmals als Argument gegen LAWS herangezogen wird: Eine entsprechende „menschliche" Abwägungsentscheidung sei durch autonome Systeme nicht sicherzustellen. Dabei soll jedoch die Darstellung der Begrenzung des individuellen Handlungsspielraums und die Abhängigkeit von den verfügbaren Technologien nicht als Argument für eine Programmierbarkeit von Abwägungsentscheidungen angeführt werden. Vielmehr soll vor einer überzogenen Fokussierung auf LAWS in der rechts- und friedenswissenschaftlichen Debatte gewarnt und dafür plädiert werden, in der friedenspolitischen Diskussion die im gesamten Planungsprozess zu treffenden Entscheidungen und die in diesem Zusammenhang genutzte Technologie kritisch in den Blick zu nehmen. Aus rechtswissenschaftlicher Sicht wäre dafür insbesondere eine verstärkte Auseinandersetzung auch mit technologiespezifischen Vorsichtsmaßnahmen erforderlich und aus friedensethischer Perspektive eine differenzierte Auseinandersetzung mit der Frage, in welchem Verhältnis *Human-Machine-Teaming* unter Humanitätsgesichtspunkten ein „optimales" Ergebnis erzeugt und gleichzeitig eine menschliche Verantwortlichkeit sichergestellt wird.

---

* Dieser Beitrag wurde anonym begutachtet (double-blind peer reviewed). Den Gutachtern gilt ein herzlicher Dank.
Dieser Artikel basiert auf einer hoch geschätzten Masterarbeit aus dem Studiengang „Peace and Security Studies" an der Universität Hamburg. Die Autorin bedankt sich bei ihrem Erstgutachter Dr. Hartwig von Schubert sowie bei ihrem Zweitgutachter Prof. Dr. Stefan Oeter für die wertvollen Ratschläge. Ein weiter Dank geht an das Redaktionsteam für seine Unterstützung.
Dieser Beitrag bezieht sich ausschließlich auf öffentlich zugängliche Quellen und gibt ausschließlich die persönliche Meinung der Autorin wieder.

1 Zusatzprotokoll I zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte vom 8. Juni 1977.

DOI: 10.5771/0175-274X-2019-4-43

2. Verhältnismäßigkeit im Humanitären Völkerrecht (HVR)

Der Verhältnismäßigkeitsgrundsatz im HVR ist unter verschiedenen Bezeichnungen bekannt. Was im angelsächsischen Raum als *Rule of Proportionality*[2] bezeichnet wird, ist in Deutschland als Verhältnismäßigkeitsgrundsatz, Verhältnismäßigkeitsprinzip oder Exzessverbot bekannt. Dieser Grundsatz findet seine Rechtsgrundlagen in den oben genannten Normen des ZP I sowie im Völkergewohnheitsrecht. Danach als unterschiedslos zu bewerten und verboten ist *„ein Angriff, bei dem damit zu rechnen ist, dass er auch Verluste an Menschenleben unter der Zivilbevölkerung, die Verwundung von Zivilpersonen, die Beschädigung ziviler Objekte oder mehrere derartige Folgen zusammen verursacht, die in keinem Verhältnis zum konkreten und unmittelbaren militärischen Vorteil stehen*". In seinem Kern fordert der Verhältnismäßigkeitsgrundsatz also eine kontextbezogene Abwägung des prognostizierten konkreten und unmittelbaren militärischen Vorteils mit den prognostizierten Verlusten in der Zivilbevölkerung oder Schäden an zivilen Objekten. Maßgeblich ist daher allein, ob aus der Perspektive des Entscheiders auf Basis der zum Zeitpunkt der Entscheidung verfügbaren Informationen ein exzessiver Schadenseintritt für möglich gehalten wird[3] nicht die durch den Angriff tatsächlich verursachten Folgen.[4] Eine gewisse Objektivierung des Verhältnismäßigkeitsgrundsatzes ergibt sich jedoch aus der Verpflichtung, angemessene Vorsichtsmaßnahmen zu treffen, die insbesondere aus Art. 57 ZP I folgt.[5] Diese Maßnahmen betreffen vornehmlich die Pflicht zur Aufklärung bei der Zielidentifizierung und die Pflicht zur Warnung in dem Fall, dass die Zivilbevölkerung in Mitleidenschaft gezogen werden könnte. Art. 57 Abs. 1 a) i) ZP I fordert insbesondere „alles praktisch Mögliche zu tun", um die Unterscheidung zwischen militärischen Zielen und zivilen Objekten sicherzustellen und Art. 57 Abs. 1 a) ii) ZP I „bei der Wahl der Angriffsmittel und -methoden alle praktisch möglichen Vorsichtsmaßnahmen zu treffen", um zivile Schäden zu vermeiden bzw. zu minimieren. Die erforderlichen Vorsichtsmaßnahmen bemessen sich damit nach dem *Feasibility*-Standard. Gemäß diesem Standard soll nach der Ratifizierungsurkunde der Bundesrepublik zum ZP I alles unternommen werden, „was praktisch möglich ist, wobei alle in dem entsprechenden Zeitpunkt gegebenen Umstände zu berücksichtigen sind, einschließlich humanitärer und militärischer Überlegungen."[6] Welche Maßnahmen dies im konkreten Einzelfall jedoch erfasst, hängt maßgeblich von der Verfügbarkeit der technischen Mittel der Konfliktparteien ab, die dem militärischen Entscheider in der konkreten Situation zur Verfügung stehen.[7]

3. In Ausgleich zu bringende Abwägungswerte

Soweit sich ein Angriff gegen ein legitimes militärisches Ziel richtet, hat der militärische Entscheider unter Berücksichtigung aller erforderlichen Vorsichtsmaßnahmen den „konkreten und unmittelbaren militärischen Vorteil" zu erfassen. Dies wirft die Frage auf, welche Maßnahme Bezugsgröße des „konkreten und unmittelbaren militärischen Vorteils" ist, ob sich der Vorteil also aus einer ganzen Offensive, einer bestimmten Operation oder dem konkreten zu prüfenden Angriff auf ein Einzelziel zu ergeben hat.[8] Der Referenzrahmen für die Bestimmung des „militärischen Vorteils" reicht somit von der Betrachtung eines Angriffs auf strategischem Level bis auf die taktische Ebene.[9] Im Rahmen der Ratifizierung des ZP I wurde in den ergänzenden Interpretationserklärungen einiger Länder festgehalten, dass der „militärische Vorteil" als „advantage anticipated from the attacks as a whole and not only from isolated or particular parts of an attack" zu verstehen sei.[10] So kommt auch nach *Oeter* als Bezugsgröße nur der militärische Vorteil des Angriffs in seiner Gesamtheit in Betracht, nicht dessen einzelne oder spezifische Bestandteile.[11] Als „Angriff in seiner Gesamtheit" kann bspw. eine Vielzahl von Luftangriffen gegen ein militärisches Ziel in einem bestimmten Gebiet verstanden werden.[12] Ein etwas größerer Bezugsrahmen findet sich bei *Neumann* mit dem Verweis auf „the advantage anticipated from the military campaign, of which the attack is part, as a whole".[13] Für eine Einzel- oder jedenfalls engere Betrachtung des „militärischen Vorteils" führt *Singer*[14] die Bezugnahme der Norm auf Art. 49 Abs. 1 an, der einen „Angriff" als „isolierte (Boden-/Luft-/See-)Operation" versteht. Obwohl sich systematische Argumente für eine Bezugnahme auf den Angriff als Einzelmaßnahme anführen lassen, kann nur eine Betrachtung des Angriffs in der Gesamtheit der Operation den Strategien moderner Kriegführung Rechnung tragen, nach denen einzelne „Angriffe" selten für sich stehen, sondern vielmehr als integrierte Bestandteile eines komplexen Mosaiks von Maßnahmen zu sehen sind, wodurch ein übergeordnetes Ziel erreicht werden soll.[15] Allerdings können auch unter Bezugnahme auf die Gesamtoperation nur einige wenige oder auch hunderte von Einzelangriffen in die Abwägung einzubeziehen sein. Sicherlich erschwert sich jedoch die Erfassung der Abwägungsgegenstände erheblich, je umfassender die Bezugsgröße gewählt wird. Während der militärische Vorteil eines einzelnen Luftschlags noch recht eindeutig zu erfassen sein mag, so sind die Auswirkungen einer

2 *Neumann,* Applying the Rule of Proportionality: Force Protection and Cumulative Assessment in International Law and Morality, Yearbook of International Humanitarian Law Vol. 7 (2004) (zit.: *Neumann*, Applying the Rule of Proportionality), S. 83.

3 *Dinstein*, The Conduct of Hostilities Under the Law of International Armed Conflict (zit.: *Dinstein*, The Conduct of Hostilities), S. 132; *Singer*, Dehumanisierung der Kriegsführung. Herausforderungen für das Völkerrecht und die Frage nach der Notwendigkeit menschlicher Kontrolle (zit.: *Singer*, Dehumanisierung der Kriegsführung), S. 366.

4 *Schmitt/Widemar*, in: Targeting: The Challenges of Modern Warfare, S. 140–141; *Singer,* Dehumanisierung der Kriegsführung, S. 366; *Dinstein*, The Conduct of Hostilities, S. 132; ausführlich zum Prognostischen Element des Verhältnismäßigkeitsgrundsatzes: *Oeter*, Specifying the Proportionality Test and the Standard of Due Precaution – Problems of Prognostic Assessment in Determinig What "May be Expected" and "Anticipated" Means (in Veröffentlichung), S. 1 ff.

5 Program on Humanitarian Policy and Conflict Research at Harvard University, Commentary on the HPCR Manual on the International Law Applicable to Air and Missile Warfare, 2010 (zit.: Commentary on the HPCR Manual), Sec. D., Rule 14, Nr. 6.

6 Bekanntmachung über das Inkrafttreten der Zusatzprotokolle I und II zu den Genfer Rotkreuz-Abkommen von 1949 vom 30. Juli 1991, BGBl. 1991, Teil II, S. 968.

7 *Pillaud/de Preux*, in: Sandoz/Swinarski/Zimmermann (Hrsg.), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Genf 1987 (zit.: *Pillaud/de Preux,* Commentary on the Additional Protocols), S. 681 f., Rn. 2199.

8 *Sassòli,* Bedeutung einer Kodifikation für das allgemeine Völkerrecht mit besonderer Betrachtung der Regeln zum Schutze der Zivilbevölkerung vor den Auswirkungen von Feindseligkeiten, Basel 1990 (zit.: *Sassòli*, Bedeutung einer Kodifikation für das allgemeine Völkerrecht), S. 414.

9 ICRC International Expert Meeting, The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law, 2016 (zit.: ICRC International Expert Meeting), S. 14.

10 ICRC International Expert Meeting, S. 14; siehe auch Commentary on the HPCR Manual, Sec. D, Rule 14, Nr. 11.

11 *Oeter*, Methods and Means of Combat, in: Fleck (Hrsg.), The Handbook of International Humanitarian Law, 3. Auflage, New York 2013 (zit.: *Oeter*, Methods and Means of Combat), S. 175.

12 Commentary on the HPCR Manual, Sec. D, Rule 14, Nr. 13.

13 *Neumann,* Applying the Rule of Proportionality, S. 100.

14 *Singer*, Dehumanisierung der Kriegsführung, S. 368.

15 *Oeter*, Methods and Means of Combat, S. 175.

Operation bestehend aus einer Vielzahl von Einzelangriffen und unter Einbindung aller Teilstreitkräfte als *Joint Operation* oder sogar als *Multi-Domain Operation*, sehr viel schwieriger vorherzusagen. Dabei wären etwa die Folgen einer parallelen Cyberoperation auf ein Infrastrukturobjekt wie die eines Luftschlags gleichermaßen zu berücksichtigen, obwohl diese in Art, Ausmaß, Eintrittszeitpunkt und Eintrittsort sehr unterschiedlich ausfallen können.

Abhängig von der zugrunde gelegten Bezugsgröße stellt sich weiterführend die Frage, welche Vorteile als „unmittelbar und direkt" einzuordnen sind. Dies soll voraussetzen, dass der Vorteil eindeutig identifizierbar und in vielen Fällen quantifizierbar sei.[16] Eine etwas andere Präzisierung findet sich in der Formulierung, das Merkmal erfordere, „to show that the advantage concerned should be substantial and relatively close, and that advantages which are hardly perceptible and those which appear only in long term should be disregarded".[17] Allgemein anerkannt, aber auch von geringer Aussagekraft, ist die Feststellung, dass nach beiden Attributen ein hoher Standard zu fordern sei, nachdem jedenfalls „hypothetische" Vorteile nicht erfasst würden, sondern nur solche, die sowohl in der Operationsplanung als auch bei der -durchführung präzise bezeichnet werden können.[18] Eine erhebliche Schwierigkeit liegt darüber hinaus insbesondere in der Frage, welche Bedeutung dem Schutz des Lebens der eigenen Soldaten zukommt. Gerade für technologisch hochentwickelte Gesellschaften stellt das Leben der eigenen Soldaten das höchste Gut dar, das durch sehr gute Ausrüstung besonders geschützt werden kann. Wird im Schutz der eigenen Soldaten jedoch regelmäßig ein konkreter und unmittelbarer militärischer Vorteil gesehen, für den Kollateralschäden in Kauf genommen werden, so bleibt vom Unterscheidungsprinzip nicht mehr viel übrig.[19] Notwendigerweise gilt jedoch: je weiter der einbezogene Gesamtvorteil gefasst wird, desto weiter ist auch der Gesamtschaden der Zivilbevölkerung zu fassen.[20] Damit bleibt die Definition des „konkreten und unmittelbaren militärischen Vorteils" aufgrund der Komplexität der Strategien der Akteure, der zugrunde liegenden Operationspläne und dem unwägbaren militärischen Gesamtkontext eine Einzelfallentscheidung.[21]

Als gegenüberzustellenden Abwägungswert werden in Art. 51 und 57 insbesondere drei Arten von Verletzungen als zivile Kollateralschäden namentlich aufgeführt: die „Verluste an Menschenleben unter der Zivilbevölkerung, die Verwundung von Zivilpersonen und die Beschädigung ziviler Objekte". Ist die kategoriale Einordnung als zivile Person oder ziviles Objekt zu bejahen, können sich insbesondere bei der Frage, welche Arten der Schädigung bei der Abwägung zu berücksichtigen sind, erhebliche Schwierigkeiten ergeben. Bspw. sollen Unannehmlichkeiten oder Belästigungen, Irritationen, Stress oder Angst oder derartige schwer fassbare Beeinträchtigungen grundsätzlich nicht als Verwundungen oder Verletzungen erfasst werden.[22] Für eine Berücksichtigung von psychischen Schäden spricht jedoch die gleichwertige Bedeutung von psychischer und physischer Beeinträchtigung, die das heutige Verständnis von Gesundheit prägt.[23] Zudem kann gerade die heute mögliche ständige Gegenwärtigkeit von Waffensystemen, wie etwa bewaffneten Drohnen, über städtischen Gebieten zu erheblichen psychischen Belastungen der Bevölkerung führen. Erhebliche Schwierigkeiten wirft auch die Frage auf, über welche Zeitdauer[24] oder über welche Distanz zivile Schäden zu berücksichtigen sind. Insbesondere bei der Zerstörung von *Dual-Use*-Objekten, die auch die zivile Infrastruktur, wie bspw. ein Elektrizitätswerk, betreffen, ist schwerlich vorhersagbar, wie viel Zeit der Gegner benötigt, um diese wieder für zivile Zwecke nutzbar zu machen.[25] Diese Frage stellt sich insbesondere auch bei Cyberoperationen, bei denen Schäden verzögert entstehen und/oder an völlig anderen Orten als dem des militärischen Ziels auftreten können. Dies hat bspw. der Cyberangriff der US-Streitkräfte auf einen IT-Server im Irak im Jahr 2008 gezeigt, der zugleich Auswirkungen auf die Internetverbindungen und IT-Systeme in Saudi-Arabien, Deutschland und Texas hatte.[26]

4. Verhältnismäßigkeit im Engeren

Diese nach den bisherigen Darstellungen bestmöglich zu erfassenden Abwägungsgegenstände sind nach den Vorgaben der Art. 51, 57 ZP I miteinander ins Verhältnis zu setzen. Art. 51 Abs. 5 b) ZP I enthält hierfür die Formulierung, durch den Angriff dürfe kein Kollateralschaden verursacht werden, „der in keinem Verhältnis" zum militärischen Vorteil steht („excessive in relation to the concrete and direct military advantage"). Diese Formulierung legt nahe, dass im Hinblick auf die Intensität der Verhältnismäßigkeitsprüfung keine „strenge Verhältnismäßigkeitsprüfung", sondern lediglich eine „Exzesskontrolle" i.S. einer „gelockerten Verhältnismäßigkeitsprüfung" zu fordern ist.[27] Überwiegend wird daher die Auffassung vertreten, Unverhältnismäßigkeit könne nur dann angenommen werden, wenn ein signifikantes Missverhältnis zwischen dem antizipierten militärischen Vorteil und dem zu erwartenden zivilen Schaden" bestehe.[28] Demnach würde eine grundsätzliche Gewichtung zugunsten des militärischen Vorteils angenommen werden, sodass ein „übermäßiges Überwiegen" des Kollateralschadens erforderlich wäre, um einen Angriff als unverhältnismäßig bzw. „exzessiv" zu qualifizieren. Eine derartige Verschiebung zugunsten des militärischen Vorteils berge die Gefahr, dass ein Angriff letztendlich kaum oder sogar niemals unverhältnismäßig sei[29], und damit das dem HVR zugrunde liegende Ziel, eine bestmögliche Balance zwischen militärischen Erwägungen und dem Prinzip der Menschlichkeit zu finden, das im Verhältnismäßigkeitsgrundsatz besonderen Ausdruck findet,[30] verfehlt würde. Mit Blick auf die Schutzfunktion des

16 Commentary on the HPCR Manual, Sec. D, Rule 14, Nr. 9.
17 *Pillaud/de Preux*, Commentary on the Additional Protocols, S. 681 f., para. 2209.
18 ICRC International Expert Meeting, S. 13.
19 *Oeter*, Methods and Means of Combat, S. 191.
20 *Sassòli*, Bedeutung einer Kodifikation für das allgemeine Völkerrecht, S. 415.
21 ICRC International Expert Meeting, S. 15.
22 Program on Humanitarian Policy and Conflict Research at Harvard University, HPCR Manual on International Law Applicable to Air and Missile Warfare, Cambridge 2013 (zit.: HPCR Manual on International Law), Rule 14, Nr. 2.
23 ICRC International Expert Meeting, S. 36.
24 *Holland*, Military Objective and Collateral Damage: Their Relationship and Dynamics, Yearbook of International Humanitarian Law Vol. 7 (2004) (zit.: *Holland*, Military Objective and Collateral Damage), S. 48.
25 *Oeter*, Comment: Is the Principle of Distinction Outdated, in: International Humanitarian Law Facing New Challenges (zit.: *Oeter*, Comment: Is the Principle of Distinction Outdated), S. 58; *Holland*, Military Objective and Collateral Damage, S. 48.
26 *Romanosky/Goldmann*, Understanding Cyber Collateral Damage, Journal of National Security Law & Policy Vol. 9 (2017), S. 246; siehe insbesondere zu indirekten Effekten von Cyberoperationen auch: *Newton*, Proportionality and Precautions in Cyber Attacks, in: Saxon (Hrsg.), International Humanitarian Law and the Changing Technology of War, Leiden, Boston 2013, S. 246 f.
27 *Müller*, Abwägung von Menschenleben im Völkerrecht, in: Baade/Ehricht/Fink/Frau/Möldner/Risni/Stirner, Verhältnismäßigkeit im Völkerrecht (zit.: *Müller*, Abwägung von Menschenleben im Völkerrecht), S. 72.
28 Commentary on the HPCR Manual, Sec.D, Rule 14, Nr. 7.
29 *Singer*, Dehumanisierung der Kriegsführung, S. 371.
30 *Gasser/Dörmann*, Protection of the Civilian Population, in: Fleck (Hrsg.), The Handbook of International Humanitarian Law, 3. Auflage, New York 2013 (zit.: *Gasser/Dörmann*, Protection of the Civilian Population), S. 244.

