
# Science Peace Security '23

## Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research

CHRISTIAN REUTER, THEA RIEBE, LAURA GUNTRUM (EDITORS)

Preprint Version 2023-09-12

**Science Peace Security ’23**
Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research
Christian Reuter, Thea Riebe, Laura Guntrum (Editors)
TUprints, Darmstadt, 2023

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

# Table of Contents

**PREPRINT VERSION 2023-09-12 ..... 1**

**EDITORIAL AND KEYNOTES ..... 7**

Science Peace Security '23: Editorial of the Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research ..... 8

Keynote: The Politics of Emerging and Destructive Technologies: How to Prepare the Ground for Arms Control and Disarmament ..... 10

Keynote: From Bytes to Action: the Promise and Perils of Digital Technologies in Combating Corruption Worldwide ..... 11

**I (NUCLEAR ARMS CONTROL) ..... 12**

[2582] A deep learning approach for safeguards-relevant change detection by combining Sentinel-1 and Sentinel-2 images ..... 13

[8687] Irreversibility of Nuclear Disarmament: long-term, latency-based approaches for monitoring and risk management ..... 14

[9362] Reconstructing nuclear histories – a field study ..... 15

**II (GEOPOLITICS OF INFRASTRUCTURES) ..... 16**

[7162] Critical Energy Infrastructures: geopolitical vulnerabilities and strategies of securitization ..... 17

[7951] Solar geopolitics - the shining rise of India ..... 18

[2905] What drives state-led Internet shutdowns? Utilizing a machine learning approach for prediction and factor exploration ..... 19

**III (AUTONOMOUS SYSTEMS AND HUMAN-MACHINE INTERACTION) ..... 20**

[9191] Human augmentation or augmented machines? Military paradigms and the problem of the unmanned/manned dichotomy in AI-assisted technologies ..... 21

[8154] Unveiling the Hidden Bias: Examining Intersectional Discrimination in Lethal Autonomous Weapon Systems and its Consideration during Arms Control Talks ..... 22

[7407] Stopping "killer robots": Cross-national experimental evidence on the relative strength of pro-regulation arguments ..... 23

**IV (CIVILIAN INFRASTRUCTURE AND PROTEST) ..... 24**

[7630] Civil Protection in a State-Centric Risk Culture - The Role of Warning Apps in Germany....25

[1095] Protest and technology in the national strike of 2021 in Cali, Colombia through an intersectional perspective ....27

[1410] Inside China's Cyber System – Ambitions, Actors, Instruments ....28

**POSTER ....30**

[2355] Unmasking Digital Threats in the Pursuit of Human Rights and Environmental Defense in La Guajira and Cesar, North Colombia ....31

[1195] NewSpace and proliferation risks – mapping the regulation of commercial space activities ....33

[7497] Global Critical Infrastructures....34

[6777] Information Warfare on Twitter: Disinformation in the Russo-Ukrainian War ....35

[8883] Supporting Victims of Hate Speech: The Role of German Reporting Centers as Intermediaries with Counseling Centers, Authorities and Digital Platforms ....36

[4906] Political Violence, Populism and Social Media in Brazil....37

[1533] Chemical Weapons Investigation Mechanisms in Syria: Scientific Methods and Standard of Proof ....38

[2914] Briar: Secure Messaging for Citizens and Activists during Internet Shutdowns ....39

[8459] The 70:20:10 framework for regulatory compliance trainings. An opportunity for CBRN-WMD awareness trainings?....40

[6245] Critical infrastructure and outer space: geopolitics, vulnerability, risk reduction and arms control....41

[2136] Oculta: Hidden Secure Communication via WhatsApp and Co. ....42

[1311] On the Origin of Gender Bias in Face Recognition....43

[5009] Investigating the contribution of website operators to the emergence and remediation of privacy risks ....45

[2024] Technology Assessment of Dual-use ICTs – How to Assess Diffusion, Governance and Design ....46

**DIALOGUE PANEL: ICT4PEACE - THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGY IN (DIGITAL) PEACEBUILDING....47**

[7623] Digital Peacebuilding – Potentials and Challenges of ICTs in Peacebuilding Efforts ....48