HVR für die Zivilbevölkerung argumentiert *Müller*[31] daher dafür, „das Exzessverbot in Richtung einer echten Verhältnismäßigkeitsprüfung aufzuladen und so die Prüfintensität im HVR jener im Menschenrechtsschutz anzunähern". Ein Mittelweg findet sich bei *Dinstein*, der darauf abstellt, ob der antizipierte zivile Schaden den militärischen Vorteil objektiv erkennbar überwiegt.[32] Die sehr unterschiedliche Akzeptanz der Staaten gegenüber zivilen Opfern lässt eine einheitliche Staatenpraxis diesbezüglich nicht erkennen. Ist bereits der Abwägungsmaßstab umstritten, bestehen noch erheblich größere Unklarheiten darüber, wann ein solches Missverhältnis tatsächlich gegeben ist. Nicht unverhältnismäßig kann allein „ein zahlenmäßiges Überwiegen bspw. von potenziellen zivilen Opfern" sein.[33] Auch ein extensiver ziviler Schaden begründet nicht zwingend Unverhältnismäßigkeit, solange diesem ein vergleichbar großer militärischer Vorteil gegenübersteht.[34] Um hierdurch jedoch nicht den Distinktionsgrundsatz gänzlich auszuhebeln, fordern *Gasser und Dörmann* die Festlegung einer Obergrenze eines akzeptierbaren maximalen Schadens.[35] Die erhebliche Schwierigkeit in der Handhabung des Verhältnismäßigkeitsgrundsatzes resultiert jedoch gerade daraus, dass hier zwei sehr ungleiche Werte gegeneinander abgewogen und in Ausgleich gebracht werden müssen. Für eine derartige Abwägung gibt es schlicht keine Methode, sodass sie stets weitgehend subjektiv bleibt.[36]

5. Operationalisierung der rechtlichen Maßgaben im militärischen Prozess

All diese rechtlichen Herausforderungen sind in der Praxis zu handhaben und ungeklärte Fragen damit letztlich auch zu beantworten. In diesem Abschnitt sollen die rechtlichen Vorgaben des Verhältnismäßigkeitsstandards in den relevanten militärischen Kontext gestellt und insbesondere soll der Frage nachgegangen werden, in welcher Weise und in welchen Prozessschritten der weite rechtliche Auslegungsspielraum ausgefüllt wird. Ein Kernstück des militärischen Planungsprozesses auf operativer Ebene in multinationalen Operationen der NATO stellt der *Joint Targeting*-Prozess dar. *Joint Targeting* bezeichnet dabei die Verlinkung der auf strategischer Ebene festgelegten Ziele und Vorgaben mit den auf taktischer Ebene erforderlichen Maßnahmen durch den *Joint Targeting Cycle* (*JTC*) auf der operativen Ebene in einer zielgerichteten und systematischen Weise, um spezifische Effekte zur Verwirklichung der militärischen Ziele und übergeordneten Zielvorgaben zu erreichen.[37]

Der *JTC* beschreibt die notwendigen Arbeitsschritte, die in einem Regelkreislauf von sechs Phasen stetig wiederholt werden und ist als ein Bestandteil einer umfassenden Architektur von ineinandergreifenden Prozessen in einer Prozesslandkarte zu verstehen. Bereits in den unterschiedlichen vorangestellten Phasen des NATO-Planungsprozesses auf der strategischen Ebene werden wesentliche Vorgaben für den *Targeting*-Prozess erarbeitet. Ein daraus entstehendes, noch generisches Operationskonzept einschließlich eines strategischen Operationsplans, wird durch den Nordatlantikrat, das oberste politische Gremium der Allianz, genehmigt. Darin können bereits wesentliche Vorgaben für den *Targeting*-Prozess auf operativer Ebene enthalten sein, wie bspw. eine Liste möglicher zu bekämpfender Ziele, die sogenannte *Joint Target List*, die im weiteren Verlauf des *Targeting*-Prozesses fortentwickelt und konkretisiert wird. Abhängig von dem festgesetzten Zeitrahmen zur Durchführung einer Zielbekämpfung stehen innerhalb des *Targeting*-Prozesses das *Deliberate* und das *Dynamic Targeting* zur Verfügung. Dabei stellt *Deliberate Targeting* den Regelfall des Prozesses dar, der iterativ etwa in einem 72-Stundenzyklus wiederholt wird, während das *Dynamic Targeting* als komprimierter Prozess für Ziele mit zeitlicher oder räumlicher Beschränkung angewendet wird[38] wie bspw. mobile Raketenabschussrampen.

Die auf politisch-strategischer Ebene vom Nordatlantikrat sehr allgemein beschriebenen Ziele, wie bspw. der Schutz von Zivilisten, werden vom *Joint Force Commander* (*JFC*) auf operativer Ebene zunächst in eindeutige militärische Zielvorgaben (*objectives and guidances*) umgesetzt, die auf den nachfolgenden Hierarchiestufen weiter konkretisiert werden. Unter Berücksichtigung der Vorgaben aus dem Operationsplan wird festgehalten, unter welchen Umständen, nach welchen Parametern und mit welchen Mitteln diese Effekte erzielt werden sollen. Für die Zielerreichung werden dabei *measures of performance* (quantitativ) und *measurements of effectiveness* (qualitativ) festgelegt, an denen die Durchführung und Folgen eines Angriffs zu bemessen sind. Dies erfolgt in einem ständigen Abstimmungsprozess zwischen dem *JFC* und seinen *Component Commanders*, den Kommandeuren der Hauptquartiere der einzelnen Domänen (Land, See, Luft, Cyber und zukünftig Space). Auf diese Weise wird sichergestellt, dass jedes militärische Ziel eindeutig einem zu erzielenden Effekt zugeordnet wird.[39] Aus rechtlicher Sicht werden bereits in dieser Phase Maßgaben für den zu avisierenden „konkreten und unmittelbaren militärischen Vorteil" getroffen. Diese werden auf den unterschiedlichen Hierarchieebenen durch die jeweilige Konkretisierung stets nach Art und Umfang variieren. Die Festlegung eindeutiger und erreichbarer Zielvorgaben in dieser Phase stellt die entscheidende Voraussetzung für den Erfolg des *Targeting*-Prozesses dar.[40] Wenn die *objectives* vage oder unpraktikabel sind oder auf fehlerhaften Informationen beruhen, wird die Verantwortung für den Erfolg auf die anderen Schritte des Prozesses verschoben. Ob dies gelingt, hängt maßgeblich von der Beachtung der politischen Ziele, einem Verständnis des Konflikts, der Qualität der Informationen und der Fähigkeiten der teilnehmenden Akteure ab.[41]

Die nächste Phase dreht sich um die Auswahl und Charakterisierung möglicher militärischer Ziele und dient der Zielauswertung, -überprüfung, -bewertung, -nominierung und -priorisierung.[42] Auf der Basis einer gründlichen Analyse der Fähigkeiten des Gegners und der Untersuchung der Umgebung der potenziellen Ziele und der Zusammenhänge oder Netzwerkverbindungen mit anderen möglichen Zielen (*Target System Analysis*) wird ein Gesamtsystem des Gegners gebildet, um die für die Zielerreichung erforderlichen Maßnahmen in quantitativer und qualitativer

31 *Müller*, Abwägung von Menschenleben im Völkerrecht, S. 73.
32 *Dinstein*, The Conduct of Hostilities, S. 131.
33 *Singer*, Dehumanisierung der Kriegsführung, S. 372.
34 HPCR Manual on International Law, Rule 14, Nr. 8.
35 *Gasser*/*Dörmann*, Protection of the Civilian Population, S. 245.
36 *Holland*, Military Objective and Collateral Damage, S. 46.
37 NATO Standard AJP 3-9 Allied Joint Doctrine for Joint Targeting, Ed. A, Vers. 1. April 2016.
38 NATO Standard AJP 3-9 Allied Joint Doctrine for Joint Targeting, Ed. A, Vers. 1. April 2016.
39 *Ekelhof*, Lifting the Fog of Targeting – "Autonomous Weapons" and Human Control Through the Lens of Military Targeting, Naval War College Review Vol. 71 (2018) No. 3. Art. 6 (zit.: *Ekelhof*, Lifting the Fog of Targeting), S. 7.
40 *Pratzner*, The Current Targeting Process, in: Ducheine/Schmitt/Osinga (Hrsg.), Targeting: The Challenges of Modern Warfare (zit.: *Pratzner*, The Current Targeting Process), S. 81.
41 *Pratzner*, The Current Targeting Process, S. 81.
42 *Ekelhof*, Lifting the Fog of Targeting, S. 7.

Hinsicht festzulegen.[43] Die auf diese Weise als relevant identifizierten militärischen Ziele werden den vom Nordatlantikrat freigegebenen Zielkategorien (*Targetsets*) zugeordnet. Hieraus ergibt sich ein Kontrollmechanismus, der die Einhaltung der Vorgaben der politisch-strategischen Ebene sicherstellen soll.[44] Soweit sich später im Prozess herausstellt, dass weitere militärische Ziele nominiert werden sollen, die nicht diesen Kategorien entsprechen, müssen diese den gesamten Prozess durchlaufen und vom Nordatlantikrat freigegeben werden. Ziele, bei denen möglicherweise zivile Schäden entstehen, werden als solche gekennzeichnet, auf die Priorisierung nimmt dies jedoch zunächst keinen Einfluss. Maßgeblich ist vielmehr, ob es sich um militärisch besonders bedeutsame Ziele handelt, deren Zerstörung der Erreichung der eigenen strategischen Ziele dient oder ob von ihnen eine akute Gefahr ausgeht oder auszugehen droht.

Von entscheidender Bedeutung in dieser Phase ist die Sensor- und Informationstechnologie zur Aufklärung (*Intelligence, Surveillance, Reconnaissance* (*ISR*)), die hierfür zur Verfügung steht.[45] Die Anzahl von *ISR*-Sensoren, der Umfang des Netzwerks menschlicher Informationsquellen und die Größe des Analyseteams zur Auswertung dieser Informationen werden hier als entscheidende Erfolgsfaktoren bei der Festlegung der militärischen Ziele und dem Erfolg der Operation genannt.[46] Dabei ist weniger die Quantität als vielmehr die Qualität der Informationen entscheidend, die ein tiefgreifendes Verständnis des Gegners, die Simulation möglicher Reaktionen auf Handlungsoptionen und ein vollständiges Bild der Resilienz und Reaktionsfähigkeiten des Gegners ermöglicht.[47] In dieser Phase ist also sicherzustellen, dass alle avisierten Ziele militärische Ziele i.S.d. Art. 52 Abs. 2 ZP I sind und alle Unsicherheiten, die im Zusammenhang mit dieser Definition bestehen, behoben werden. Hierfür werden insbesondere *No-Strike*-Listen geführt. Diese benennen Objekte, die nicht angegriffen werden dürfen, entweder, weil es sich um zivile Objekte handelt oder weil deren Angriff den Beziehungen zu Bündnispartnern schaden würde. Demgegenüber enthält die *Restricted target*-Liste militärische Ziele, die jedoch bestimmten Einschränkungen unterliegen, bspw. weil deren Bekämpfung negative operative oder politische Folgen hätte.[48]

Nach der Festlegung der möglichen militärischen Ziele werden diese priorisiert und es wird für deren Bekämpfung eine aufeinander abgestimmte Kombination möglicher letaler oder nicht letaler Fähigkeiten und Einsatzmodalitäten entwickelt.[49] Hierbei spielen insbesondere die Berechnung der Waffenwirksamkeit, also der Wirkung der verfügbaren Waffensysteme unter den jeweiligen Parametern (*Weaponeering*) und die mögliche Auswirkung auf die Zivilbevölkerung, eine Rolle. Die Abschätzung möglicher Kollateralschäden erfolgt in den Einsätzen der NATO nach der US-amerikanischen *Collateral Damage Estimation Methodology* (*CDE*), die eine Abstufung der erwarteten Auswirkung des Einsatzes eines Wirksystems auf die *CDE*-Level 1–5 vorsieht. Die jeweilige Abstufung richtet sich dabei nach den entsprechenden operationellen Einschränkungen, die sich aus der Wirkung dieses Wirksystems ergeben. Entsprechend dem ansteigenden *CDE*-Level steigt auch die notwendige militärische Befehlsgewalt (*Target Engagement Authority*) an, sodass die Entscheidungsbefugnis bei einer Operation auf *CDE*-Level 5, bei der mit zivilen Opfern zu rechnen ist, auf einer hohen militärischen Hierarchieebene oder sogar auf politischer Ebene liegt, während eine Entscheidung auf *CDE*-Level 1 auch durch den Piloten getroffen werden könnte.[50]

Auf der Grundlage dieser Informationen erteilt der *JFC* im nächsten Schritt seine endgültige Genehmigung hinsichtlich der priorisierten Ziele und der entsprechenden Maßnahmen und Wirkmittel, mit denen dieses Ziel bekämpft werden soll. Für den *JFC* stellt sich damit für jedes einzelne Ziel die Frage, ob oder inwieweit er beim Angriff eines militärischen Ziels zivile Schäden in Kauf nimmt. Hierbei stehen ihm regelmäßig ein Rechtsberater, ein politischer Berater und ein interkultureller Einsatzberater zur Seite. Der Entscheider muss hierfür also Klarheit darüber haben, welche Bezugsgröße er bei seiner Entscheidung zugrunde zu legen hat, dies auch, wenn die Gesamtoperation aus hunderten von Zielen besteht. Der Entscheidungsspielraum des *JFC* wird in der Praxis jedoch erheblich durch die politischen Vorgaben aus dem Operationsplan und den *ROEs* bestimmt. Durch die Zuordnung dieser Ziele an die nachgeordneten *Component Commands* erfolgt die Weitergabe der militärischen Ziele vom operativen auf das taktische Level.[51] In der nächsten Phase erfolgt die Ausplanung und Durchführung der Maßnahmen auf taktischer Ebene, indem wiederum die in den Phasen 1-4 beschriebenen Arbeitsschritte in vergleichbarer Weise durchlaufen werden.[52] Hierfür werden im ersten Schritt die aus allen verfügbaren Quellen vorhandenen Informationen zusammengeführt, um die priorisierten Ziele aufzuklären und zu analysieren, ob Umstände eingetreten sind, aufgrund derer die Zielbekämpfung abgebrochen werden muss. Ist dies nicht der Fall, werden die (geografischen) Daten der Ziele ermittelt, das Ziel durchgehend beobachtet, angegriffen und überprüft, ob die erwünschten Effekte eingetreten sind. Für den auf taktischer Ebene agierenden Operateur bleibt hier nur noch geringfügiger Entscheidungsspielraum, es geht vielmehr darum, die Ziele nach den freigegebenen Vorgaben erfolgreich zu bekämpfen. Erhebliche Bedeutung kommt hier allerdings der Pflicht nach Art. 57 Abs. 2 a) iii) ZP I zu, Angriffe gegebenenfalls abzubrechen. Abschließend folgt mit dem *Battle Damage Assessment* die Evaluation der eingetretenen Effekte.

Die Planung der multinationalen militärischen Operationen der NATO erfolgt in komplizierten Prozessen und Organisationsstrukturen. Die ständige Wiederholung der dargestellten Prozessschritte spiegelt dabei das Bemühen wider, auf der Grundlage eines stets aktuellen Lagebildes den rechtlichen Vorgaben bestmöglich Rechnung zu tragen. Die aus dem Verhältnismäßigkeitsgrundsatz resultierenden Vorgaben werden hierbei in standardisierte militärische Prozesse oder Kategorien übersetzt, die der Vereinfachung, Beschleunigung und Kontrolle der Durchführung der Operationen dienen. Diese Betrachtung zeigt, dass die individuelle Abwägungsentscheidung eines militärischen Entscheiders als Ergebnis eines komplexen Prozesses zu verstehen ist, in dem jede Entscheidung Auswirkungen und Dynamiken für Folgeentscheidungen entfaltet und der individuelle Beurteilungsspielraum mit Blick auf die Frage, ob normativ betrachtet ein Missverhältnis vorliegt, innerhalb des weiten rechtlichen Rahmens erheblich eingeschränkt ist. Von erheblicher Relevanz ist innerhalb dieser

43 *Ekelhof*, Lifting the Fog of Targeting, S. 10.
44 *Ekelhof*, Lifting the Fog of Targeting, S. 7.
45 NATO Standard AJP 3-9 Allied Joint Doctrine for Joint Targeting, Ed. A, Vers. 1. April 2016, Chapter 4, Section VI.
46 *Pratzner*, The Current Targeting Process, S. 81.
47 *Pratzner*, The Current Targeting Process, S. 83.
48 NATO Standard AJP 3-9 Allied Joint Doctrine for Joint Targeting, Ed. A, Vers. 1. April 2016.
49 *Ekelhof*, Lifting the Fog of Targeting, S. 7.
50 *Werres*, Der Targeting-Prozess in der NATO, in: Gillner/Stümke (Hrsg.), Kollateralopfer. Die Tötung von Unschuldigen als rechtliches und moralisches Problem, S. 49.
51 *Ekelhof*, Lifting the Fog of Targeting, S. 8.
52 *Ekelhof*, Lifting the Fog of Targeting, S. 8.

Prozessschritte, mit welchem Grad an Wahrscheinlichkeit das jeweils prognostizierte Ergebnis vorhergesagt werden kann und ob dieses dann tatsächlich auch eintritt.

6. Implikationen der Nutzung von auf Künstlicher Intelligenz-basierter Software im Targeting-Prozess

Von herausragender Bedeutung für die Antizipation dieser Eintrittswahrscheinlichkeit von Handlungsoptionen ist die in modernen Streitkräften als *Intelligence, Surveillance, Target acquisition, and Reconnaissance (ISTAR* oder *ISR))* bekannte Funktion. Diese Funktion kann durch technologische Mittel so ausgestaltet werden, dass militärischen Entscheidern durch die Bereitstellung von Echtzeitinformationen die Kontextualisierung von Geschehnissen kontinuierlich ermöglicht wird.[53] Während bislang die entscheidenden Herausforderungen in der Generierung der relevanten Daten lagen, erweisen sich heute aufgrund der rasant angewachsenen verfügbaren Rohdatenmassen die fehlenden Kapazitäten in der Analyse und Bewertung dieser Daten als entscheidende Schwachstelle. Die in den letzten Jahren veröffentlichten militärischen Strategiepapiere zur Nutzung Künstlicher Intelligenz (KI)[54] verbunden mit den erheblichen Investitionen in die Forschung KI-basierter Technologie zeigen, welche Bedeutung der Steigerung der Analysefähigkeiten durch diese Technologie militärstrategisch beigemessen wird. Ein Blick auf aktuelle Projekte der DARPA[55] gibt Hinweise darauf, welche künftigen Entwicklungen in diesem Bereich zu erwarten sind, und in welchem erheblichen Ausmaß die menschliche Wahrnehmung und Bewertung durch KI-basierte Technologie beeinflusst werden wird. So soll die Vernetzung unstrukturierter Datenquellen aus Texten, gesprochener Sprache, Bildern, Videos oder anderen Informationsquellen ein ganzheitlicheres Lagebewusstsein erzeugen. Zudem könnten Datenanalyseprogramme etwa unterschiedliche Interpretationsmöglichkeiten des aus vernetzten Datenquellen extrahierten Informationsgehaltes anbieten,[56] sicherheitsrelevante Ereignisse in zeitliche Abfolge gesetzt und die involvierten Teilnehmer identifiziert werden,[57] oder aus Texten implizit enthaltene Informationen zur Unterstützung bei der Bewertung und Durchführung von Operationen extrahiert werden.[58]Auch die Verifikation von Informationen wie etwa die Bewertung der Authentizität von Bildern,[59] die Entdeckung und Abwehr von Cyberbedrohungen[60] oder die Abwägung möglicher Handlungsalternativen und Berechnung der Eintrittswahrscheinlichkeit von Optionen,[61] rechtlich gesprochen also der Eintrittswahrscheinlichkeit eines militärischen Vorteils bzw. möglicherweise auch ziviler Schäden sollen durch entsprechende Analyseprogramme ermöglicht werden. Diese Projekte zeigen beispielhaft, wie mittels KI-basierter Algorithmen auch Informationen erzeugt werden, die nur als Teilstücke einer in dem hochkomplexen Prozess moderner militärischer Informationsgewinnung generierten *Intelligence* verstanden werden können. Es besteht die Hoffnung, aus einer Vielzahl dieser Einzelelemente ein noch umfassenderes Lagebild und daraus resultierende Handlungsoptionen insbesondere auch für den Cyber- und Informationsraum schaffen zu können. Im Hinblick auf den oben dargestellten *Targeting Cycle* kann festgehalten werden, dass die so generierten Informationen das Grundverständnis der militärischen Entscheider über das konzeptionelle und moralische Verständnis des Gegners prägen und von Beginn an den Prozess des *Targetings* beeinflussen. Aber auch die Durchführung von Aufgaben auf operativer Ebene wie etwa die extrem verantwortungsvolle, zeitaufwendige und entsprechend ressourcenbeanspruchende Aufgabe der *Target System Analysis* soll im Rahmen des *Algorithmic Warfare Cross-Functional Team* (*AWCF*) des US Department of Defense (*DoD*) zukünftig auch durch KI-basierte Technologien unterstützt oder sogar durchgeführt werden, was zum Wegfall einer Entscheidungsebene führen kann. Hierfür wird angeführt, dass gerade die Kontinuität des Prozesses relevant ist, um die notwendige Anpassungsfähigkeit an sich ändernde Umstände zu erzeugen, die mit der derzeit immer zu geringen Anzahl des *Targeting*-Personals westlicher Streitkräfte nicht sichergestellt werden kann.[62] Dies bedeutet, dass zukünftig die entscheidenden vorbereitenden Maßnahmen, die die Priorisierung auf der Zielliste beeinflussen und die Grundlage für die Bewertung des militärischen Vorteils darstellen, durch KI-basierte Technologie erfolgen können. Auch die Berechnung der Waffenwirksamkeit und möglicher ziviler Schäden erfolgt mittlerweile teilweise softwarebasiert.[63] Diese Software berechnet auf der Basis von Einsatzerfahrungen sowie zahlreicher Versuche und Experimente die Schadens- und Zerstörungswahrscheinlichkeit für die spezifische Einsatzmodalität. Gerade die Prognostizierung der Auswirkungen von Angriffen auf Infrastruktureinrichtungen, die auch zu zivilen Zwecken genutzt werden, oder Netzwerksysteme, mit denen auch zivile Einrichtungen verbunden sind, sind durch den hohen Vernetzungsgrad sehr schwer vorherzusagen.[64] Daher wird insbesondere für die Abschätzung der Folgen der Beschädigungen von kritischer Infrastruktur wie Stromnetzen, Abwassersystemen oder Wasseraufbereitungsanlagen die Erweiterung durch KI-basierte Technologien als hilfreich erachtet. Diese könne bspw. Informationen von Ingenieuren über die städtischen Infrastrukturen, Informationen aus Satellitenaufklärungssystemen und *Signals Intelligence* in neuronalen Netzwerken oder durch andere KI-Algorithmen verarbeiten und hierauf aufbauend weitere online verfügbare Daten ausfindig machen und gegebenenfalls mit Hilfe von GPS ermittelten Koordinaten versehen.[65] Darüber hinaus wird KI-basierte Technologie auch für die Überprüfung und Sicherstellung der Einhaltung von Prozess- und Sicherheitsstandards in Informationssystemen als hilfreich erachtet. Hierdurch könnten bspw. automatische Warnmeldungen erfolgen, wenn bestimmte Sicherheitskriterien nicht erfüllt sind, wie etwa

53 *Stewart*, Maximising Compliance with IHL and the Utility of Data in an Age of Unlimited Information: Operational Issues, in: Saxon (Hrsg.), International Humanitarian Law and the Changing Technology of War, Leiden, Boston 2013 (zit.: *Stewart*, Maximising Compliance with IHL), S. 178.

54 Summary of the 2018 Department of Defense Artificial Intelligence Strategy, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (Zugriff: 09.02.2020); Next Generation Artificial Intelligence Development Plan (AI-Strategiepapier für zivile und militärische Zwecke), http://fi.china-embassy.org/eng/kxjs/P020171025789108009001.pdf (Zugriff: 09.02.2020).

55 Die Defence Advanced Research Projects Agency ist eine staatliche Forschungsagentur, die dem US-Verteidigungsministerium unterstellt ist.

56 Siehe etwa https://www.darpa.mil/program/active-interpretation-of-disparate-alternatives (Zugriff 09.02.2020).

57 Siehe etwa https://www.darpa.mil/program/knowledge-directed-artificial-intelligence-reasoning-over-schemas (Zugriff 09.02.2020).

58 Siehe etwa https://www.darpa.mil/program/deep-exploration-and-filtering-of-text (Zugriff 09.02.2020).

59 Siehe etwa https://www.darpa.mil/program/media-forensics (Zugriff 09.02.2020).

60 Siehe etwa https://www.darpa.mil/program/cyber-hunting-at-scale (Zugriff 09.02.2020).

61 Siehe etwa https://www.darpa.mil/program/causal-exploration (Zugriff 09.02.2020).

62 *Ekelhof*, Lifting the Fog of Targeting, S. 18 f.

63 *Ekelhof*, Lifting the Fog of Targeting, S. 14.

64 *Holland*, Military Objective and Collateral Damage, S. 60.

65 *Margulies*, The Other Side of Autonomous Weapons, Legal Studies Research Paper Series, Research Paper 182 (2018), http://ssrn.com/abstract=3194713 (zit.: *Margulies*, The Other Side of Autonomous Weapons), S. 41.

die Beachtung der *No Strike List*, was etwa bei dem Angriff auf das Krankenhaus in Kunduz unterlassen wurde und eine der Ursachen für den tödlichen Angriff war. Zudem könnten diese Tools Hinweise darauf geben, ob Veränderungen eingetreten sind, die einen Aktualisierungsbedarf dieser Listen erfordern.[66] Sollte durch die Nutzung KI-basierter Technologien tatsächlich ein deutlich verbesserter Schutz von Zivilisten erzeugt werden, könnte dies für militärische Entscheider eine Pflicht zum Einsatz dieser Technologien begründen. Für Staaten könnte sich daraus dann sogar die Pflicht zur Entwicklung oder Beschaffung dieser Technologien ergeben.[67]

7. Ausblick

Der weite rechtliche Auslegungsspielraum hinsichtlich der Frage, unter welchen Voraussetzungen ein Missverhältnis zwischen militärischer Notwendigkeit und zivilen Schäden gegeben ist, wird mit Blick auf den individuellen Entscheidungsspielraum militärischer Planer und Entscheider erheblich von den jeweils angewendeten militärischen Prozessen und verfügbaren technologischen Fähigkeiten determiniert. Dabei scheint sich die Herausforderung dieser Abwägung von der Frage, ob im konkreten Einzelfall normativ betrachtet ein konkretes Missverhältnis anzunehmen ist zunehmend auf die Frage zu verlagern, mit welchem Grad an Wahrscheinlichkeit dieses Verhältnis prognostiziert werden sollte, welche Quellen als ausreichend transparent heranzuziehen sind und wieviel originäres menschliches Einschätzungsvermögen gegenüber der technologischen Assistenz hierbei mit einzubeziehen ist. Grundsätzlich stellen die technologischen Fortschritte und die Generierung riesiger Datenmengen verbunden mit entsprechenden Analysetools einen eindeutig positiven Beitrag zu einer informierten und wohl abgewogenen Entscheidung dar, wenn diese Datenmengen auch tatsächlich verarbeitet werden können. In asymmetrischen Konflikten, in denen u.a. Operationen hochtechnologisierter Staaten aus großen Entfernungen geführt werden[68] und technologisch unterlegene Akteure den Schutz unter der Zivilbevölkerung suchen[69] oder im Cyberraum, in dem Grenzziehung bereits im Hinblick auf Territorialität nicht existiert[70] und die klassische Vorstellung klarer Frontlinien aufgehoben wird, kommt der umfassenden Aufklärung, der Attribution und der Simulation von Handlungsoptionen sowie der Präzision der Berechnung des Wirkmitteleinsatzes zum Schutz der Zivilbevölkerung eine entscheidende Rolle zu. Auch die Beschleunigung von Entscheidungsprozessen und Reaktionsfähigkeiten kann in Auseinandersetzungen gerade zwischen hochtechnologisierten Staaten zum Schutz der Bevölkerung entscheidend sein. Mit Blick auf aktuelle Entwicklungen KI-basierter Technologie finden sich daher im angelsächsischen Raum Stimmen, die in KI-basierten Technologien im *Targeting*-Prozess ein erhebliches Potenzial i.S. einer verbesserten „IHL Compliance" sehen.[71] Dies setzt jedoch voraus, dass durch deren Einsatz für spezifische Anwendungsbereiche Kontrollmechanismen *hinzutreten* und nicht menschliches Beurteilungsvermögen grundsätzlich *ersetzt* oder Angriffsszenarien *ermöglicht* werden.

Die entscheidende Herausforderung wird also darin liegen, die Nutzung von technologischer Assistenz so weit in die spezifischen militärischen Prozesse zu implementieren, wie hierdurch zusätzliche Kontrolle erzeugt wird und die *funktionale* Entscheidungsmacht militärischen Personals und damit eine moralische und rechtliche menschliche Verantwortlichkeit sichergestellt werden kann. Nur auf diese Weise wird neben einer Staatenverantwortlichkeit grundsätzlich auch eine vielseits geforderte individuelle menschliche Verantwortlichkeit begründet werden können. Dies wird vor allem die Konkretisierung technologiespezifischer Vorsichtsmaßnahmen und ein kritisches Bewusstsein gegenüber einem übersteigerten Vertrauen in die Automation erfordern.[72] Zudem müsste für die militärischen Entscheider Rechtssicherheit in der Frage geschaffen werden, welche Konsequenzen bei Entscheidungen für oder gegen die Handlungsempfehlung eines technologischen Assistenzsystems zu erwarten sind. Denn würden militärische Entscheider stets der Empfehlung der Software folgen, läge hier *funktional* keine menschliche Entscheidung mehr vor, würden sie sich jedoch auf ihre persönliche Erfahrung verlassen und sich gegen eine Empfehlung der Software entscheiden, könnte ein tatsächlich unverhältnismäßiger ziviler Schaden zu einem erheblichen Haftungsrisiko des militärischen Entscheiders führen.[73] Insbesondere die frühzeitige Einbindung der Rechtsberater[74] und eine intensive Partizipation technischer Berater könnte dazu beitragen, auf der Grundlage kritischer Beratung Erfahrungswerte zu erzeugen, um entsprechende Maßnahmen zu etablieren. Zwar kann argumentiert werden, dass hierdurch an technologisch hochentwickelte Staaten ein ungleich höherer Standard gestellt wird als an technologisch weniger entwickelte Staaten. Würde dies jedoch nicht gefordert, könnten die Entwicklungen in der Mensch-Maschine-Interaktion dazu führen, dass in technologisch hochentwickelten Staaten überhaupt keine menschliche Verantwortlichkeit mehr begründet werden kann.

Sophie Scheidt (M.A.) hat Rechtswissenschaften an der Universität Hamburg studiert und einen Mastertitel im Bereich Internationale Friedens- und Sicherheitspolitik. Sie war Legal Advisor beim European Center for Constitutional and Human Rights und arbeitet seit 2015 im Geschäftsbereich des Bundesverteidigungsministeriums. Derzeit ist sie Referentin am German Institute for Defence and Strategic Studies (GIDS) an der Führungsakademie der Bundeswehr in Hamburg.

66 *Margulies*, The Other Side of Autonomous Weapons, S. 36.
67 *Trapp*, Great Resources Mean Great Responsibility: A Framework of Analysis for Assessing Compliance with API Obligation in the Information Age, in: Saxon (Hrsg.), International Humanitarian Law and the Changing Technology of War, Boston, Leiden 2016 (zit.: *Trapp*, Great Resources Mean Great Responsibility), S. 157 ff.
68 *Oeter*, Comment: Is the Principle of Distinction Outdated, S. 54.
69 *Schmitt*, Asymmetrical Warfare and International Humanitarian Law, in: Saxon (Hrsg.), International Humanitarian Law Facing New Challenges, Berlin, Heidelberg 2007, S. 22.
70 *Turns*, Cyber War and the Concept of „Attack", in: Saxon (Hrsg.), International Humanitarian Law and the Changing Technology of War, Leiden, Boston 2013, S. 219.
71 Ausführlich siehe: *Margulies*, The Other Side of Autonomous Weapons; Zu der Methodik KI-basierter Technologie und dem Element der Vorhersehbarkeit siehe insbesondere *Schuller*, At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law, *Harvard National Security Journal* Vol. 8 No. 2, 30 May 2017, S. 379–425, auch *Ekelhof*, Lifting the Fog of Targeting.
72 Ausführlich zu *Automation Complacency* und *Automation Bias* siehe etwa *Parasuraman/Manzey*, Complacency and Bias in Human Use of Automation: an Attention Integration, https://depositonce.tu-berlin.de/handle/11303/8923 (Zugriff 12.02.2020).
73 *Trapp*, Great Resources Mean Great Responsibility, S. 167.
74 *Stewart*, Maximising Compliance with IHL, S. 180.

Juristische, politische und ethische Dimensionen der Aufarbeitung des Völkermords an den Herero und Nama*

Julia Böcker

English Title: Legal, Political and Ethical Dimensions in Dealing with the Genocide of the Herero and Nama

Abstract: Germany struggles to deal with its past colonial atrocities. From 1904 to 1908, the Empire has committed the first genocide of the 20th century in Africa; descendants of Herero and Nama in Namibia bear the consequences until today. Why full responsibility is still missing: the interdisciplinary approach identifies legal, political and ethical dimensions. The essential point is to recommend a political apology. If victim communities are included, this can be a powerful transitional justice tool even if the violence dates long back. With the return of art and human remains and with a remembrance culture, more instruments of conflict transformation are introduced.

Keywords: Dealing with the past, Namibia, colonialism, political apology, Transitional Justice
Stichworte: Aufarbeitung, Namibia, Kolonialismus, politische Entschuldigung, Transitional Justice

1. Einführung

„Wenden Sie nicht allzu viel Humanität gegen blutrünstige Bestien in Menschengestalt an!“[1], hieß es 1904 im Deutschen Reichstag zum Krieg gegen die indigenen Herero und Nama in der Kolonie Deutsch-Südwestafrika. Über 100 Jahre später kam die an sich bahnbrechende Einordnung als Völkermord nur verhalten zustande.[2] Schwierige Fragen des historischen Erinnerns, juristischen Einordnens, politischen Umgangs belasten eine Aufarbeitung.

Eigentlich hat sich Deutschland seiner schwierigen Geschichte vielfach gestellt.[3] Solche Schritte, die demokratisch orientierte, den Menschenrechten verpflichtete Gesellschaften anstreben, um mit einer gewaltbelasteten Vergangenheit umzugehen, bezogen sich zunächst auf die juristische, politische und gesellschaftliche Aufarbeitung des Nationalsozialismus als Grundlage für den Frieden in Europa. Unsere Gegenwart bestimmen Fragen des globalisierten Miteinanders. Deshalb rückt die brutale Kolonialgeschichte, die bereits jahrhundertelang Nord und Süd in Beziehung gesetzt hat, spätestens jetzt ebenfalls auf die Agenda.[4]

Die kritische Aufarbeitung der Kolonialgeschichte ist ein Regierungsziel.[5] Medienbeiträge, Ausstellungen, Kunst und Satire deuten ein koloniales Erwachen an.[6] Doch während Deutschland erst beginnt, sich dieser Vergangenheit bewusst zu werden, leiden die die Opfernachkommen in Namibia bis heute.. Dies zeigt vor allem die Landverteilung. Eine unmittelbare Folge der kolonialen Besatzung ist, dass bis heute 70 Prozent des Grundbesitzes in der Hand von deutschstämmigen oder ausländischen Eigentümern sind, die fünf Prozent der Bevölkerung ausmachen.[7] Ein kolonialapologetisches Bild, das den europäischen Besatzern eine positive zivilisatorische Wirkung zuschreibt, ist aus diesem Grund nicht angemessen.[8] Hoffnung versprechen begonnene deutsch-namibische Gespräche.

Um dafür eine Politikempfehlung abgeben zu können, umfasst die interdisziplinäre Agenda hier eine historische Einführung; eine (völker-)rechtliche Prüfung und eine Analyse des politischen Umgangs. Darauf aufbauend wird über eine politische Entschuldigung nachgedacht. Analysiert werden damit Prozesse und Praktiken der *Transitional Justice*: juristische und (gesellschafts-)politische Instrumente der Konflikttransformation.[9]

2. Historischer Hintergrund: Völkermord in der Kolonie

„The Germans wanted land from Samuel Maharero. Maharero took a tin and gave them soil and he said: there is the soil you asked for.“[10] Die Überlieferung stellt das souveräne Handeln der Herero („Viehzüchter“) gegenüber den Deutschen heraus. Deren Ziel einer „weißen“ Siedlerkolonie, gegründet am 24. April 1884, sollte international Prestige sichern.[11] Zuwanderer eigneten sich Boden und Vieh durch zwielichtige Verträge, skrupellose Kredite oder Raub an. Dass die (halb-)nomadischen

* Dieser Beitrag basiert auf einer hoch geschätzten Masterarbeit aus dem Studiengang „Peace and Security Studies“ an der Universität Hamburg. Die Autorin bedankt sich bei ihrer Erstgutachterin Dr. Veronika Bock sowie bei ihrer Zweitgutachterin Prof. Dr. Anna Geis für die wertvollen Ratschläge. Ein weiterer Dank geht an das Redaktionsteam für seine Unterstützung.

1 Stenographische Reichstagsberichte, XI. Legislaturperiode, LX. Sitzung, Bd. 199, 1903/05, S. 1900/C, Ludwig zu Reventlow, 17.03.1904. Der Diskurs war von solchen pejorativen, rassistischen Fremdzuschreibungen („Hottentotten“) und euphemistischen Eigennamen („Schutzgebiet“) bestimmt.

2 Martin Schäfer (Auswärtiges Amt), Regierungspressekonferenz, Berlin, 10.07.2015.

3 Vgl. Christopher Daase/Stefan Engert/Judith Renner: Guilt, Apology and Reconciliation in International Relations, in: Christopher Daase/Stefan Engert (Hrsg.): Apology and Reconciliation in International Relations: The Importance of Being Sorry, London/New York 2016, S. 1-28, hier S. 15.

4 Hans Dieter Heimendahl: Wir brauchen eine neue Erinnerungskultur, Deutschlandfunk Kultur, 31.01.2019.

5 Siehe Koalitionsvertrag für die 19. Legislaturperiode des Bundestags vom 12.03.2018, S. 154, S. 169.

6 Z.B. Birte Schneider/Oliver Welke: Genozid – Reine Ansichtssache“, in: ZDF Heute Show vom 03.06.2016 und Jan Böhmermann: Neo Magazin Royale in ZDF Neo vom 14.11.2019 als Satirebeiträge und „Hereroland. Eine deutsch-namibische Geschichte“. Thalia Theater Hamburg, Uraufführung am 19.01.2020 als Theaterbeitrag.

7 Quelle: Namibia Statistics Agency, Namibia Land Statistics Booklet, 2018, S. 44.

8 So der Afrikabeauftragte der Bundeskanzlerin Günter Nooke (CDU) im Interview: „Wir haben lange Zeit zu viel im Hilfsmodus gedacht“, in: Berliner Zeitung vom 06.10.2018. Kritik übte Jürgen Zimmerer: „Afrika-Beauftragter nicht mehr tragbar!“ Interview im Westdeutschen Rundfunk am 09.10.2018.

9 Vgl. Stefan Engert/Anja Jetschke: Transitional Justice 2.0 – Zur konzeptionellen Erweiterung eines noch jungen Forschungsprogramms, in: Die Friedens-Warte 86/1-2 (2011), S. 15-43, hier S. 15f.

10 Karla Poewe: The Namibian Herero: A History of their Psychosocial Disintegration and Survival, Lewiston 1985, S. 69 Fn. 17.

11 Allgemein: Deutsches Historisches Museum (Hrsg.): Deutscher Kolonialismus: Fragmente seiner Geschichte und Gegenwart. Darmstadt 2016, S. 16ff.