[2258] Postcolonial Perspectives on Digital Peacebuilding: Moving from «Inclusion» to «Agency» ....49

[2657] Digitalization and e-government in the lives of urban migrants: Evidence from Bogotá ....50

[4159] The Ethics of PeaceTech: Ownership and Outsourcing of Risk in Distributed Systems ....51

[1470] An intersectional feminist lens on digital peacebuilding ....52

**V (DUAL-USE AND TECHNOLOGY ASSESSMENT) .... 53**

[4387] Adjusting the Wheel: Ethical Deliberation as a Method for Dual-Use Assessment in the ICT Development Process ....54

[9033] Missile Defenses for Europe: Computer Modeling and Analysis ....55

[4198] The Impact Of Quantum Technologies On Deterrence, Arms Control, Nonproliferation, and Verification ....56

**VI (CYBER OPERATIONS) .... 57**

[3174] The Normative Power of the Factual: How State Practice Shapes Understandings About Direct Public Political Attribution of Cyber Operations ....58

[514] The Role of Cyber Ranges within European Cybersecurity Strategy: A Primer ....59

[8638] International Cybersecurity and Peace Research: Challenges at the Interception of Peace and Conflict Research and Cyber Security Research ....60

**VII (BIOLOGICAL, CHEMICAL AND CONVENTIONAL WEAPONS) .... 61**

[7088] Biological Weapons: A Harm Potential Assessment ....62

[551] Taking biological security education forward and building up an international biological security education network ....63

[4167] Access to Information about Chemical Weapon Attacks: Increasing Resilience in Kurdistan ....64

[325] Small space launch vehicle technology in the NewSpace era: A new challenge for missile non-proliferation? ....66

**VIII (TECHNOLOGY POLITICS AND STRATEGIES) .... 67**

[5183] Narratives of "Tech Wars": Technological Competition, Power Shifts and Conflict Dynamics Between the US, China and the EU ....68

[2698] The Promise of Track-Two Diplomacy Amidst US-China Tech War ....69

[2282] Trust in AI: Producing Ontological Security through Governmental Visions ....70

[9728] Maritime Critical Infrastructures Protection: Technical and Political Approaches Beyond the Military ..... 71

**WORKSHOP AND CLOSING PANEL ..... 72**

[1735] Thinking about the future: Nuclear verification in a complex world ..... 73

[7486] New military technologies – fundamental challenges to the international system? . 75

# Editorial and Keynotes

# Science Peace Security ’23: Editorial of the Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research

Christian Reuter, Thea Riebe, Laura Guntrum (PEASEC, TU Darmstadt).

*Motivation*

As the most important science policy advisory body in Germany, the German Council of Science and Humanities published its recommendations for the further development of peace and conflict research in July 2019. In it, the Council points to an urgent need for action to strengthen scientific and technical peace and conflict research, which is now structurally too precarious in Germany to meet the massive demand for advice from policymakers: "In order to maintain the necessary scientific and technical research and expertise in Germany in the long term, however, the Council considers the institutional development and expansion of this sub-field of peace and conflict research [...] to be indispensable and recommends that the Federal Government and the Länder become active in this area". Furthermore, the panel calls on the recently established research institutions on cybersecurity to also increasingly take up issues of peace and conflict research.

The Technical University of Darmstadt was cited as a positive example of the permanent establishment of this discipline at a university, the venue for the inaugural event for the new SCIENCE - PEACE - SECURITY 2019 conference series, and after a virtual stop in Aachen in 2021, the conference series returned to Darmstadt in 2023 before moving to Jülich in 2025: scientists will present current research on interdisciplinary challenges and approaches to solutions on issues of international security, peace-building as well as transparency and confidence-building measures, arms control, disarmament and conflict management at the TU Darmstadt.

*Aim*

The conference Science - Peace - Security '23 will take place from September 20 to 22, 2023 at the Technical University of Darmstadt. It is dedicated to the transformation of technologies, their role in wars and conflicts, and questions of arms control. On September 21, a public dialogue panel will invite civil society organizations in particular to promote exchange between research and practice. The general public is also invited to this event. The English-language conference is organized by TraCe, a Hessian BMBF research network on transformations of political violence, by the DFG Collaborative Research Center CROSSING and by the research network Natural Science, Disarmament and International Security FONAS.

*Technological transformations in armed wars and conflicts*

Around 100 participants are expected to attend the three-day scientific conference to discuss current and future challenges in the field of technical peace and conflict research in around 40 lectures, workshops, discussion rounds and panels. Artificial intelligence, unmanned weapons systems, missile and space technologies, (nuclear) arms control, regulation of biological and chemical weapons, information

technologies for the surveillance and repression of civilians, (civilian) critical infrastructures, digital peacebuilding, human-machine interaction, dual-use and cyber-attacks as well as corresponding technology and security policies: the spectrum of the programme is broad and reflects overall societal discourses in the light of a changing global security landscape.


About TraCe:

TraCe is an association of the Leibniz Institute for Peace and Conflict Research (HSFK) and the universities of Frankfurt, Gießen, Marburg and Darmstadt. It bundles Hessian peace and conflict research and is funded by the Federal Ministry of Education and Research (BMBF). From April 2022 to March 2026, more than 30 researchers in the network will use various disciplinary and methodological approaches to research the effects of global developments on political violence. The results will serve to further develop social and political discourse. www.trace-center.de

About CROSSING:

CROSSING's goal is to develop cryptography-based security solutions to strengthen trust in new next-generation computing environments. The solutions developed should meet the efficiency and security requirements of the new environments and implement them soundly. The aim is to create ease of use for different groups, including developers, administrators and end users. To achieve this goal, CROSSING researchers from complementary fields such as cryptography, quantum physics, systems and software engineering are working together. https://www.crossing.tu-darmstadt.de

About FONAS:

The Research Network on Science, Disarmament and International Security (FONAS) emerged from a collaboration of interdisciplinary research groups, and aims to promote scientific work on issues of disarmament, international security and international peace using mathematical, natural or technical scientific methods - taking into account interdisciplinary references - in research, teaching and the public communication of findings. http://www.fonas.org

TraCe meets SPS:

Already since 2019, the Chair of Science and Technology for Peace and Security (PEASEC) at TU Darmstadt has been hosting the interdisciplinary conference Science - Peace - Security '23 together with the Research Network for Science, Disarmament and International Security (FONAS). In 2019 it took place in Darmstadt, in 2021 in Aachen. Through PEASEC's membership in the BMBF-funded regional research centre Transformations of Political Violence (TraCe), founded in 2022, as well as in the Collaborative Research Centre CROSSING, SPS'23 takes up overarching guiding questions and topics of these research groups.

# Keynote: The Politics of Emerging and Destructive Technologies: How to Prepare the Ground for Arms Control and Disarmament

Oliver Meier (European Leadership Network).

*Abstract*

Many governments are using and misusing emerging technologies to gain military and strategic advantages. A critical analysis of the structures, actors and motivations driving such qualitative arms dynamics is important. It helps to identify political opportunities to reduce risks for peace and security resulting from the integration of emerging technologies into warfare. Focusing on the role of Germany, the talk will use some current examples of military innovations in nuclear weapons-related areas to highlight opportunities for scientists and others to shape political decision-making and prepare the ground for arms control and disarmament.

# Keynote: From Bytes to Action: the Promise and Perils of Digital Technologies in Combating Corruption Worldwide

Alice Mattoni (University of Bologna, Political Sciences, Social Movement).

*Abstract*

Through compelling real-world case studies and stories of anti-corruption activism from around the world, the talk sheds light on how grassroots movements are using digital technologies to promote integrity in their societies and pave the way for a more accountable world. It explores the transformative potential of digital technologies in the grassroots fight against corruption. It presents a typology of anti-corruption technologies, discusses their opportunities and examines the challenges they pose to civil society organisations. It also analyses their impact on democracy and civic engagement, highlighting the democratic ideals embedded in these technologies and their role in redefining citizenship and promoting active participation in society.

# I (Nuclear Arms Control)

# [2582] A deep learning approach for safeguards-relevant change detection by combining Sentinel-1 and Sentinel-2 images

Lisa Beumer (Forschungszentrum Jülich GmbH) and Irmgard Niemeyer (Forschungszentrum Jülich GmbH).