DOI: 10.5771/0175-274X-2019-4-50

Bevölkerungsgruppen politisch entmachtet, wirtschaftlich enteignet, ihre Gesellschaft empfindlich gestört wurde, war die eigentliche Kriegsursache.[12]

Am 12. Januar 1904 überfielen Herero Farmen und töteten mehr als 100 Deutsche. Auf beiden Seiten war das Ziel anfangs ein begrenzter Krieg – bis Weichenstellungen zur völligen Eskalation erfolgten. Siedler und Truppen verübten blutige Feldzüge – eine „Brutalisierung von unten"[13]. Der ortsfremde Generalstab übernahm die militärische Gesamtleitung, General Lothar von Trotha den Oberbefehl. Er erklärte *de iure* den Kriegszustand: „Ich vernichte aufständische Stämme mit Strömen von Blut und Strömen von Geld."[14]

Im Drängen auf eine Entscheidungsschlacht wurde der Waterberg, wo sich 60.000 Herero – Männer, Frauen und Kinder – versammelt hatten, umstellt und am 11./12. August 1904 angegriffen. „Wem gehört Hereroland? Uns gehört Hereroland!"[15] – so die überlieferten Gesänge der Herero-Frauen. Über eine militärische Niederlage hinaus wurde ihre Gruppe in die Wüste verfolgt. Das Generalstabswerk: „Die wasserlose Omaheke sollte vollenden, was die deutschen Waffen begonnen hatten."[16] Am 2. Oktober 1904 erließ von Trotha einen Aufruf, der alle Herero mit dem Tod bedrohte.[17] Auch gegen die Nama gingen die Deutschen rigide vor. Mehr Menschen starben zu dieser Zeit durch Durst und Erschöpfung als zuvor in den Gefechten.

Mit Hilfe der Mission wurden bis 1907 etwa 20.000 Kriegsgefangene in „Konzentrationslager" eingeliefert.[18] Katastrophale hygienische Bedingungen, Unterernährung, überschwere Zwangsarbeit und Misshandlungen führten zu einer hohen Todesrate. Erst als deutsche Siedler über Arbeitskräftemangel klagten, wurde 1908 die Internierung aufgehoben.[19] Bis 1914 übten die Deutschen rigide Kontrolle aus.

Die ungleiche Landverteilung, die Demografie und politische Mehrheitsverhältnisse, die wirtschaftliche Ungleichverteilung und nicht zuletzt die Symbolkraft verschiedener nationaler Erinnerungen zeigen:[20] Die Kriegsfolgen sind bis heute eine „strukturelle, materielle und sozialpsychologische Erblast"[21] in Namibia.

3. Zur rechtlichen Aufarbeitung – die Kategorie Völkermord

Die *Convention on the Prevention and Punishment of the Crime of Genocide* (CPPCG) der Vereinten Nationen (UN) beschreibt den völkerrechtlichen Straftatbestand (Art. 2).[22] Der Gesetzentwurf geht auf den polnisch-jüdischen Juristen Raphael Lemkin zurück, der für die nationalsozialistischen Verbrechen – „a crime without a name"[23] – aus dem altgriechischen γένος (Rasse, Volk) und dem lateinischen caedere (töten) einen Namen schuf.

Als geschützte Gruppen gibt das Vertragswerk nationale, rassische, ethnische oder religiöse Entitäten an. Insbesondere bestimmten die Täter den Status der einzelnen Opfer und schreiben ihnen Andersartigkeit zu.[24] Die stabilen Herero- und Nama-Gruppen fallen darunter.

Ihre Zerstörung erfolgte durch die Verfolgung, wo Erschöpfung und Verdursten zum Tod der Menschen führte. Andere wurden von Soldaten erschossen oder erhängt. Auch die Lagerbedingungen führten zum Tod oder richteten körperlichen und seelischen Schaden an. Selbst nach vorsichtigsten Schätzungen kam insgesamt mindestens ein Drittel der Bevölkerungen um.[25]

Doch gilt: „The fundamental question is not how many victims were actually killed or injured, but rather how many victims the perpetrator intended to attack."[26] Den Handelnden musste das Ziel der Zerstörung vor Augen stehen.[27] Die rassistisch imprägnierten Gewalt- und Vernichtungsfantasien wurden explizit in den Proklamationen angekündigt.

Als großes *Caveat* wird allerdings einschlägig angeführt, dass die Kategorie Genozid erst 1948 rechtlich normiert wurde und es daher zweifelhaft ist, ob der Genozidtatbestand bis in die Kolonialzeit zurück angewandt werden kann. Einen Ausweg kann die Genozidforschung bieten, auch wenn diese nicht von dem Grundsatz der Intertemporalität des Völkerrechts entbindet. Völkermord wird in der Genozidforschung als staatlich verant-

12 Von „Erosion" spricht Jürgen Zimmerer: Deutsche Herrschaft über Afrikaner: Staatlicher Machtanspruch und Wirklichkeit im kolonialen Namibia., 2. Aufl., Berlin 2002, S. 27. Vgl. auch Gesine Krüger: Kriegsbewältigung und Geschichtsbewusstsein: Realität, Deutung und Verarbeitung des deutschen Kolonialkriegs in Namibia 1904-1907, Göttingen 1999, S. 44, S. 55.

13 Matthias Häußler/Trutz v. Trotha: Brutalisierung von ‚unten'. Kleiner Krieg, Entgrenzung der Gewalt und Genozid im kolonialen Deutsch-Südwestafrika, in: Mittelweg 36 21/3 (2012), S. 57-89, hier S. 57.

14 Lothar von Trotha, 05.11.1904, zit. n. Horst Drechsler: Aufstände in Südwestafrika: Der Kampf der Herero und Nama 1904 bis 1907 gegen die deutsche Kolonialherrschaft, Berlin 1984, S. 180.

15 Überliefert durch den Pfarrer Wilhelm Anz: Gerechtigkeit für die Deutschen in Südwestafrika!, in: Die christliche Welt, 18 (28), 07.14.1904, S. 657; vgl. auch Dag Henrichsen: „Ehi rOvaherero". Mündliche Überlieferungen von Herero zu ihrer Geschichte im vorkolonialen Namibia, in: WerkStatt Geschichte 9 (1994), S. 15-24, hier S. 15.

16 Preußen Großer Generalstab: Die Kämpfe der deutschen Truppen in Südwestafrika, Bd. 1: Der Feldzug gegen die Herero, Berlin 1906-1908, S. 207.

17 Aufruf von Trothas, zit. n. Michael Behnen (Hrsg.): Quellen zur deutschen Außenpolitik im Zeitalter des Imperialismus: 1890-1911, Darmstadt 1977, S. 291ff. Abschriften wurden auch auf Otjiherero, d.h. in der Sprache der Herero, verbreitet.

18 Erstmals von spanischen Kolonialbehörden verwendet ist der Begriff heute anders geprägt; vgl. Joël Kotek/Pierre Rigoulot: Das Jahrhundert der Lager: Gefangenschaft, Zwangsarbeit, Vernichtung, Berlin 2001, S. 27f. Als Missionar berichtete Heinrich Vedder: Kurze Geschichten aus einem langen Leben, Wuppertal-Barmen 1953, S. 153.

19 Vgl. Jon Bridgman/Leslie J. Worley: Genocide of the Hereros, in: Samuel Totten u.a. (Hrsg.): Century of Genocide: Eyewitness Accounts and Critical Views, New York 2004, S. 15-52, hier S. 37f.

20 Daten bei Namibia Statistics Agency, Namibia Land Statistics Booklet, 2018 und im Human Development Report des Entwicklungsprogramms der Vereinten Nationen (UNDP), 2017/18.

21 Vgl. Reinhart Kößler/Henning Melber: Völkermord – und was dann? Die Politik deutsch-namibischer Vergangenheitsbearbeitung, Frankfurt a. M. 2017, S. 12, S. 45.

22 UN-Generalversammlung, Resolution 260 A (III) vom 09.12.1948, Inkrafttreten am 12.01.1951. Vgl. Birthe Kundrus/Henning Strotbek: „Genozid". Grenzen und Möglichkeiten eines Forschungsbegriffs – ein Literaturbericht, in: Neue Politische Literatur 51/1 (2006), S. 397-423, hier S. 402.

23 Raphael Lemkin: Genocide, in: American Scholar 15 (1946), S. 227-230, hier S. 227. Vgl. auch Dominik J. Schaller: Genozidforschung: Begriffe und Debatten, in: Ders. u.a. (Hrsg.): Enteignet – vertrieben – ermordet. Beiträge zur Genozidforschung, Zürich 2004, S. 9-26, hier S. 11.

24 Vgl. Joe Verhoeven: Le Crime de Génocide. Originalité et Ambiguïté, in: Revue Belge de Droit International 1 (1991), S. 5-26, hier S. 21.

25 Vgl. Susanne Kuß: Deutsches Militär auf kolonialen Kriegsschauplätzen: Eskalation von Gewalt zu Beginn des 20. Jahrhunderts, 2. Aufl., Berlin 2004, S. 86.

26 William A. Schabas: The Law and Genocide, in: Donald Bloxham/Dirk A. Moses (Hrsg.): The Oxford Handbook of Genocide Studies, Oxford/New York 2010, S. 123-141, hier S. 136.

27 Zur Absicht William Schabas/Holger Fliessbach: Genozid im Völkerrecht, Hamburg 2003, S. 27 und John Quigley: Intent Without Intent, in: Adam Jones (Hrsg.): Genocide in Theory and Law, London 2008, S. 86-94, hier S. 86ff.

wortete Serie von Angriffen, die über die militärische Niederlage hinaus ein Opferkollektiv zu vernichten sucht, verstanden.[28] Der Begriff gilt wie beim Holocaust „im Sinne einer historischen Analysekategorie“[29] auch für den Herero-Nama Fall als anwendbar.

Fragen zur juristischen Bewertung stellten sich konkret dadurch, dass seit 1999 eine Herero-Vertretung vor verschiedenen Gerichten Klage erhebt.[30] Vor dem Internationalen Gerichtshof in Den Haag, wo der erste Versuch erfolgte, sind allerdings nur Staaten klageberechtigt.[31] Unter Berufung auf das *Alien Tort Statute* aus dem Jahr 1789[32] wurden mehrere Verfahren vor Gerichten in den USA angestrengt, doch stehen Staatenimmunität, Verjährung und Zuständigkeiten entgegen. Andere Haftungsgründe wie die Genfer Konventionen greifen nicht, Indigene waren davon ausschlossen. Die Taten wurden für nicht mehr justiziabel erklärt.[33]

Damit kommen Zweifel auf, dass Völkerrecht überhaupt koloniales Unrecht aufarbeiten kann. Das heutige Rechts- und Moralempfinden würde zwar aufgrund von Billigkeit und Ausgleich bevorzugen, den Hinterbliebenen klagbare Ansprüche zuzuerkennen. Doch schloss die damalige Rechtsordnung die Indigenen gerade aus dem den europäischen Mächten vorbehaltenen Regelkanon aus und kann deshalb keine Grundlage sein, ihnen Gerechtigkeit zuteil werden zu lassen. Ungeachtet lässt der juristische Befund, wie schwer die moralische Schuld wiegt.[34]

4. Ansätze politischer Aufarbeitung

Auch über das Ende der deutschen Kolonialzeit hinaus dienten die Kolonien als Projektionsraum; sie rückten erst in den beiden deutschen Teilstaaten in den Hintergrund. Die sich 1989 anbahnende Unabhängigkeit Namibias brachte das Thema zurück in den Bundestag, der einen Beschluss zur Zusammenarbeit mit Namibia fasste.[35] Doch blieb die koloniale Gewalt als Anstoß zur Wiedergutmachung unerwähnt. Beim ersten und bislang einzigen Besuch eines deutschen Regierungschefs in Namibia wurden von Helmut Kohl (CDU) 1995 mehrere hundert deutschsprachige, weiße Namibier, aber keine Herero empfangen.[36]

Um mögliche Zahlungen zu vermeiden, wurde jedes Schuldeingeständnis vermieden. Außenminister Joschka Fischer (Die Grünen) fasste dies 2003 folgendermaßen:

> „Wir sind uns unserer geschichtlichen Verantwortung in jeder Hinsicht bewusst, sind aber auch keine Geiseln der Geschichte. Deshalb wird es eine entschädigungsrelevante Entschuldigung nicht geben.“[37]

Zu diesem Ansatz gehörte lange, die Rolle Deutschlands als entwicklungspolitischem Geldgeber Namibias zu unterstreichen. Tatsächlich floss seit 1990 rund eine Milliarde Euro. Problematisch ist daran, dass die Verfügungsgewalt nicht den Opfern zugebilligt wird, die zudem in der Minderheit sind.[38] Ein zusätzliches Dilemma ist, ob Deutschland die namibische Landreform unterstützen soll. Mit dem Programm sollen zum Wohl des Tourismus Enteignungen vermieden werden; doch profitieren davon die ohnehin privilegierten Weißen.[39]

Blieb die offizielle deutsche Politik auch für weitere Jahre unverändert, kam dem Thema durch die Klagen und Impulse aus beiden Zivilgesellschaften mehr Aufmerksamkeit zu. Bei der Gedenkfeier am Waterberg am 12. August 2004 brach zumindest Bundesentwicklungsministerin Heidemarie Wieczorek-Zeul (SPD) das begriffliche Tabu: „Die damaligen Gräueltaten waren das, was man heute als Völkermord bezeichnen würde.“[40] Man beachte die peinlich genaue Betonung der Intertemporalität.

Der fehlende offizielle Wandel führte zu peinlichen Wechselwirkungen.[41] 2015/16 wurden die Massaker an den Armeniern, die sich zum 100. Mal jährten, diskutiert; zugleich mussten die europäischen Länder ausgerechnet mit dem Land, in dem die Leugnung dieses Völkermords offizielle Politik ist, ein Flüchtlingsabkommen erzielen.[42] Als der Bundestag den Armeniergenozid anerkannte, sprach der türkische Präsident Recep Tayyip Erdoğan prompt Deutschland angesichts der Verbrechen in Namibia jegliches Urteilsrecht über die Türkei ab.[43]

Dabei war die Sprachregelung bereits 2015 in einer Bundespressekonferenz korrigiert worden. Doch geschah die Anerkennung der kolonialen Gewalt als Kriegsverbrechen und Völkermord derart indirekt und informell, dass sich die Journalisten erst vergewissern

28 Vgl. Helen Fein: Definition and Discontent. Labelling, Detecting and Explaining Genocide in the Twentieth Century, in: Stig Förster/Gerhard Hirschfeld (Hrsg.): Genozid in der modernen Geschichte, Berlin u.a. 1999, S. 11-21, hier S. 18.

29 Jürgen Zimmerer: Krieg, KZ und Völkermord in Südwestafrika, in: Ders./Joachim Zeller (Hrsg.): Völkermord in Deutsch-Südwestafrika: Der Kolonialkrieg (1904-1908) in Namibia und seine Folgen, 3. Aufl., Bonn 2016, S. 45-63, hier S. 53.

30 Vgl. Sydney L. Harring: The Herero Demand for Reparations from Germany, in: Max du Plessis/Stephen Peté (Hrsg.): Repairing the Past? International Perspectives on Reparations for Gross Human Rights Abuses, Antwerpen 2007, S. 437-450, hier S. 437ff. und Jeremy Sarkin: Germany's Genocide of the Herero: Kaiser Wilhelm II, his General, his Settlers, his Soldiers, Cape Town, South Africa u.a. 2010, S. 55.

31 Vgl. Janntje Böhlke-Itzen: Kolonialschuld und Entschädigung. Der deutsche Völkermord an den Herero 1904-1907, Frankfurt a. M. 2004, S. 31 und Steffen Eicker: Der Deutsch-Herero-Krieg und das Völkerrecht, Frankfurt a. M./New York 2009, S. 83f.

32 Vgl. Daniel Felz: Das Alien Tort Statute: Rechtsprechung, dogmatische Entwicklung und deutsche Interessen, Berlin 2017, S. 29ff.

33 Vgl. Felicia Jaspert: Setback for the Descendants of the Nama and Ovaherero Indigenous Peoples. A New York Court Declines Jurisdiction in Rukoro et al. v. Germany, in: Völkerrechtsblog, 08.05.2019.

34 Vgl. Jörn Axel Kämmerer/Jörn Föh: Das Völkerrecht als Instrument der Wiedergutmachung? Eine kritische Betrachtung am Beispiel des Herero-Aufstandes, in: Archiv des Völkerrechts 42/3 (2004), S. 294-328, hier S. 325f.; Manfred O. Hinz: Der Krieg gegen die Herero: Friedensschluss hundert Jahre danach. In: Norman Paech (Hrsg.): Völkerrecht statt Machtpolitik, Hamburg 2004, S. 148-171, hier S. 163 sowie Patrick Heinemann: Die deutschen Genozide an den Herero und Nama: Grenzen der rechtlichen Aufarbeitung, in: Der Staat 55 (2016), S. 461-487, hier S. 483.

35 Vgl. Ulrich Roos/Timo Seidl: Im „Südwesten“ nichts Neues? Eine Analyse der deutschen Namibiapolitik als Beitrag zur Rekonstruktion der außenpolitischen Identität des deutschen Nationalstaates, in: Zeitschrift für Friedens- und Konfliktforschung 4/2 (2015), S. 182-224, hier S. 193.

36 Kohl sprach die Gäste mit „Liebe Landsleute“ an, so als Augenzeuge Henning Melber: „Wir haben überhaupt nicht über Reparationen gesprochen“. Die namibisch-deutschen Beziehungen: Verdrängung oder Versöhnung?, in: Jürgen Zimmerer/Joachim Zeller (Hrsg.): Völkermord in Deutsch-Südwestafrika: Der Kolonialkrieg (1904-1908) in Namibia und seine Folgen, 3. Aufl., Bonn 2016, S. 215-225, hier S. 220f.

37 „Wir sind jetzt am Maximum“, in: Allgemeine Zeitung (Namibia) vom 30.10.2003.

38 Vgl. Jürgen Zimmerer: Entschädigung für Herero und Nama, in: Blätter für deutsche und internationale Politik 6 (2005), S. 658-660, hier S. 658.

39 Vgl. Leonard Jamfa: Germany Faces Colonial History in Namibia: A Very Ambiguous „I Am Sorry“, in: Mark Gibney u.a. (Hrsg.): The Age of Apology: Facing Up to the Past, Philadelphia 2008, S. 202-215, hier S. 213.

40 Rede von Bundesministerin Heidemarie Wieczorek-Zeul, Okakarara, Namibia, 14.08.2004; vgl. Dies.: Welt bewegen: Erfahrungen und Begegnungen. Berlin 2007, S. 48ff.

41 Lammert fordert Bekenntnis zu „deutschem Völkermord an Herero“, in: Tagesspiegel vom 13.06.2016, S. 4.

42 Zu der Situation Joachim Riecker: Ja, Völkermord, in: Die Zeit vom 01.06.2016, online.

43 Siehe: Look at your own genocide history, President Erdogan tells Germany, in: Daily Sabah, 05.06.2016.

mussten: „das wäre ja jetzt eine Meldung“ – „dann melden Sie es.“[44] Frank-Walter Steinmeier (SPD), heute Bundespräsident, war zu der Zeit Außenminister. Er initiierte im gleichen Jahr Gespräche mit Namibia über die gemeinsame Vergangenheit.

Bei den bisher acht Treffen im Wechsel zwischen Berlin und Windhoek gehörten der namibischen Delegation auch Herero- und Nama-Vertreter an. Beobachter sehen in dem Dilemma um die Bestimmung der Gesprächspartner das größte Problem.[45] Der deutsche Sondergesandte Ruprecht Polenz lehnt eine Einmischung in diese Frage – insbesondere als ehemalige Kolonialmacht – ab; er versucht gleichwohl, vielerorts für Akzeptanz zu werben. Das Ziel sei *kein* rechtsförmiges Schuldanerkenntnis, sondern ein politisch-moralisches Bekenntnis: Man wolle „das, was man tun kann, tun, um noch vorhandene Wunden zu heilen.“ [46]

5. Ein ethisch-moralischer Ansatz: der Weg der Entschuldigung

Mit dem deutsch-namibischen Dialog wird die Aufarbeitung nicht mehr defensiv als eine legale Frage, sondern an der Schnittstelle von Politik und Ethik behandelt. Der Einsatz von Wahrheitskommissionen und Tribunalen sind mangels Zeugen und direkt Betroffener nach so langer Zeit nicht mehr möglich; Reparationen in einem Rechtssinn ausgeschlossen.[47] Eine große historische, psychologische und sogar religiöse Bedeutung wird politischen Entschuldigungen beigemessen.[48] Bei dem dyadischen Sprechakt *gesteht* ein Täter ein schad- und schuldhaftes Verhalten ein, bestätigt seine *Verantwortlichkeit* und äußert tiefes *Bedauern*; eine *Kompensation* wird angeboten und die *Nichtwiederholung* zugesichert.[49]

Im namibischen-deutschen Fall deutete erstmals die Rede von Bundesministerin Wieczorek-Zeul 2004 in diese Richtung. Weitere Entschuldigungen brachten 2007 entfernte Verwandte von Trothas und 2017 die Evangelische Kirche, die durch Missionare am Krieg beteiligt war, vor. Bei einer Zeremonie zur Rückgabe menschlicher Gebeine bat Staatsministerin Claudia Pieper (FDP) 2011 um *Versöhnung*, nicht aber um *Entschuldigung* und wurde dafür abgestraft.[50] 2015 erfolgte die Initiative des damaligen Außenministers Steinmeier, Gespräche mit Namibia anzustoßen, ohne dass er eine Entschuldigung vorbrachte. Schon weiter gingen 2018 der Hamburger Kultursenator Carsten Brosda (SPD) und der Berliner Justizsenator Dirk Behrendt (Die Grünen), die anlässlich einer Tagung bzw. einer Restitutionszeremonie Herero- und Nama-Vertreter empfingen und diese für die große Beteiligung ihrer Städte an dem Leid ihrer Vorfahren um Vergebung baten. Doch ist eine Entschuldigung erst bedeutsam, wenn der Sprecher den Staat angemessen vertreten kann.[51]

Als Meilenstein auf dem Weg der Aufarbeitung deutscher kolonialer Schuld wurde die Rede von Staatsministerin Michelle Müntefering (SPD) bei einer weiteren Restitutionszeremonie 2018 wahrgenommen. Nicht zufällig beschrieb sie mit Worten eine Demutsgeste:

> „Ich verbeuge mich in tiefer Trauer. Das schreckliche Unrecht, das unsere Vorfahren begangen haben, kann ich nicht rückgängig machen. Doch bitte ich Sie aus tiefstem Herzen um Verzeihung.“[52]

Viele Herero und Nama warten allerdings noch darauf, dass ein höchster Repräsentant der Bundesrepublik Deutschland derart Stellung bezieht.

Eine historische Zeitenwende im politischen Umgang mit der Erblast kolonialer Vergangenheit zeichnet sich in den Worten des deutschen Sondergesandten für die deutsch-namibischen Gespräche Ruprecht Polenz ab. Im Interview mit der Autorin gab er zu Protokoll:

> „Deutschland möchte für das, was damals verbrochen wurde, um Entschuldigung bitten. Man kann sich ja nicht selbst entschuldigen, sondern man kann nur darum bitten und hoffen, dass die andere Seite das annimmt.“[53]

Für eine *Benennung* der Taten wurde dort bereits eine gemeinsame Erklärung erarbeitet. Daraus müsste auch die *Verantwortlichkeit* des Deutschen Reiches hervorgehen. Man wolle den Nachfahren vermitteln, dass einem die Verbrechen heute leid tun. Das bringt *Bedauern* zum Ausdruck; eng verbunden mit dem tatsächlichen Versuch, den Schaden wenigstens zu *mildern*: Kollektivmaßnahmen in den Bereichen Wohnraum, Energie, Berufsbildung sollen die Lebenschancen der Nachfahren verbessern. Um durch Sicherheit vor Enteignungen den Tourismus als Einnahmequelle zu erhalten, wird auch die Landreform unterstützt. Schließlich sind Bildungs- und Gedenkprojekte als Garantie für eine *Nichtwiederholung* gedacht.

Zudem müsste ein höchster Staatsrepräsentant Deutschland bei einem Entschuldigungsakt vertreten – Bundespräsident oder Bundeskanzlerin. Auch ist wichtig, die richtige Symbolsprache in beiden Kulturen zu finden. Überdies muss der Sprechakt im Land des Senders gesellschaftlich gebilligt sein. Forderungen nach einer Entschuldigung in Deutschland lassen darauf schließen, aber ob auch der Einsatz von Steuergeldern gutgeheißen wird? Um die namibische Seite bei der Annahme der Entschuldigung nicht unter Druck zu setzen, ist außerdem Geduld erforderlich.

Zugleich wächst die Sorge vor wachsenden innernamibischen Spannungen. Werden nicht alle Herero und Nama eingebunden, werden die nicht kompromissbereiten Stimmen lauter. Dann besteht die große Gefahr von Landbesetzungen und Selbstjustiz.[54]

44 Martin Schäfer (Auswärtiges Amt), Regierungspressekonferenz vom 10.07.2015.
45 Vgl. Sefan Engert: Germany – Namibia. The Belated Apology to the Herero, in: Ders./Christopher Daase (Hrsg.): Apology and Reconciliation in International Relations: The Importance of Being Sorry, London, New York 2016, S. 127-145, hier S. 139f.
46 Interview mit Ruprecht Polenz am 16.05.2019 in Münster, Transkript in der Masterarbeit der Verfasserin.
47 Vgl. Christopher Daase: Addressing Painful Memories. Apologies as a New Practice in International Relations, in: Aleida Assmann/Sebastian Conrad (Hrsg.): Memory in a Global Age. Discourses, Practices and Trajectories, Basingstoke 2010, S. 19-31, hier S. 24; vgl. auch: Stefan Engert: Politische Schuld, moralische Außenpolitik? Deutschland, Namibia und der lange Schatten der kolonialen Vergangenheit, in: Sebastian Harnisch u.a. (Hrsg.): Solidarität und internationale Gemeinschaftsbildung, Frankfurt a. M. 2009, S. 277-304, hier S. 294.
48 Siehe etwa Tom Bentley: Empires of Remorse: Narrative, Postcolonialism and Apologies for Colonial Atrocity, London/New York 2016, S. 75ff.
49 Vgl. Stefan Engert: Die Staatenwelt nach Canossa. Eine liberale Theorie politischer Entschuldigungen, in: Die Friedens-Warte 86/1-2 (2011), S. 155-189, hier S. 155ff.; Ders.: Das kollektive Gewissen. Warum Staaten sich (nicht) entschuldigen, in: Stephan Schaede/Thorsten Moos (Hrsg.): Das Gewissen, Tübingen: Mohr Siebeck, S. 511-538, hier S. 518ff. und Raymond Cohen: Apology and Reconciliation in International Relations, in: Yaacov Bar-Siman-Tov (Hrsg.): From Conflict Resolution to Reconciliation, S. 177-198, hier S. 177.
50 Rede von Staatsministerin Cornelia Pieper, Berlin, 30.09.2011.
51 Vgl. Ruben Carranza/Cristián Correa/Elena Naughton: Reparative Justice. More Than Words: Apologies as a Form of Reparation, International Center for Transitional Justice 2015, S. 13.
52 Rede von Staatsministerin Michelle Müntefering, Berlin, 29.08.2018.
53 Interview mit Ruprecht Polenz am 16.05.2019 in Münster, Transkript in der Masterarbeit der Verfasserin.
54 Siehe Jürgen Zimmerer u.a.: In großer Sorge um den Aussöhnungsprozess mit Herero und Nama: Brief an Bundeskanzlerin Angela Merkel vom 02.04.2019; als Offener Brief veröffentlicht am 10.05.2019.

Insofern drängt auch die Zeit. Die Verhandlungsergebnisse liegen gerade zur Begutachtung bei den Regierungen. Doch konnten anscheinend weder die Reise des Entwicklungshilfeministers Gerd Müller (CSU) nach Namibia am 29. August 2019 noch die Feier von 30 Jahren Unabhängigkeit Namibias am 31. März 2020 dazu einen Anstoß geben.

6. Politikempfehlung

Deutschland wird die historisch-politische Anerkennung als Völkermord und eine Bitte um Entschuldigung bei den betroffenen Gruppen empfohlen. Auf dem Weg dorthin sollten – in Absprache mit der namibischen Regierung – mit Transparenz und Partizipation die entscheidenden Faktoren genutzt werden, um weitere Dialogmöglichkeiten für die verschiedenen Opfergruppen und die Zivilgesellschaft zu schaffen, z.B. durch die Kirchen beider Länder.

Angesichts gegenwärtiger Fragen, von denen viele – über Migrationsfragen weit hinaus – im kolonialen Erbe wurzeln, muss sich Deutschland in seiner Afrikapolitik positionieren.

Unter den Prozessen und Praktiken, die den Übergang von Gewalt zu Frieden unterstützen, heben sich Entschuldigungen ab von retributiven (Strafverfolgungs-)Verfahren, die auch auf Strafe bzw. Vergeltung abzielen. Mit ihrem Gegenwartsbezug und ihrem Zukunftsanspruch gehören Entschuldigungen zur *Transitional*, ja *Restorative Justice*, welche die Beziehungen neu ausrichtet.[55] Deutschland würde damit Namibia als gleichberechtigten Partner anerkennen.[56]

Im Völkerrecht werden Entschuldigungen als Wiedergutmachung angesehen.[57] Dies unterstreicht den Stellenwert des Sprechakts als diplomatischer Konvention. Der Staat kann damit einer Eskalation vorbeugen und Verhandlungen einleiten. Der vorliegende Fall hat gezeigt: Staaten befürchten, dass eine Entschuldigung als Grundlage für Reparationsforderungen ausgelegt wird. Dabei kann diese im Gegenteil einen juristischen Weg ersetzen.[58] Ein internationaler Standard von Entschuldigungen könnte das Dilemma auflösen.

Nach der Ankündigung der Restitution afrikanischer Kunst des französischen Präsidenten Emmanuel Macron wäre eine formale Entschuldigung von höchster Stelle gerade kein Tabubruch mehr in der westlichen Staatenwelt.[59] Bestenfalls kommt damit einem kritischen Umgang mit der Geschichte ein Platz in einem deutschen wie in einem selbstreflektierten europäischen Bewusstsein zu. Die Aufarbeitung der eigenen, gewaltbelasteten Vergangenheit enthält dann auch eine Aussage über die Geltung von Menschenrechtsstandards heute.

Wir sind außerdem in einem Wandel in eine heterogene, multiethnische Gesellschaft begriffen. Menschen, die aus Afrika zuziehen, haben möglicherweise Folgen des Kolonialismus von der anderen Seite erfahren.[60] Daraus ergibt sich die politische und gesellschaftliche Aufgabe, alte Muster von Macht und Überlegenheit aufzubrechen. Dafür lässt sich aus der Geschichte viel lernen.

Erinnerungspolitisch sind Straßenumbenennungen wichtige Korrektive.[61] Einer historischen Bewusstseinsbildung nützt, wenn Anwohner, die Black Community und afrikanische Vertreter in die Entscheidungen eingebunden werden. Dies gilt erst recht für das Desiderat einer zentralen Gedenkstätte als Erinnerungsort.[62] Zur Rückführung von Gebeinen muss die Provenienzforschung individuelle Identitäten bzw. ethnische Zugehörigkeiten verifizieren. Für die indigenen Gemeinschaften bringt Klarheit über die Herkunft einzelner Totenschädel mehr als viele anonyme Überreste.[63] Außerdem braucht es Lösungen für Objekte in Privatbesitz.[64] Restitutionsprozesse, auch von kolonialem Kulturgut, können in beiden Ländern notwendige Erinnerungsdiskurse anstoßen. Für eine transnationale Annäherung liegen in Museen, Kunst und Wissenschaften große Hoffnungen.[65] Die Wissenschaft sollte die Perspektiven der verschiedenen Herero- und Nama-Gruppierungen näher in den Blick nehmen. Die hier angesprochenen Fragen stellen sich dem Einzelfall übergeordnet im Zuge transformativer Vergangenheitsaufarbeitung und postkolonialer Kommunikation. Kamerun, von 1884 bis 1919 unter teils brutaler deutscher Herrschaft, wäre das nächste Land im Fokus einer Wiedergutmachung.[66]

Julia Böcker, M.A., M.P.S., ist Historikerin, Mediatorin und Friedensforscherin. Sie ist am Zentrum für ethische Bildung in den Streitkräften (zebis) in Hamburg tätig. Der europäische Zweig der *International Society for Military Ethics* hat ihre Masterarbeit 2020 mit dem *EuroISME-Award for the Best Thesis in Military Ethics* ausgezeichnet.

55 Vgl. Kora Andrieu: „Sorry for the Genocide": How Public Apologies Can Help Promote National Reconciliation, in: Millennium – Journal of International Studies 38/1 (2009), S. 3-23, hier S. 5 und Martha Minow: Between Vengeance and Forgiveness: Facing History after Genocide and Mass Violence, Nachdruck, Boston 2009, S. 114.

56 Vgl. Andreas Guibeb, in: Hans Jessen: Namibia wartet, in: Politik und Kultur, 05/2019, S. 4.

57 Art. 37 Draft articles on the Responsibility of States for Internationally Wrongful Acts, vgl. UN Doc. A/56/10, 2001, S. 28.

58 Vgl. Richard Bilder: The Role of Apology in International Law and Diplomacy, in: Virginia Journal of International Law 46/3 (2006), S. 433-473, hier S. 464 und Arthur Watts: The Art of Apology, in: Maurizio Ragazzi (Hrsg.): International Responsibility Today. Essays, Leiden/Boston 2005, S. 107-116, hier S. 107f.

59 Rede von Präsident Emmanuel Macron, Burkina Faso, 28.11.2017.

60 Jürgen Zimmerer: Umbenennung ist richtiger Schritt, in: Die Tageszeitung (taz) vom 11.09.2013.

61 Vgl. Ders. (Hrsg.): Kein Platz an der Sonne: Erinnerungsorte der deutschen Kolonialgeschichte. Bonn 2013, S. 21.

62 Vgl. Reinhart Kößler: Namibia and Germany: Negotiating the Past, Windhoek 2015, S. 74.

63 Vgl. gleich mehrere Beiträge in Holger Stoecker u.a. (Hrsg.): Sammeln, Erforschen, Zurückgeben? Menschliche Gebeine aus der Kolonialzeit in akademischen und musealen Sammlungen, Berlin 2013.

64 Siehe Christoph Titz: Herr Ziegenfuß ist den Schädel los, in: Spiegel Online vom 28.08.2018.

65 Beispiele sind die Ausstellung *Ovizire. Somgu: From Where Do We Speak?*, Museum am Rothenbaum – Kulturen und Künste der Welt (MARKK) und Kunstraum M. Bassy Hamburg, 2018/2019 und die Forschungsstelle *Hamburgs (Post-)Koloniales Erbe – Hamburg und die Frühe Globalisierung* der Universität Hamburg.

66 Maria Ketzmerick: Postkoloniale Außenpolitik: Wie sich Deutschland in Kamerun engagieren sollte, in: PeaceLab-Blog des Global Public Policy Institute Berlin, 20.05.2019.

Ute Runge

1. Themenschwerpunkt – Special Focus Topic
Interdisziplinäre Beiträge zur naturwissenschaftlich-technischen Friedensforschung – Interdisciplinary Contributions to Scientific-Technical Peace Research

Bittencourt, Carla/ Ewels, Chris/ Llobet, Eduard (Hrsg.): Nanoscale Materials for Warfare Agent Detection: Nanoscience for Security, Dordrecht (Springer) 2019.

Hippel, Frank von/ Takubo, Masafumi/ Kang, Jungmin: Plutonium: How Nuclear Power's Dream Fuel Became a Nightmare, Singapore (Springer) 2019.

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

Zichichi, Antonino (Hrsg.): International Seminars on Nuclear War and Planetary Emergencies (49th Session). Science for Peace the World Over. The New Manhattan Project, Singapore (World Scientific) 2019.

2. Theorien internationaler Beziehungen – International Relations Theory

Epstein, Charlotte (Hrsg.): Against International Relations Norms. Postcolonial Perspectives, London (Routledge) 2019.

Haukkala, Hiski/ Wetering, Carina van de / Vuorelma, Johanna (Hrsg.): Trust in International Relations. Rationalist, Constructivist, and Psychological Approaches, London (Routledge) 2019.

Kocks, Alexander: Internationale Friedensmissionen und nationale Interessen. Die deutsche Unterstützung militärischer Auslandseinsätze, Baden-Baden (Nomos Verlagsgesellschaft) 2019.

Lemke, Christiane: Internationale Beziehungen. Grundkonzepte, Theorien und Problemfelder, Berlin (de Gruyter Oldenbourg) 2019.

Matthews, Elizabeth G./ Callaway, Rhonda L.: International Relations Theory. A Primer, New York (Oxford University Press) 2019.

3. Völkerrecht und internationale Organisationen – International Law and Organisations

Baber, Graeme: The United Nations System. A Synopsis, Newcastle upon Tyne (Cambridge Scholars Publishing) 2019.

Harris, Paul G. (Hrsg.): A Research Agenda for Climate Justice, Cheltenham (Edward Elgar) 2019.

Kreuder-Sonnen, Christian: Emergency Powers of International Organizations. Between Normalization and Containment, Oxford (Oxford University Press) 2019.

Loh, Wulf: Legitimität und Selbstbestimmung. Eine normative Rekonstruktion des Völkerrechts, Baden-Baden (Nomos Verlagsgesellschaft) 2019.

Shepherd, Laura J.: Gender, UN Peacebuilding, and the Politics of Space. Locating Legitimacy, New York (Oxford University Press) 2019.

4. Konflikte, Sicherheit und Militär – Conflict, Security and Armed Forces

Butcher, Charity/ Hallward, Maia Carter (Hrsg.): Understanding International Conflict Management, London (Routledge) 2019.

Gavin, Francis J.: Nuclear Weapons and American Grand Strategy, Washington, DC (Brookings Institution) 2019.

Lemay-Hebert, Nicolas (Hrsg.): Handbook on Intervention and Statebuilding, Cheltenham (Edward Elgar) 2019.

Maniscalco, Maria Luisa/ Rosato, Valeria (Hrsg.): Preventing Radicalisation and Terrorism in Europe. A Comparative Analysis of Policies, Newcastle upon Tyne (Cambridge Scholars Publishing) 2019.

Sauer, Tom/ Kustermans, Jorg/ Segaert, Barbara (Hrsg.): Non-Nuclear Peace. Beyond the Nuclear Ban Treaty, Cham (Palgrave Macmillan) 2019.

5. Europa – Europe

Casier, Tom/ DeBardeleben, Joan (Hrsg.): EU-Russia Relations in Crisis. Understanding Diverging Perceptions, London (Routledge) 2019.

Clarke, Michael/ Ramscar, Helen: Tipping Point. Britain, Brexit and Security in the 2020s, London (I.B. Tauris) 2019.

Skedsmo, Pål Wilter: Armenia and Europe: Foreign Aid and Environmental Politics in the Post-Soviet Caucasus, London (I.B. Tauris) 2019.

Szwed, Stefan: Poland, Germany and State Power in Post-Cold War Europe: Asymmetry Matters. London (Palgrave Macmillan) 2019.

Zieba, Ryszard: Poland's Foreign and Security Policy. Problems of Compatibility with the Changing International Order, Cham (Springer) 2019.

6. Globale Fragen – Global Issues

Badie, Bertrand: Humiliation in International Relations. A Pathology of Contemporary International Systems, London (Hart) 2019.

Snow, Donald M.: Cases in International Relations. Principles and Applications, Lanham, MD (Rowman & Littlefield) 2019.

Winter, Tom: Geocultural Power. China's Quest to Revive the Silk Roads for the Twenty-First Century, Chicago, IL (University of Chicago Press) 2019.

Wunderlich, Carmen: Rogue States as Norm Entrepreneurs. Black Sheep or Sheep in Wolves' Clothing?, Cham (Springer) 2019.

Zenker, Anja: International Climate Agreements under Review. The Potential of Negotiation Linkage between Climate Change and Preferential Free Trade, Wiesbaden (Springer VS) 2019.