*Abstract*

Earth observation through satellite imagery has historically played a unique role for the implementation and verification of nuclear non-proliferation, arms control and disarmament treaties. Nowadays, huge volume of satellite images, including different Earth Observation mission data made available, inter alia, by the European Copernicus program Copernicus, are constantly acquired. With the development and implementation of deep learning algorithms in change detection, many of these existing models have been designed to process optical imagery. Although, several studies have shown that synthetic aperture radar (SAR) data, e.g., provided by Sentinel-1, also contains unique information about image features and is less affected by weather and atmospheric conditions.

Since labeled data is scarce and expensive to produce, we propose an unsupervised framework which uses optical and SAR images jointly to achieve to detect generic but relevant changes of nuclear related fuel sites. The framework is composed of three modules. The first one is extracting the bands of interest and resampling them to the same spatial resolution. Then all images are co-registered and sorted chronologically. The last module computes pairwise change detection maps of the time-series. Therefore, features are extracted separately to efficiently use information from both data sources using an unsupervised approach based on stacked autoencoders. By reconstructing the image from a compressed representation, the network is forced to capture the main features of the image. Finally, the features are then combined by convolutional operations.

By applying this methodology, the accuracy of change detection can be improved and could therefore add a big value in the safeguard's verification process.

# [8687] Irreversibility of Nuclear Disarmament: long-term, latency-based approaches for monitoring and risk management

Alberto Muti (VERTIC), Grant Christopher (VERTIC) and Andreas Persbo (Open Nuclear Network).

*Abstract*

Irreversibility in the context of nuclear disarmament has been acknowledged as a continuum rather than a state of disarmament with no possibility of reversal. Identifying what factors contribute to the 'degrees' on the continuum of irreversibility, and the practical ways to implement irreversibility measures in the context of a nuclear disarmament or denuclearization campaign remains understudied.

This paper will reframe the concept of irreversibility in nuclear disarmament and denuclearization to focus on long-term management and monitoring of states' latent nuclear capabilities and their associated risks. To do so, the paper will leverage existing understandings of nuclear latency to bring into focus how states approach – and potentially cross – the threshold of producing nuclear weapons.

The proposed framing aims to open up the concept of irreversibility to analysis using practical, actionable categories such as risk, latent capability, and, possibly, signals of intent. This approach would shift discussions on how to achieve irreversibility in nuclear disarmament and denuclearization from the broader goal of "making rearmament impossible" to more defined and pragmatic goals of increasing both the cost – in both time and resources – and the probability of detection of any attempt to pursue rearmament.

# [9362] Reconstructing nuclear histories – a field study

Sophie Kretzschmar (Nuclear Verification and Disarmament, RWTH Aachen University), Max Schalz (Nuclear Verification and Disarmament, RWTH Aachen University) and Malte Göttsche (Nuclear Verification and Disarmament, RWTH Aachen University).

*Abstract*

Reconstructing how much fissile material was produced in nuclear facilities could become a key element in the verification of future arms control or disarmament agreements. The past production of plutonium can be modeled with reactor simulations, using information on both reactor design and operating history. That information is typically provided by the inspected state and must be independently verified. In a first step, the available documentation of the reactor program can be thoroughly examined, for instance by studying its self-consistency. In a second step, forensic measurements, e.g., of samples from inside the reactor core, can be used to verify the documentation. For both these methods, questions remain, especially related to the practical application: How can one handle the potentially large amount of archived operating-history documentation? How to deal with gaps in the documentation? How can the document analysis be effectively combined with forensic measurements? To answer those questions, systematic approaches need to be developed.

We explore a real-world scenario with the former nuclear research program from Karlsruhe, Germany, for which we gained access to the archives containing documentation of the operational histories and facility designs. The nuclear research program included a pilot reprocessing plant and the heavy water reactors FR-II and MZFR, which were operated between 1961 and 1984. While the program was used for civilian purposes only, the fact that the reactors were moderated by heavy water makes them ideal candidates for this study as this type of reactor is elsewhere used to produce plutonium. This presentation will show first results on how the documentation of a past nuclear reactor program can be used to develop and test approaches to nuclear archaeology.