7. Sonstiges – Miscellaneous

Brush, Kathleen: A Brief History of International Relations. The World Made Easy, New York (Lang) 2019.

Gardocki, Sylwester/ Ozarowski, Rafal/ Ulatowski, Rafal (Hrsg.): The Islamic World in International Relations, Frankfurt am Main (Lang) 2019.

Iterson Scholten, Gijsbert M. van: Visions of Peace of Professional Peace Workers. The Peaces We Build, Cham (Palgrave Macmillan) 2019.

Taylor, Charles Lewis/ Russett, Bruce M. (Hrsg.): Karl W. Deutsch: Pioneer in the Theory of International Relations, Cham (Springer) 2019.

Worth, Owen: Morbid Symptoms. The Global Rise of the Far-Right, London (ZED Books) 2019.

Werner Sonne: Leben mit der Bombe. Atomwaffen in Deutschland. Springer Fachmedien, Wiesbaden 2020 (2. Aufl.), 358 S.

Spätestens die jüngste Kontroverse um die Zukunft der Stationierung von US-Kernwaffen auf deutschem Boden, ausgelöst Anfang Mai 2020 durch den Fraktionsvorsitzenden der SPD im Deutschen Bundestag, Rolf Mützenich, hat deutlich werden lassen: Die nukleare Teilhabe Deutschlands ist auch nach mehr als 60 Jahren politisch noch immer hoch umstritten, seitdem im Jahre 1957 die Bundeswehr erstmals Trägersysteme für Atomwaffen innerhalb der NATO bereitgestellt hatte.

Die aktuelle Kontroverse entzündete sich einerseits am Zusammenbruch von wesentlichen Teilen der nuklearen Rüstungskontrolle im vergangenen Jahr, insbesondere der letztlich beiderseitigen Aufkündigung des Vertrags über die Beseitigung von landgestützten Raketen mit einer Reichweite zwischen 500 und 5.500 km seitens der USA und Russland, sowie in der nachfolgenden Diskussion um die künftige Nuklearstrategie der USA und der NATO sowie die Kernwaffendoktrin Moskaus. Die Stationierung von mutmaßlich vertragsverletzenden Raketen durch Russland sowie die unmittelbar nach Auslaufen des Vertrags erfolgte Indienststellung ebensolcher Raketen der USA, hatten dem Vertragswerk den Todesstoß verpasst und damit den Grundpfeiler nuklearer Rüstungskontrolle in Europa zum Einsturz gebracht. Die im April 2020 offensichtlich mit dem Koalitionspartner SPD nicht abgestimmte Ankündigung der deutschen Verteidigungsministerin Annegret Kramp-Karrenbauer, bei der Nachfolge für die veralteten Tornado-Flugzeuge nicht nur auf Euro-Fighter, sondern zum Zweck einer reibungslosen Zertifizierung neuer Atomwaffenträger auch auf den Ankauf amerikanischer F-18 Flugzeuge zu setzen, hat die Kontroverse deutlich zugespitzt – zwischen jenen, die nukleare Abschreckung und Teilhabe weiter für unverzichtbar halten, und jenen, die sich im Abzug aller Atomwaffen einen Sicherheitsgewinn für die Bundesrepublik ausrechnen.

Das Dickicht der Argumente für und wider die nukleare Teilhabe zu erhellen, ist eines der Motive, welche Werner Sonne, den renommierten Journalisten und sicherheitspolitisch geschulten Beobachter veranlassten, dem Wunsch nach einer aktualisierten Neuauflage seines Buches „Leben mit der Bombe“ zu entsprechen. Der Zeitpunkt der Veröffentlichung hätte kaum besser gewählt werden können. Nachdem in der sogenannten Corona-Krise die brennenden sicherheitspolitischen Fragen, darunter eben auch die Zukunft der nuklearen Rüstungskontrolle, in den Hintergrund gedrängt worden waren, bricht aktuell die Debatte mit neuer Macht hervor, nicht zuletzt, weil Entscheidungen über die Zukunft der nuklearen Teilhabe wegen der auslaufenden Lebensdauer der Bundeswehr-Tornados jetzt und nicht erst nach den nächsten Wahlen in den USA oder gar in Deutschland getroffen werden müssen.

Werner Sonne hat in erster Linie kein wissenschaftliches, aber ein quellenreiches Buch geschrieben. Viele der aufgeführten Primärquellen, vor allem aus dem politischen Raum, werden einer breiteren Leserschaft erstmals zugänglich gemacht. Der Autor macht dabei keinen Hehl aus seiner Befürwortung der weiteren nuklearen Teilhabe. Die Argumente sind jene eines scharfsinnigen journalistischen Beobachters, des profunden Kenners der politischen Diskussionskulturen der USA und Deutschlands sowie des sachkundigen Analysten der transatlantischen wie auch der deutschen und russischen sicherheitspolitischen Debatten.

Von den einst auf deutschem Boden lagernden tausenden Atomwaffen der Sowjetunion/Russlands, der USA, Frankreichs und Großbritanniens sind nur noch wenige übriggeblieben. Vermutet werden sie seit Jahren in Büchel, in der Eifel, ca. 20 amerikanische Atombomben, vorgesehen als Traglast für flugzeuggestützte Systeme. Genauere Angaben werden bis heute von den US-Streitkräften nicht gemacht, jedoch ist deren Modernisierung als Kostenpunkt im Verteidigungsetat des Pentagon seit Jahren vermerkt, die Modernisierung und Umrüstung zu intelligenten Lenkwaffen im Gange.

Werner Sonne lässt die Geschichte der Atomwaffen auf deutschem Boden Revue passieren, als Geschichten und Geschichtchen eines Zeitzeugen, gut erzählt und zudem für ein breites Publikum gut lesbar geschrieben. Mit zahlreich zu Wort kommenden Zeitzeugen wird Geschichte buchstäblich lebendig, wenngleich natürlich die in das Buch einfließenden Wertungen mehr die jeweilige Diskussions- und Wahrnehmungsebene erhellen als auf wasserdicht geprüftes Archivmaterial zurückzugreifen. Werner Sonne erhebt diesen Anspruch aber auch nicht. So oder so ist seine Form der Beobachtung überaus nützlich: Sie kann zum Einstieg in eine gründlichere Recherche Anregung bieten, sie kann aber auch den Hintergrund erhellen, vor dem sich anhand von nachprüfbaren Dokumenten strategische Weichenstellungen für die Geschichte der Atomwaffen auf deutschem Boden ermitteln lassen.

Die Tatsache, dass Werner Sonne eine klare Haltung zur fortdauernden nuklearen Teilhabe hat, fließt in Summe in seine Wertungen ein und lässt ihn aus der Sicht von Gegnern fortdauernder Stationierung von Atomwaffen in der Bundesrepublik gewiss als voreingenommen erscheinen. Tatsächlich ist das Buch als informierte Stellungnahme zu verstehen, nicht als Untersuchung eines neutralen Beobachters. Die Schlüsselfragen der Kontroverse werden kenntnisreich herausgearbeitet, ebenso die mit ihr verbundenen politischen Dilemmata. Vor allem die mitregierenden oder die nach den kommenden Bundestagswahlen nach Regierungsbeteiligung strebenden kleineren Parteien werden sich spätestens zur nuklearen Teilhabe positionieren müssen, wollen sie mit der CDU und CSU koalieren. Die Diskussion über Für und Wider der nuklearen Teilhabe bleibt jedenfalls spannend, auch unabhängig von den Koalitionsoptionen künftiger Bundesregierungen.

Doch zurück zur Substanz der Abhandlung. Dass Atomwaffen einen Beitrag zur Zügelung der Großmächte im Ringen miteinander während des Kalten Krieges geleistet haben, ist kaum zu bestreiten. Sie konnten es, gestützt auf ein System der Rüstungskontrolle und sicherheitsbildender Absprachen zwischen Ost und West. Die Zukunft der Rüstungskontrolle ist nunmehr jedoch fraglich, und vor allem für Europa stehen die Zeichen auf neues nukleares Rüsten. Werner Sonne fragt eingangs, ob nach 30 Jahren deutscher Einheit und europäischer Einigung die Lagerung von Atomwaffen auf deutschem Boden noch zeitgemäß sei. Sein Hauptargument für die nukleare Teilhabe – neben der transatlantischen Verklammerung auch das Argument der meisten ihrer Befürworter – ist, auf einen Nenner gebracht, die Möglichkeit zur Informationsteilhabe

und zur Mitentscheidung im Rahmen der Nuklearen Planungsgruppe der NATO. Ohne Teilhabe keine Mitsprache, so das Credo. Solange die NATO Atomwaffen für ihre kollektive Verteidigung vorhält – bzw. solange sich die NATO einer äußeren Bedrohung durch Atomwaffen ausgesetzt sieht – sei die Integration der Bundesrepublik in die Entscheidungsstruktur des Bündnisses in dieser Frage unverzichtbar.

Ob die kernwaffenbesitzenden Partner der Bundesrepublik letztlich Mitsprache oder gar ein Veto zur Entscheidung einräumen, bleibt freilich als Frage unbeantwortet. Die Gegner verneinen dies unter Hinweis auf die wiederholten Alleingänge der Trump-Administration. Dass diese allerdings nicht mit dem langjährigen Bündnispartner USA verwechselt werden darf, steht außer Frage. Dennoch: Neue Herausforderungen für die strategische Stabilität und die europäische Sicherheit stehen im Raum. Sie bedürfen einer sorgsamen Prüfung und vorausschauendes Handeln. Das Scheitern des Iran-Deals, die weitergehende Proliferation von Kernwaffen, die Unberechenbarkeit und Sprunghaftigkeit der US-Regierung, die problematische Zukunft des Nichtverbreitungsvertrags, schließlich die Miniaturisierung von Kernwaffen bei gleichzeitig erhöhter Treffergenauigkeit und mutmaßlich geringerem Schadensausmaß durch Russland und die USA mit dem damit verbundenen Verlust an strategischer Qualität atomarer Waffen als ausschließlich „politisches Mittel" sowie nicht zuletzt eine drohende neue Finanzkrise im Nachgang von Corona und ihre Folgen für die zur Verteidigung bereitgestellten Haushalte, all dies wird die Diskussion zur Relevanz von Atomwaffen für die Zukunft sicherheitspolitischer Stabilität in den kommenden Monaten stark beeinflussen. Der Streit um die nukleare Teilhabe ist bereits eröffnet.

Insofern ist das lesenswerte Buch von Werner Sonne hochaktuell, und eine gewichtige Quelle für Sachkunde und Erfahrungswissen sowie für den ebenso dringlichen wie geboten verantwortungsvollen Diskurs über die Sicherheit Deutschlands und Europas im 21. Jahrhundert. Abschließend sei noch angemerkt: Neben der Printausgabe liegt die Publikation erfreulicherweise auch als kostengünstiges E-Book vor.

Prof. Dr. Dr. Hans-Joachim Gießmann

Christian Forstner/ Götz Neuneck (Hrsg.), Physik, Militär und Frieden. Physiker zwischen Rüstungsforschung und Friedensbewegung. Wiesbaden: Springer Spektrum, 2018, 271 S.

Dass Physik und Militär miteinander zu tun haben, ist nicht erst seit der Atombombe Allgemeinwissen. Das Engagement von Physiker*innen für den Frieden ist in der Öffentlichkeit weniger bekannt, aber Friedensforschungskreise kennen z.B. die Aktivitäten der Pugwash-Konferenzen. Auf der Ebene der hohen Politik und Wissenschaftsorganisation sind beide Zusammenhänge in der Literatur gut erfasst. Das vorliegende Buch behandelt sie mit einer Reihe von Beispielen, die bisher nicht oder kaum untersucht und beschrieben wurden, mit Schwerpunkt auf Europa und Deutschland. Es geht zurück auf gemeinsame Sitzungen des Fachverbands Geschichte der Physik und der Arbeitsgruppe Physik und Abrüstung der Deutschen Physikalischen Gesellschaft aus dem Jahr 2015. Die zwölf Autor*innen kommen aus der Wissenschaftsgeschichte oder sind als Physiker in Wissenschafts-Abrüstungsbewegungen aktiv.

In seinem Beitrag „Der Erste Weltkrieg und seine Auswirkungen auf die deutschen Physiker" arbeitet Stefan Wolff (Deutsches Museum München) heraus, dass die Mehrheit der bedeutenden Physiker – wie auch Gelehrte anderer Disziplinen und Kulturschaffende – sich hinter die deutschen Kriegsziele stellte, etwa mit dem „Aufruf an die Kulturwelt", der den deutschen Militarismus als Bedingung der deutschen Kultur verteidigte. Einige betrieben aktiv Forschung für die Streitkräfte, aber Umfang und Wirkungen waren erheblich geringer als in der Chemie, die mit dem Gaskrieg eine neue Form der Kriegführung eingeführt hatte.

Bernd Helmbold (Universität Jena) zeigt in „Der Röntgenblitz – Universalwerkzeug für Industrie, Militär und Medizin", wie in den 1930er Jahren bei Siemens an Röhrengleichrichtern extrem kurze Pulse von Röntgenstrahlung entdeckt wurden (ebenso wie gleichzeitig bei General Electric in den USA). Der Physiker Max Steenbeck entwickelte verbesserte Entladungsrohre und machte Aufnahmen schnell bewegter Objekte, etwa Gewehrkugeln. Spätere Entwicklungen wurden und werden für die Untersuchung von Detonationen sowie die Entwicklung der panzerbrechenden Hohlladung verwendet. Bei der Entwicklung der Atombombe vom Implosionstyp (mit Plutonium als Spaltstoff, in Nagasaki eingesetzt) spielten Röntgenblitzaufnahmen eine zentrale Rolle.

In „Alltagsphysik statt Atombomben. Ein erneuter Blick auf den deutschen Atomverein" untersucht Christian Forstner (Universität Frankfurt/M.) die Wiener Gruppe im Uranverein. Nach der Eingliederung Österreichs in das Nazi-Reich 1938 wurden Leitungspositionen in Wien mit NS-Anhängern oder -Mitläufern besetzt. In drei zentralen Experimentierbereichen – Identifikation des bei Neutronenbeschuss aus Uran entstehenden neuen Elements (Plutonium), Spaltung von Urankernen mit schnellen Neutronen und Charakterisierung der Kernbruchstücke nach der Spaltung – zeigt der Autor, dass es sich bei den Aktivitäten des deutschen Uranvereins und speziell der Wiener Gruppe nicht um Großforschung wie beim US-Manhattan-Projekt handelte, sondern um „relativ unspektakuläre Messungen im physikalischen oder chemischen Labor".

In einem längeren Beitrag beschreibt Manfred Heinemann (Universität Hannover) die „Alliierte Erschließung und Aneignung des deutschen Industrie- und Wissenschaftspotentials 1944-47 durch die ‚Field Intelligence Agency, Technical (FIAT) (US)/(UK)'". Bekannt ist die Mission zum Abholen der deutschen Kernphysiker, der Umfang des Abschöpfens war aber weitaus größer. Ab 1944 gab es Richtlinien und Personal für Sammlung, Erfassung und Abtransport erbeuteter militärischer Dokumente. Wissenschafts- und Industrievertreter wurden systematisch befragt, Listen mit Tausenden von Personen angelegt. Hunderttausende von Reports, Mikrofilme von Dokumenten und Plänen wurden erstellt, deutsche Wissenschaftler schrieben Übersichtstexte über die Arbeiten in den jeweiligen Gebieten während der NS-Zeit. Die Ausbeutung deutschen Wissens beschränkte sich nicht auf militärische Fragen, sondern bezog alle Bereiche von Industrie und Wissenschaft ein. Der Autor wirft eine Reihe von Fragen in diesem Zusammenhang auf, die weiterer Forschung bedürfen.

Martin Fechner (Berlin-Brandenburgische Akademie der Wissenschaften) behandelt in „Laser als Waffen? Framing im Wissenstransfer", wie der Erfinder des Lasers,

Theodore Maiman (Hughes Aircraft Company, USA), 1960 in einer Pressekonferenz das neue Gerät als „atomares Radio-Licht" beschrieb ", als "Quelle sehr hoher ‚effektiver' oder äquivalenter Temperatur, höher als im Zentrum der Sonne oder von Sternen". Damit sei eine militärische Konnotation gegeben. Die gewählten Analogien sollten bei Laien Assoziationen eines kleinen, aber sehr potenten Strahlgeräts hervorrufen und Aufmerksamkeit für die eigene Wissenschaft herstellen.

Dieter Hoffmann (Max-Planck-Institut für Wissenschaftsgeschichte, Berlin) behandelt „Albert Einstein – relativ politisch". Während führende Physiker sich im ersten Weltkrieg dem nationalistischen „Aufruf an die Kulturwelt" anschlossen, war Einstein einer der wenigen, die für ein rasches Kriegsende und Völkerverständigung eintraten. Eine gewisse Inkonsequenz lag darin, dass er auch an Forschung und Entwicklung militärrelevanter Themen teilnahm, nämlich für ein neues Tragflächenprofil und den Kreiselkompass. In den 1920er und frühen 1930er Jahren erhöhte der wachsende Antisemitismus in der deutschen Gesellschaft seine politische Sensibilität. Mit der Bestätigung seiner Relativitätstheorie bei einer Sonnenfinsternis wurde er zu einer öffentlichen Person. Nach der Emigration geißelte er die Nazi-Diktatur. Im Zweiten Weltkrieg sah er im militärischen Kampf das einzige Mittel gegen die Weltherrschaft Hitlerdeutschlands, was dann auch zur Unterzeichnung des bekannten Briefes für ein US-Atombombenprogramm an Präsident Roosevelt führte.

Wolfgang L. Reiter (Österreichisches Bundesministerium für Wissenschaft und Verkehr) betrachtet mit „Hans Thirring – ein Leben im Spannungsfeld von Physik und Politik" ein weiteres Beispiel eines hervorragenden Physikers, der sich für Abrüstung einsetzte. Durch die Erfahrungen des Ersten Weltkriegs zum Kriegsgegner und Antimilitaristen geworden, war der Professor der Universität Wien einer der wenigen Hochschullehrer, die sich dem Naziterror widersetzten. In den 1930er Jahren nahm er an der österreichischen und internationalen Friedensbewegung teil. Nach 1945 setzte er sich gegen Nuklearaufrüstung ein. Den von der kommunistischen Partei unterstützten Österreichischen Friedensrat verließ er nach der Invasion Südkoreas durch nordkoreanische Truppen und wurde dann aktiver Teilnehmer der Pugwash-Konferenzen. Sein Thirring-Plan zur vollständigen Abrüstung des neutralen Österreich fand keine Akzeptanz.

Ulrike Wunderle (Vereinigung Deutscher Wissenschaftler) widmet sich dem Thema „Die Genfer Atomkonferenz von 1955 und die Anfänge der Pugwash Conferences on Science and World Affairs: Zwei diplomatische Handlungsebenen US-amerikanischer Kernphysiker im Kalten Krieg". Die UN-Atomkonferenz entstand aus der US-Initiative „Atoms for Peace" und sollte in der Systemauseinandersetzung ein positives Bild der USA und der zivilen Atomenergie fördern. Die US-Physiker erhofften sich wissenschaftlichen Austausch mit den sowjetischen Kollegen und ein höheres Ansehen der eigenen Wissenschaft. Für die systematische Befassung mit der Gefahr eines Nuklearkriegs wurde 1957 die erste Conference on Science and World Affairs im kanadischen Pugwash durchgeführt. Die Pugwash-Konferenzen versammelten Spitzenforscher aus Ost und West; in vertraulicher Atmosphäre wurden Konzepte für Abrüstung entwickelt, die dann den Regierungen nahegebracht wurden. Beiden Arten von Konferenzen war gemeinsam, dass ein Zusammenhang von wissenschaftlicher und gesellschaftlicher Entwicklung gesehen wurde und dass die „Einheit der Wissenschaft" Ansätze bietet, ideologische Gegensätze zu überbrücken.