# II (Geopolitics of Infrastructures)

# [7162] Critical Energy Infrastructures: geopolitical vulnerabilities and strategies of securitization

Matteo Gerlini (University of Siena - Chair of International Nuclear Security Education Network) and Fabio Indeo (University of Siena - NATO Defence College Foundation).

*Abstract*

The protection of Critical Energy Infrastructures (CEI) represents a key priority for both global energy suppliers and consumers in order to preserve the energy security condition, namely “the uninterrupted availability of energy sources at an affordable price”. As a matter of fact, the high relevance of energy in the global economy, CEI infrastructures have progressively become an attractive target for terrorist attacks – both physical and cyber attacks – aimed at provoking energy disruptions and economic damages, highlighting the condition of high vulnerability of the affected country in security terms. In the last years, mainly Middle East producers and Ukraine have suffered terrorist attacks aimed to destroy CEI, but all CEI - included the RES-based infrastructures such as solar plants, wind farms and hydrogen industries which will be the cornerstone of the energy transition - represent a vulnerable asset which is necessary to protect in order to preserve the geopolitical stability based on a condition of energy security without disruptions. Nuclear power plants have the added security value to be target for radionuclear terrorist attacks, beside the energy supply chain's disruption. The main aim of this proposal is to evaluate the existing threats to CEI and how efficiently prevent, contain and downplay the negative impact on the global energy security: considering the sharing interest of both energy suppliers and consumers to preserve the regularity of the energy flows to the markets, a joint engagement which could be profitable to improve the security conditions and to avoid dangerous geopolitical unbalances.

# [7951] Solar geopolitics - the shining rise of India

Markus Lederer (TU Darmstadt), Jens Marquardt (TU Darmstadt), Shyamaasree Dasgupta (IIT Mandi) and Pooja Sankhyayan (IIT Mandi).

*Abstract*

For the last decade, India has witnessed a massive increase in renewable energy development, particularly in solar photovoltaics. The country has not only a massive theoretical capacity of 748 GW, but it has already installed more than 64 GW (https://mnre.gov.in/the-ministry/physical-progress). This is short of its 100 GW goal that it had hoped to achieve by the end of 2022, but compared to other developing countries and considering that the initial goal of 2022 was 20 GW, the growth in solar is enormous. The size of installations ranges from millions of solar lanterns and solar cookers for rural households to rooftops for urban areas and large solar parks that provide power for household as well as industrial use. The growing social science literature on India's renewable energy policies has primarily focused on the economics of solar, development impacts, policy designs, and implementation issues such as equity and justice. Also, land availability has recently become a hot topic due to trade-offs between solar power and primarily agricultural use. Except for some economists who have lamented the dependence of India on Chinese products, the academic debate on India's solar power development has treated the issue as a purely domestic story. Our paper argues that there is also a story of foreign policy to be told and thus takes a geopolitical perspective on the shining rise of solar in India. Geopolitical analyses of renewable energies have so far had a very Eurocentric perspective dealing with issues of the dependence of the West on critical raw materials from China or the competitive subsidies for renewables in the EU and the US. Some have also taken a more critical geopolitical perspective analyzing ideological elements of the growth in renewables. These insights can also help to understand the situation in India and will thus be taken up for analyzing the Indian solar revolution. We focus mainly on the competition with China, as India's solar ambition and policy have – so we argue – been inspired by China being a first mover in the region.

# [2905] What drives state-led Internet shutdowns? Utilizing a machine learning approach for prediction and factor exploration

Fabiola Schwarz (Technical University of Munich).