Stefano Salvia (Universität Pisa) behandelt in „Bewehrte Kooperation(en) – friedliche Atome, pazifistische Physiker und Friedenspartisanen zu Beginn des Kalten Krieges (1947-1957)" verschiedene Bewegungen, beginnend mit dem kommunistisch beeinflussten Weltfriedensrat. Solchen Bemühungen setzten die USA das „Atoms-for-Peace"-Programm entgegen, mit der Genfer Konferenz von 1955 und dem Export von Forschungsreaktoren – mit hoch angereichertem Uran – in viele Länder. Das Russell-Einstein-Manifest von 1955 sollte pro- wie antikommunistische Kräfte ansprechen. In Deutschland verabschiedeten 1955 18 internationale Nobelpreisträger die Mainauer Deklaration gegen die Nuklearbewaffnung. Politisch wichtiger wurde die Erklärung der Göttinger Achtzehn von 1957 gegen die Nuklearbewaffnung der neuen Bundeswehr. Ab 1957 fanden die internationalen Pugwash-Konferenzen statt, die sich um Track-II-Diplomatie bemühten. Niels Bohr trat dagegen für weitgehende Transparenz ein, gerade bezüglich Nuklearwaffen; Regeln sollten im UN-Zusammenhang beschlossen werden.

Eckhard Wallis (Deutsches Museum München) beschreibt in „'Suivre son propre rhythme' – Alfred Kastler zwischen Physik und Politik 1950-1960" ein weiteres Beispiel eines Spitzenphysikers, der für Frieden eintrat. Ab 1951 nahm er am „Mouvement des 150" für Kernwaffenabrüstung teil und sprach sich gegen die aufkommende französische Nuklearrüstung aus, auch gegen totalitäre Tendenzen. Seine Mitarbeit am Internationalen Geophysikalischen Jahr 1957-58 mit Raketenexperimenten in der oberen Atmosphäre und Kontakten zu Militärbehörden zeigt, dass er diese nicht prinzipiell ablehnte.

Der letzte Beitrag, „Die Amaldi-Konferenzen", ist ein Zeitzeugenbericht von Klaus Gottstein (Akademien-Union), der von Anfang an beteiligt war. Die nach dem italienischen Physiker benannten Konferenzen nationaler Akademien und wissenschaftlicher Gesellschaften gehen auf eine Initiative der US-Akademie zurück, die auch europäische Vertreter in die Track-II-Diplomatie einbeziehen wollte. Die Konferenzen fanden ab 1988, zunächst meist in Italien, statt. Schwerpunkte sind internationale Sicherheit und Rüstungskontrolle, aber auch Nachhaltigkeit und Gerechtigkeit sind wichtige Themen. Das Ziel, ähnlich wie die US-Akademie ein europäisches Komitee für Sicherheit und Rüstungskontrolle zu gründen, ist noch nicht erreicht.

Der Band versammelt Beiträge verschiedener Art, leider mit einer Vielzahl von Druckfehlern. Die Auto*innen schildern wichtige Personen und deren Herangehensweisen an Fragen im Spannungsfeld von Physik und Militär sowie Physik und Frieden bzw. nationaler und internationaler Politik. Zum Teil werden neue Fakten erschlossen. Bei den Konferenzen sind interessante Details zu den jeweiligen Vorgeschichten, Motivationen und Entwicklungen angegeben. Wer mehr wissen will, kann auf die meist detaillierten Literaturlisten zurückgreifen. Ein ausführliches Personenverzeichnis erschließt das Buch. Insgesamt bietet es einen guten Einstieg in die verschiedenen Facetten des Verhältnisses von Physik, Militär und Frieden.

PD Dr. Jürgen Altmann

Hans-Dieter Heumann: Strategische Diplomatie. Europas Chance in der multipolaren Welt, Paderborn 2020: Verlag Ferdinand Schöningh (249 S.)

Andraž Zidar: The World Community between Hegemony and Constitutionalism, The Hague 2019: Eleven International Publishing (356 S.)

Interessant ist zunächst eine Parallele der beiden hier zur Diskussion stehenden Bücher. Ihre Verfasser teilen vergleichbare berufliche Erfahrungen in Wissenschaft und Praxis, einerseits der ehemalige Diplomat und Biograph des langjährigen deutschen Außenministers Hans-Dietrich Genscher, Akademiepräsident und Hochschullehrer Dr. Hans-Dieter Heumann sowie andererseits Dr. Andraž Zidar, früher Universitätsdozent und Akademischer Direktor des Europäischen Masterprogramms ‚Menschenrechte und Demokratisierung' in Venedig, bevor der erfahrene Diplomat zum Direktor der Akademie des slowenischen Außenministeriums berufen wurde.

Beide Autoren widmen sich einer ähnlichen Thematik, dem Zusammenspiel von Macht, Politik und Diplomatie – der eine allerdings eher gestützt auf die Analyse der großen politischen Machtzentren sowie der strategischen Entwicklungen in den letzten Jahren, der andere eher aus dem Blickwinkel einer fundierten wissenschaftlichen Durchdringung strategischer Grundmuster von Politik und Diplomatie seit dem Ende des Ost-West-Konflikts. Im letzteren Falle ist der Ursprung des Projekts als Dissertation am Genfer Institut für Höhere Studien zu berücksichtigen, jedoch reichen die Überlegungen von Andraž Zidar weit in die aktuellen politischen Diskursräume hinein. Beide Veröffentlichungen sind umfänglich quellengestützt, sehr gut recherchiert und ungeachtet ihrer politischen Ausrichtung auch als wissenschaftliche Veröffentlichungen von großem Wert. Neben den genannten Parallelen gibt es Unterschiede in den jeweiligen Generationen und der Herkunft der Autoren, welche die beiden Sichtweisen aus europäischer Perspektive nicht nur im Vergleich, sondern auch in Summe lohnen lassen.

Das Leitthema Hans-Dieter Heumanns ist ‚Strategische Diplomatie'. Es ist die Politik ‚langer Linien', der engen Verknüpfung von Theorie und Praxis, einer kohärenten Sicht, die aber zugleich der Außenpolitik konzeptionell im Vergleich zur Innenpolitik „einen eigenen Raum verschafft" (H. Münkler). Seine Ausführungen fokussieren vor allem auf strategische Dynamiken und Wendepunkte globaler und europäischer Politik, und sein Blick auf die Gestaltungsräume der Diplomatie sieht Handlungsstärke insbesondere im Agieren starker Führungspersönlichkeiten und der großen Mächte. Zidar hingegen sieht eine stärkere Bindewirkung der globalen und regionalen Institutionen auch unter veränderten Vorzeichen als gegeben, wobei sich die Autoren in der Grundannahme offenkundig einig sind, dass Europa und die Welt sich in einer Phase des Übergangs befinden. Die gewohnten Paradigmen sind verblichen, neue Paradigmen noch nicht final etabliert.

Heumann sieht allerdings als dominierenden Trend eine Verschiebung von gemeinschaftlicher Zusammenarbeit hin zu machtpolitischer Verantwortung und Rivalität großer Staaten gegeben, während Zidar ausführt, dass Macht und gemeinschaftliche Regelwerke nicht allein als Antinomien zu verstehen seien, die einander ausschließen, sondern sich Hegemonie und Recht einander in gewisser Weise sogar bedingen. Seine These zu einer „klaren Tendenz" in der internationalen Gemeinschaft, supranationale Strukturen zu schaffen, die normatives und institutionelles Recht zur Regelung globaler Fragen entfalten können, mag angesichts gegenläufiger Entwicklungen in Bezug auf den Rückhalt von Regimen, etwa der Rüstungskontrolle, oder von Institutionen, wie zum Beispiel der UNESCO oder WHO, zu bestreiten sein. Allerdings räumt der Autor selbst ein, dass sich die von ihm ausgemachte Tendenz dauerhaft nur zu behaupten vermag, wenn sie von den Staaten, vor allem den mächtigsten unter ihnen, weiterhin unterstützt wird.

Das neue supranationale Paradigma, wie der Autor es nennt, ist jedenfalls noch nicht gegeben. Heumann sieht eine solche Wirklichkeit aber aktuell auch nicht im Entstehen. Im Gegenteil. Seiner Einschätzung nach bildet sich tendenziell vielmehr eine multipolare, eine „oligarchische Welt" regionaler Machtzentren heraus – namentlich einerseits geführt durch die USA, China, Russland, andererseits geprägt durch Entwicklungen im Nahen Osten und in Europa. Für Heumann ist ein neues strategisches Paradigma bereits deutlicher umrissen. Jedenfalls sei das tradierte Paradigma einer Welt stabiler Allianzen oder Gemeinschaften nicht mehr vorhanden, und die globalen Kräfteverschiebungen zwischen den Zentren seien längst und weiter andauernde Realität. Als bittere Erkenntnis in diesem Zusammenhang sei in der Welt der Verlust von Demokratie und Rechtsstaatlichkeit als nachahmenswerte Rollenmodelle zu beklagen. Vielmehr rückten Interessen und Einflusspotenziale in den Vordergrund, ohne dass dieser Kurs den Nachweis erbringen könnte, bessere Antworten auf die globalen Zukunftsfragen zu besitzen. Europa kann, so Heumann, nur bestehen, wenn es seine Interessen und Werte als Einheit versteht und eine Allianz für den Multilateralismus schmiedet, in der eine regelbasierte multilaterale Weltordnung gut aufgehoben ist. Es sei ein Irrtum anzunehmen, dass deren Attraktivität für viele Akteure in der Welt allein dadurch schwindet, dass die Rivalität der großen Mächte deren Einigungswillen zum Vorteil aller schmälert.

Hier überlagern sich die Erkenntnisse beider Autoren, denn auch Zidar kommt zu dem Schluss, dass kollektive Regelwerke zur Zügelung von Anarchie und zur Verregelung von Verfahren für den Umgang mit globalen Herausforderungen – von der Klimakrise bis zur Bekämpfung von Pandemien – unverzichtbar seien, denn ohne die Hilfestellung global geteilter Normen, Mechanismen und Verfahren könnten diese und andere Krisen nicht bearbeitet oder gar überwunden werden. Während Zidar dabei auf die Gestaltungskraft einer Weltgemeinschaft setzt, welche Hegemonie und Recht in Balance zu halten imstande ist, geht Heumann davon aus, dass es vor allem darum gehen müsse, die multipolare Welt in eine regelbasierte Ordnung einzubetten, die allen nutzt, aber den Rechtsbruch nicht hinnimmt und stark genug, ist ihre Werte und gemeinsamen Interessen zu schützen.

So verstanden interpretieren beide Bücher mit zwar unterschiedlicher Methodik gleichermaßen einen althergebrachten Aphorismus und bekräftigen ihn zugleich auf neue Weise: „Recht ohne Macht ist machtlos – Macht ohne Recht ist rechtlos. Also muss man dafür sorgen, dass das, was Recht ist, mächtig und das, was mächtig ist, gerecht sei" (Blaise Pascal, 1669, freie Übersetzung).

Prof. Dr. Dr. Hans-Joachim Giessmann

Matthias Herdegen: Der Kampf um die Weltordnung. Eine strategische Betrachtung. München: C.H. Beck, 2019.

„Kampf um die Weltordnung" lautet der Titel des Werkes von Matthias Herdegen. Dementsprechend beginnt es mit einem sorgenvollen Blick auf die Verschiebungen im internationalen Machtgefüge. Seine Diagnose einer „Weltunordnung" (S. 15) kommt keineswegs überraschend, gehört sie doch zum gängigen Repertoire westlicher Regierungen und ihnen nahestehender Think Tanks. Verantwortlich macht Herdegen die üblichen Verdächtigen, genauer den „imperiale[n] Drang Chinas und Russlands nach Ausdehnung ihrer Einflusssphären" (S. 11), aber auch die am „amerikanischen Eigeninteresse" (S. 12) ausgerichtete Politik der Trump-Administration. Allerdings dient dieser Einstieg lediglich als Sprungbrett ins eigentliche Thema des Buches, nämlich den Kampf um die Deutung des Völkerrechts. Denn die skizzierten Entwicklungen konnten nach Herdegen nur deshalb zur Weltunordnung führen, weil sie auf das „Versagen eines naiven Westens und die Illusion einer Verrechtlichung der internationalen Beziehungen" (S. 15) trafen.

Das globale Kräftespiel kann Herdegen als Professor für Völkerrecht natürlich nicht in seinem Sinne beeinflussen, die wissenschaftliche wie politische Debatte aber sehr wohl. So möchte er dem völkerrechtlichen Diskurs der westlichen Staatenwelt eine „bewusst strategische Ausrichtung" (S. 13) verpassen, die sich „stärker als bisher auf die realen Macht- und Interessenbeziehungen" (S. 12f.) einlässt und sich dem „Ziel von Sicherheit und Stabilität" (S. 12) verschreibt. Das bedeutet für ihn auch, sich von „Illusionen einer harmonischen Weltgesellschaft" zu verabschieden und „sich einem Realismus [zu] stellen" (S. 12), der schon vor Trumps Wahl Einzug in die Weltpolitik gehalten habe.

Damit steht das Urteil über die im Anschluss durchaus kenntnisreich vorgetragenen politikwissenschaftlichen Großtheorien fest: „Die Vorstellung einer wahrhaft überstaatlichen, kosmopolitischen oder auch solidarisch ausgerichteten ‚global governance' hat den Realitäten nicht standgehalten. […] Die wirkungsmächtigen internationalen Organisationen bleiben […] dem Kräftespiel ganz im Sinne des klassischen Realismus ausgesetzt." (S. 94). Wenngleich diese Aussagen eher als starke Behauptung denn als gut begründeter Beweis daherkommen, könnte ihnen auf den ersten Blick noch der Status einer schonungslosen Realitätsbeschreibung attestiert werden, deren ‚Wahrheitsgehalt' sich im akademischen Diskurs zu erproben hätte. Diesen führt Herdegen jedoch ganz im Foucault'schen Sinne als Machtdiskurs unter Einsatz tendenzieller Ausschließungsmechanismen. So stuft er ihm unliebsame Positionen als dermaßen weltfremd ein, dass sie einem vernünftigen Zeitgenossen als alternative Denkoption nicht mehr zur Verfügung stünden. Beispielsweise verortet Herdegen „manche idealistische Deutung auf einer Insel der Seligen" (S. 19), auf der „Biotope überstaatlicher Werte und transnationaler Kommunikationsräume" (S. 20) eigentlich nur deshalb gedeihen können, weil sie unter dem „transatlantischen Schutzschirm" (S. 20) stehen, den die „militärische[…] Hegemonie der USA" (S. 20) aufspannt.

Herdegen zielt aber nicht auf die politikwissenschaftliche Theoriebildung, sondern auf die Völkerrechtslehre ab. Die Auseinandersetzung mit einigen Denkschulen aus der Teildisziplin der Internationalen Beziehungen leistet hierzu aber eine wichtige Vorarbeit, denn deren Ordnungsvorstellungen „spiegeln sich auch im Völkerrecht wider" (S. 53). Das Verdikt, das Herdegen über idealistisch inspirierte kooperative und kosmopolitische Ansätze fällt, träfe mithin auch ihr völkerrechtliches Pendant. Damit meint er die Position einer Konstitutionalisierung des Völkerrechts. Deren Anhänger fügten sich seines Erachtens zu einer „kleinen Bekenntnisgemeinschaft in Kontinentaleuropa und Nordamerika" (S. 246). Diese Fremdbeschreibung dient Herdegen gleichsam als Negativfolie, die seine eigene Position positiv ins Bild setzt: Demnach bestätigt die dem Konstitutionalismus attestierte Irrelevanz und Realitätsuntauglichkeit jene Relevanz und Realitätstauglichkeit, die der Autor für seine strategische Neuausrichtung des Völkerrechts reklamiert. Dabei könnte fast übersehen werden, dass der Vorwurf der Bekenntnisfreudigkeit auf seinen Urheber zurückfällt. Denn auch Herdegen bekennt sich: zur „Privilegierung großer Mächte" (S. 133), zum „Gleichgewicht der Macht" (S. 135), zur „nukleare[n] Abschreckung" (S. 136), zur „Beschränkung der Zahl der Atommächte" (S. 136) ohne Erwähnung der im Nichtverbreitungsvertrag festgeschriebenen Abrüstungsverpflichtungen (S. 158-160), zum „Schutz internationaler, vor allem maritimer Transportwege" (S. 35) ebenso wie zum „gesicherten Zugang zu begrenzten und endlichen Ressourcen (Rohstoffe, Energie, Wasser)" (S. 35f.) einschließlich eines „‚kleine[n] Selbstverteidigungsrecht[s] im Sinne einer verhältnismäßigen Abwehrreaktion" (S. 191) beispielsweise bei Übergriffen auf einzelne Handelsschiffe.

Vor allem aber bekennt sich Herdegen zur „Selbsterhaltung der Staaten [als] [e]lementarer Zweck einer internationalen Ordnung" (S. 107). Damit stellt er nicht nur eine weitere (diskussionswürdige) Sachbehauptung auf, sondern diese fungiert als Axiom für die Entfaltung seiner Völkerrechtskonzeption. Daher nimmt es kaum wunder, dass Herdegen „Sicherheit [als] das wichtigste aller internationalen Güter" (S. 24) begreift, die sich unmittelbar aus dem Zweck der Selbsterhaltung ableitet. Auf diese Weise entsteht eine sicherheitslogische Version des Völkerrechts, die innerhalb des ordnungspolitischen wie normativen Gefüges strikt vom einzelnen Staat her denkt, der in seinem Selbsterhaltungstrieb möglichst wenig eingeschränkt werden dürfe.

Insofern ist es durchaus konsequent, dass Herdegen sich das Gewaltverbot besonders intensiv vorknöpft. Zwar spricht er sich letzten Endes doch dafür aus, „im Sinne der globalen Nachkriegsordnung am Gewaltverbot als systembildenden Element der internationalen Sicherheitsordnung festzuhalten" (S. 148). Andernfalls drohe der „Rückfall in eine Zeit der absoluten Selbsthilfe" (S. 148), der Herdegen offenbar dann doch nicht das Wort reden will. Allerdings kratzt er offensiv am Absolutheitsanspruch der Norm. Zumindest rhetorisch stellt er sie sogar zur Disposition, wenn er aus empirischer Sicht die Frage für berechtigt hält, „ob das Gewaltverbot zu den unverzichtbaren Grundlagen einer Weltordnung gehört" (S. 148). Dessen Bedeutung relativiert er in der Folge gleich zweifach. Zum einen gilt ihm ein „‚grosso modo' funktionierendes Konfliktmanagement durch die großen Mächte [als] eine weitaus wichtigere Bedingung für die Stabilität der

territorialen Ordnung“ (S. 148). Zum anderen stellt Herdegen anhand eines konkreten Symptoms, nämlich der Ablehnung eines Rechts der Staaten auf gewaltsame Rettung eigener Bürger im Ausland, die allgemeine Diagnose einer „obsessive[n] Verklärung des Gewaltverbotes“ (S. 192).

Der lockere Umgang mit dem Gewaltverbot setzt sich in der Auseinandersetzung über die Reichweite des Selbstverteidigungsrechts fort. Hier wiederholt Herdegen auch die bereits erprobte Argumentationstechnik. So orientiert er sich am Ende zwar an einem weitgehend akzeptierten Recht auf „‘preemptive self-defense‘“ (S. 193), das auf einen unmittelbar bevorstehenden Angriff beschränkt ist. Bei nuklearen, chemischen oder biologischen Bedrohungen greife es ausdrücklich „nur dann, wenn objektiv erkennbar (erstens) Waffenvernichtungspotentiale bereits verfügbar sind, (zweitens) mit einem Angriff mit Massenvernichtungswaffen *jederzeit* zu rechnen ist und (drittens) zu einem späteren Zeitpunkt ein Angriff nicht mehr verlässlich abgewehrt werden kann“ (S. 196 – Herv. im Original). Allerdings hadert Herdegen ersichtlich mit dem Umstand, dass ein noch weiter „vorverlagertes Recht auf Selbstverteidigung“ (S. 194) sich bislang ebenso wenig hat durchsetzen können wie ein „mindere[r] Status der Staatlichkeit“ (S. 220) für sogenannte Schurkenstaaten, der auch zum „Einsatz von Zwangsmitteln mit dem Ziel eines Regimewechsels“ (S. 220) berechtigen würde. Unverkennbar liebäugelt Herdegen mit der Nationalen Sicherheitsstrategie der USA von 2002, die beides enthält: ein Konzept antizipatorischer Selbstverteidigung bei bestehenden Unklarheiten über Ort und Zeitpunkt eines militärischen Angriffs sowie die Selbstermächtigung zu Präventivschlägen gegen ‚Schurkenstaaten‘. Mit Blick auf Iran und Nordkorea attestiert Herdegen der Bush-Doktrin „weit mehr Substanz als ihre pauschale Verurteilung erkennen lässt“ (S. 195). Über die Antwort auf die Frage, ob das Urteil genauso ausgefallen wäre, stünde der Passus in der russischen oder chinesischen Militärdoktrin, ließe sich an dieser Stelle nur spekulieren. Immerhin räumt Herdegen Umsetzungsprobleme im Kontext des Irakkriegs 2003 ein. Dem Waffengang hafte unter den gegebenen Bedingungen nolens volens „das Stigma der offensichtlichen Völkerrechtswidrigkeit“ (S. 46) an. Darüber hinaus hätten die regional verheerenden Folgen den gewaltsamen Regimewechsel zugunsten demokratischer Verhältnisse „völlig diskreditiert“ (S. 220).

Bei aller völkerrechtlichen Expertise handelt es sich eher um eine Kampfschrift als um eine akademische Abhandlung. Daran ändern auch allseits zustimmungsfähige Passagen wie etwa das Bekenntnis zum Ziel der „normative[n] Einhegung von Konflikten schon im Vorfeld einer gewaltsamen Auseinandersetzung“ (S. 20) nichts, wirken sie doch wie die unverzichtbare Kulisse für das eigentliche Schauspiel. Frappierend ist vor allem die Chuzpe, mit der der Autor einen ganzen Strang der Völkerrechtslehre entsorgt und deren Anhänger abserviert. So unbestreitbar es ist, dass Völkerrecht im Wesentlichen zwischenstaatliches Recht ist, dass Staaten in ihrer territorialen Integrität geschützt sind und ihnen im Falle eines bewaffneten Angriffs ein Recht zur individuellen wie kollektiven Selbstverteidigung zusteht, so problematisch ist es, Völkerrecht radikal aus dieser sicherheitslogischen Perspektive zu entwickeln. Bereits in der Präambel der Charta der Vereinten Nationen erklären sich die „Völker der Vereinten Nationen“ eben nicht fest entschlossen, den Staaten zu ihrer Selbstbehauptung möglichst freie Hand zu verschaffen, sondern „künftige Geschlechter vor der Geißel des Krieges zu bewahren, die zweimal zu unseren Lebzeiten unsagbares Leid über die Menschheit gebracht hat“. Ziel ist nicht die partikulare Sicherheit der jeweils einzelnen Staaten, sondern „den Weltfrieden und die internationale Sicherheit zu wahren“. Das bedeutet nun aber gerade nicht, den einzelnen Staat auf dem „Altar einer idealistischen Weltsicht“ (S. 17) zu opfern, wie Herdegen konstatiert. Im Gegenteil: Das Ringen um den Weltfrieden schließt die Sicherheit der Staaten im Sinne einer verlässlichen Abwesenheit personaler Großgewalt mit ein, während das auch militärisch instrumentierte Streben der Staaten nach partikularer Sicherheit den Weltfrieden eben nicht ermöglicht, sondern unterminiert. Das zumindest lehrt das altbekannte Problem des Sicherheitsdilemmas, das John H. Herz als Grenzgänger zwischen Realismus und Idealismus so prägnant beschrieben hat.

Ohne Zweifel schafft allein das lautstarke Bekenntnis keinen Weltfrieden. Das wussten auch die Architekten der Vereinten Nationen, andernfalls hätten sie das Selbstverteidigungsrecht nicht in deren Charta zu verankern brauchen. Immerhin haben sie es dort strikt konditioniert. So gilt das Selbstverteidigungsrecht gemäß Artikel 51 ausschließlich für den Fall eines bewaffneten Angriffs, wie auch Herdegen explizit hervorhebt (S. 189). Darüber hinaus darf es nur solange beansprucht werden, „bis der Sicherheitsrat […] die erforderlichen Maßnahmen getroffen hat“. Diese Einschränkung versteckt der Autor jedoch im ausführlichen Zitat des einschlägigen Artikels, ohne sie nochmals eigenständig herauszustellen (S. 189). Im Falle einer Explikation wäre die subsidiäre Position des Selbstverteidigungsrechts gegenüber dem Kollektivsystem der Vereinten Nationen sichtbar geworden. Die Folge läge auf der Hand: Die Argumentation hätte viel stärker vom Ziel des Friedens einschließlich der Gewaltvermeidung her entwickelt werden müssen. Und damit eng verbunden wäre das Völkerrecht deutlicher in seiner normativen Eigenwertigkeit erkennbar gewesen, die sich auch gegenüber jenen Großmächten als widerborstiger erweist, die Herdegen strukturell privilegiert. Gewiss dürfte heute der Anspruch vermessen wirken, das Völkerrecht möge der politischen Macht die Fackel vorantragen, wie es Immanuel Kant einst noch im Verhältnis der Philosophie gegenüber der Theologie für möglich gehalten hatte. Dass aber das Völkerrecht sich weigert, der politischen Macht einfach nur die Schleppe nachzutragen, müsste ihm schon abverlangt werden können.

Dr. habil. Sabine Jaberg

Wolfgang Peischel (Hrsg.), Wiener Strategie-Konferenz 2018. Strategie neu denken. Berlin: MILES-Verlag 2019.

Seit über 75 Jahren unterhalten die US-Amerikaner mit Erfolg wissenschaftliche Denkfabriken, um Strategien zur Bewältigung der politischen und militärischen Herausforderungen zu entwickeln. Nach dem Desaster des II. Weltkrieges war eine eigene deutsche Militärstrategie nicht gefragt – dafür waren nun die NATO-Hauptquartiere zuständig. Wie aber Offiziere der Bundeswehr künftig strategisches Können für

die Tätigkeiten in NATO-Stäben erwerben könnten, blieb außer Betracht. Soweit strategische Fähigkeiten nicht als „angeboren" gelten, gab es nur den Weg des learning by doing – on the job. Denn bis vor drei Jahren gab keine entsprechende Lernstätte im Deutschen Militär. Daher darf man gespannt sein, wie sich der Vorstoß der ehemaligen Verteidigungsministerin von der Leyen zur Gründung eines Think-Tanks für strategische Fragen, das GIDS (German Institute for Defence and Strategic Studies) an der Führungsakademie der Bundeswehr (FüAkBw), entwickeln wird.

Das nicht wegzudiskutierende „gegenwärtigen Strategiedefizit" im deutschsprachigen Raum in Politik, Diplomatie, Sicherheitsexekutive, öffentlicher Verwaltung, privatwirtschaftlicher Unternehmensführung, dem Non-Profit-Bereich wie auch NGO's erklärt Matlary (S. 405) damit, dass „politische Eliten die Weltkriege und den Kalten Krieg vergessen hätten. Sie zeigten daher wenig Interesse an Sicherheits- und Verteidigungserfordernissen und setzten militärische Macht nur in humanitären Interventionen zum ‚guten Zweck' ein. Damit würde Europa aber unfähig, glaubhaft Abschreckung auszuüben, und zum Spielball der Akteure, die sehr wohl strategiefähig sind. Zum anderen fällt eine zunehmend inflationäre Nutzung und Unklarheit des Begriffs Strategie für Tätigkeiten aller Art auf. Dies bedarf der Klärung, nicht nur für die Lehre und Forschung der militärischen Strategie, sondern auch wie diese zivilisiert und damit interdisziplinär akademisiert werden kann.

Dieser Aufgabe stellt sich Brigadier Wolfgang Peischel seit 2016 mit der Initiative der Österreichischen Militärschen Zeitschrift (ÖMZ) in Verbindung mit der EMPA (European Military Press Association) und in Zusammenarbeit mit der Generalstabsausbildung des Österreichischen Bundesheeres mit der jährlichen „Wiener Strategie-Konferenz". Es geht dabei um

- die Suche nach dem inhaltlichem Fundament für eine wissenschaftliche Strategielehre, nicht nur für den militärischen Bereich,
- die Erfassung und Analyse des gegenwärtigen Strategiedefizits,
- die akademische Anerkennung eines Lehrstuhls für einen universitären Lehr- und Forschungsgegenstand „Strategiedenken",
- die Lehre in den Streitkräften mit entsprechender Didaktik und Methodik und
- eine Grundlage für den weitergehenden dialektischen wissenschaftlichen Diskurs im Konferenzformat auch über teilstrategische Grenzen hinaus.

Die Arbeitsergebnisse werden veröffentlicht. Der voluminöse dritte Bericht von 2018 setzt nun den Diskurs der beiden Vorläuferkonferenzen fort. Daraus entsteht schrittweise ein Lehrwerk zu „Strategiedenken". Die Dokumentation der Texte gliedert sich nach den Vorträgen, den Einführungen und Ergebnissen der Panels sowie weiterführenden Aufsätzen. Über allem steht als leitende Fragestellung die nach vier modernen Begriffen: „Narrative, Hybridität/Hybride Kriege, Resilienz und Cyber". Diese Begriffsquadriga wird in allen Panels und Vorträgen aus unterschiedlichen Sichtweisen geprüft und definiert. Dabei stellt sich die Frage, ob dies nicht nur alter Wein in neuen Schläuchen sei oder umgekehrt und ob die vier Begriffe Theoriefragmente oder konkrete Aspekte für das Verstehen, Denken und Arbeiten in Strategie sind. Deutlich ist, dass diese Ausdrücke für Komplexität und Ungewissheit als „Kernprobleme jeder Strategiebildung" stehen, als Ausdruck des „unknown unknown". Es wurde auch auf manipulative Gefährdungen und Fehldeutungen hingewiesen, die den Begrifflichkeiten Narrativ, Cyber, Hybridität und Resilienz innewohnen. Sie seien nämlich im Strategiefeld nicht nur Instrumente, Mittel oder Medien, sondern immer auch und zugleich Gegenstand, Gefahrenpunkt und eigen-wirkmächtiges Element im Rahmen von Strategiedenken (Jeschonnek S. 366 – 370). Generell wird kritisch die „permanente Produktion" neuer Termini gesehen, sie wirke sich eher negativ auf die wissenschaftliche Produktion aus, da sie „die Aufmerksamkeit auf die taktische Ebene lenken und breitere strategische und politische Fragen ausblenden (S. 341). Deutlich wird auch, dass es keinen einheitlichen Gebrauch und Nutzen so eines Terminus' auf den verschiedenen Ebenen des Strategiedenkens geben kann, denn die Bedeutung und Prognosekapazität derartiger Begriffe liegt in der Vielheit von Bezügen und Ebenen bis zum individuellen Bild und Verständnis dessen, was der einzelne, ob Politiker, Verwalter oder Soldat für sich in der Weltunordnung oder Welt im Aufbruch braucht (Birk S. 188).

Die Befassung mit der begrifflichen Quadriga trägt im Laufe der Dokumentation zum eigentlichen Gewinn der Konferenz bei:

Cyber wird als ein Handlungsfeld für Strategie gesehen, sei es als Ziel oder Zweck, sei es als Mittel zur strategischen Behandlung in Form einer Offsetstrategie des Nieder- oder Kaputtrüstens bzw. als der zu beeinflussende Teil des strategischen Prozesses.

Hybridität bezeichnet aus politischer wie militärischer Sicht ein Zusammen von militärisch-kriegerischen Wegen, Mitteln und Methoden vom konventionellen über subversiven bis atomaren Krieg mit anderen vergleichbaren aber nicht originär militärischen Formen. Dabei wird vor einer „Marginalisierung" der militärischen Kompetenz gewarnt, „dass die breite Palette an nicht-militärischen Instrumenten Sicherheit auch ohne wirkungsvolle Streitkräfte garantieren könnte" (Peischel,. S. 106). Das hybride Risikopotenzial sei bisher nicht ausreichend untersucht, um daraus strategieentsprechende Ableitungen entwickeln zu können (s. Gegner S. 230ff).

Staatlich-politische Resilienz wird meist statisch als Resilienz-Sicherung gedacht. Resilienz ist aber in ihrer ganzen (begrifflichen) Bandbreite zu verstehen. Deshalb müssen Funktionsprinzipien gesamtheitlich strategischen Denkens entwickelt werden, um damit zum Aufbau und zur Aufrechterhaltung einer dynamischen Resilienz beitragen zu können. Die Beispiele zu diesem Thema aus israelischer Sicht verdeutlichen, dass Resilienz sowohl als persönlich-individuelle, wie als „nationale Resilienz" Bedeutung hat und zwar mit „realistischen Auswahlmöglichkeit" zwischen Schadensbegrenzung und definitiver Lösung.

Die Bedeutung von Narrativen als politische Denkfigur, die handlungsanleitende, gesellschaftliche und soziale Maximen zur Verfügung stellt, ist am weitesten durchdacht. Sie sind „Grautöne", die zur „Komplexität" und der Unmöglichkeit des exakten Abwägens bei Strategie schlechthin zu zählen sind. Sie bieten „weiche Zugänge zu harten Fakten" (Birk, S. 237 ff.). Dabei geht es um „kulturelle Selbstbespiegelungen", „wie die für den jeweiligen Teilbereich zuständigen Akteure und Eliten die Rolle des eigenen Bereiches sehen und daraus abgeleitet eine Ressourcenverteilung für die Errei-

chung oder Durchsetzung eigener Ziele priorisiert“ (S. 177). Jeder folgt unausgesprochen „seinem selbst gebildeten, eigenen Leitbild“ (S. 173). Narrative können entweder bewusst zur Lenkung oder zur Täuschung anderer genutzt werden oder eher unbewusst bleiben. Sie können aber auch leicht zum eigenen Nachteil vernachlässigt werden. Deshalb bedarf es einer Art Verstehen, das über das reine Faktenwissen hinausgeht (Kneissl, S. 78).

Unabhängig von der Begriffsquadriga setzten die Panels jeweils eigene Themenschwerpunkte.

Im Mittelpunkt des geisteswissenschaftlich ausgerichteten Panels „Religion, Werte und Interkulturalität“ stand die Begrifflichkeit der Quadriga selber. Dies ist insofern für die weitere Betrachtung sinnvoll, da die Findung und Bedeutung der Begriffe von Strategie ein geisteswissenschaftliches Moment ist, auch wenn bei deren Anwendung, d.h. beim Strategiedenken, andere fachliche Orientierungen vorherrschen können (Schuh, S. 319). Dabei ist auch der methodisch-analytische Zugang aus dem Social-political-culture-Ansatz zu sehen, denn unterschiedliche Akteure haben zu den anderen Akteuren eine bestimmte Grundeinstellung, je nach Nation, Kultur oder Gesellschaft, wodurch ihr Verhalten in bestimmten Situationen beeinflusst wird (Pankratz S. 336-342).

In den Panels Militärwissenschaft (S. 300-317), Strategieberatung (S. 343-360) und Strategische Kommunikation (S. 361-378) wurden die Politikfelder Militär, Sicherheitsexekutive, hoheitliche Verwaltung und privatwirtschaftliches Unternehmertum zwischen „Beratungspraktikern“ verschiedener Nationalitäten diskutiert. Wo überall Gefahren für weitere Entwicklungen aufbrechen können, wird deutlich am Thema Hybridität. Diese ist nicht nur in Form von hybriden Kriegen zu bedenken. Hier wird aber auch deutlich, dass das Militärische eine Art Steuerinstanz für den Lehrgegenstand „Strategisches Denken“ noch für einige Zeit übernehmen kann, bis Strategiedenken allgemein in Lehre und Forschung etabliert sein wird (S. 300-317). Die Vergleichbarkeit der Organisation von Militär und Wirtschaft ist evident. Doch es gibt (s. Holler S. 267) eine spezielle Ausbildung für Führungsverfahren und Informationsgewinnung im Wirtschaftskrieg bisher nur in Frankreich. D.h. auch, die vielfältigen Herausforderungen und Möglichkeiten eines Wirtschaftskrieges, wie wir ihn seit wenigen Jahren erleben, sind wissenschaftlich noch nicht erfasst. So regt Mantovani auch eine interdisziplinäre Methodik und die Kombination verschiedener Analysedimensionen wie Geschichte, Politik, Militär, Ökonomie Kultur und Natur an.

Im Panel Natur- und Technikwissenschaften zeigt sich die rasante Entwicklung in den letzten 150 Jahren, besonders seit dem 2. Weltkrieg. Hier sei ein nachhinkend-vorrausschauender Ansatz zu fordern, international, interdisziplinär wie fachübergreifend; an die Stelle einer Disziplinorientierung müsse eine Problemorientierung treten (Hinterstoisser S. 282-284).

Das Panel Strategie und Medizin, Biologie, Biotechnologie, Biogenetik und synthetische Genetik zeigt im Zusammenhang mit Biowaffen ein neues Einfalltor auf. Ob das Risiko in möglichen Fehlern von Entwicklungen im medizinischen Bereich liegt, im Missbrauch oder gar im gezielten Einsatz als Waffe z.B. bei Bioterrorismus, das alles ist nicht mehr Fiktion (Knoepffler S. 292-295).

Beim Panel zu Geostrategie und maritimen Aspekten wurden die sicherheitspolitischen Risiken durch den Wegfall von räumlicher Distanz behandelt. Das Problem der „gefühlten Sicherheit“ stellt sich nicht mehr die Frage des „ob“ der Verwundbarkeit einer Gesellschaft durch Krieg, sondern (nur) die des „wie“ deren Ausmaßes. Das verdeutlichten Vorträge wie z.B. die Analyse der österreichischen Außenministerin Karin Kneissl zur politischen und besonders außenpolitischen Situation (S. 75-81) oder Matlarys Reflexionen zur strategischen Situation 2014 in Europa/in der NATO unter der Fragestellung: Kann Europa angesichts des Russischen Revisionismus strategisch handeln? (S. 43-74), oder die militärstrategischen Betrachtungen zur erweiterten Nordflanke der NATO im Ostseeraum (Neretnieks S. 83ff.), die derzeitige NATO-Strategie in ihrer offensichtlichen Hilflosigkeit gegenüber Russland seit der Krim-Annexion 2014 (Peischel S. 107 ff.), Khandares Betrachtung zu Chinas „Vision“ und dessen Politikentwicklung (S. 152-158) und Gegners Vortrag über die hybriden Bedrohungen im maritimen Bereich (S. 230-236).

Eher zwischen den Vorträgen stellte sich die Frage nach der (Aus-)Bildung zum Strategiedenken. Dabei sind drei Ansätze zu unterscheiden: 1. Die wissenschaftlich-akademische Ausbildung auf der Ebene der Theorieentwicklung zum Strategiedenken; 2. die Ausbildung auf der Ebene der praktischen Gestaltung und Anwendung von Strategien im Alltag und 3. die Gestaltung im gesellschaftspolitischen Raum. Auf jeder dieser drei Ebenen geht es um Bildung als „strategische Ressource“. Dabei unterscheiden sich die Möglichkeiten der Vermittlung grundsätzlich.

Die vorliegenden drei Dokumentations-Bände von 2016, 2017 und nun auch 2018 markieren einen Aufbruch in dem bisher weitgehend vernachlässigten Feld der Strategie. Es hat sich gezeigt, dass eine vorgegebene Ordnung mit Vorträgen und Panels allein nicht sinnvoll wäre. Vielmehr hat sich ein unter einer Vielfalt von Aspekten gleichzeitiger und multidimensionaler Ansatz auf drei Behandlungsebenen entwickelt und bewährt: Die Vorgabe der Begriffsquadriga als Leitfaden und die interdisziplinären Fachgebietsschwerpunkte in den Panels und der Praxisbezug aus Sicht konkreter strategischer Handlungsfelder. Ein derart multipolarer Ansatz entspricht dem Strategiedenken an sich. Die Wiener Strategiekonferenz hat mit diesem internationalen und multidisziplinären Format des Strategiedenkens im deutschsprachigen Raum eine Vorreiterrolle übernommen. Wünschenswert ist die weitere Öffnung der Konferenz zu anderen Handlungsfeldern im nationalen wie internationalen Bereich sowie zu weiteren wissenschaftlichen Disziplinen.

Prof. Dr. Claus Freiherr v. Rosen