*Abstract*

With the often-cited rise of digital authoritarianism, the popularity of targeted surveillance as well as censorship techniques such as blocking websites, throttling bandwidth, and deep packet inspection has skyrocketed. The most extreme form of censorship is the so-called Internet shutdown or kill-switch, mostly observed in conjunction with human rights violations. In the last years, the numbers of such Internet shutdowns and of countries deploying those have been steadily growing, especially on the African continent. Their far-reaching impact on civil society requires a better understanding of and preparation for this form of political violence. Although a common phenomenon noticed to accompany intra-state conflicts, elections, and protests, we know comparatively little about the driving factors of Internet shutdowns, let alone about how to foresee this form of digital repression. Therefore, this study asks two questions: How can the deployment of Internet shutdowns be predicted? And which factors are most important in doing so? This is the first paper to forecast Internet shutdowns. To do so, I synthesize existing research into a conceptual framework which comprises two levels, a structural and a dynamic model to explain Internet shutdown deployment in Africa. Having collected over 100 predictors, I train a random forest algorithm to evaluate prediction capacity and derive the most important factors for Internet shutdown forecasts. The country-week level dataset entails dynamic variables such as protest, elections, and violent conflict as well as structural factors, like economic, political, and demographic aspects of a country. Data on Internet shutdowns comes from the #KeepItOn coalition published by Access Now. First results show that pure event-based and pure structural models perform less well in predicting Internet shutdown onset than a joint model. It is a specific combination of event-based and structural variables that explain most of the model's variance. Among those are Internet censorship practices, violent protests, elections, academic surveillance, and population size. These findings outline avenues for future research on causal links between single factors and the deployment of Internet shutdowns. This study thus contributes to further theory-building in the wide research area of digital authoritarianism and, more specifically, in the field of Internet shutdowns and censorship practices.

# III (Autonomous Systems and Human-Machine Interaction)

# [9191] Human augmentation or augmented machines? Military paradigms and the problem of the unmanned/manned dichotomy in AI-assisted technologies

Christoph Ernst (Rheinische Friedrich-Wilhelms-Universität) and Thomas Christian Bächle (Alexander Humboldt-Institut für Internet und Gesellschaft).

*Abstract*

The ideas of network-centric warfare, cyber and information warfare, human-machine teaming in combat, the enhanced soldier (with the “Infanterist der Zukunft” being the German army rendition of this concept) and autonomous weapons are among the latest military development goals. They are tied to larger strategy- and technology-related paradigms, which are often strongly calibrated along the lines of machine agency, human control and the unmanned/manned dichotomy. Yet, recent debates on how developments such as artificial intelligence, robotics and automation are bound to fundamentally change military practices and future warfare tend to overlook or downplay the deep entanglement of autonomous (weapon) systems with the (long-standing) idea of human augmentation.

As will be argued, the military paradigm of augmentation and the subsequent technological developments call into question the seemingly self-evident dichotomy of manned/unmanned systems. In order to establish an approach that rethinks the role of the human (agent) in human/machine interactions, we will give a brief overview over existing discussions of human-computer-interaction in the context of cognitive anthropology and media theory. Important theories and terminologies like, among others, "distributed cognition" (Hutchins) will be explained within the context of an approach which focusses primarily on the issue of interfaces as media and relays for the distribution of agency between human and machine actors. Providing insights for further research with theoretical frameworks like actor-network theory or systems theory this shift in understanding of the sociotechnical relationship presents a new perspective on questions of regulation and control of said weapons systems.

# [8154] Unveiling the Hidden Bias: Examining Intersectional Discrimination in Lethal Autonomous Weapon Systems and its Consideration during Arms Control Talks

Anja-Liisa Gonsior (PEASEC, TU Darmstadt).

*Abstract*

The development of lethal (semi-)autonomous weapon systems (LAWS) is increasingly gaining momentum and the topic has been discussed between member states, civil society and experts in the Group of Governmental Experts (GGE) on LAWS within the UN Convention on Certain Conventional Weapons since 2013. While the debate initially focused on definitional issues of LAWS, the forum is currently dominated by technical and legal issues, which is also reflected in the corresponding academic discourse. On the other hand, civil society actors have also significantly influenced the debate, not least the Campaign to Stop Killer Robots, which was instrumental in initiating the negotiation framework. One of the central strands of argumentation of these civil society actors focuses on an intersectional perspective that, among other things, draws attention to biases in technologies and applications, and seeks to introduce and strengthen these perspectives in the GGE on LAWS. Analysis of over 50 GGE documents and interviews with several experts show that - with regard to intersectionality - especially the concepts of gender and race are taken into account in the GGE discussions, albeit with only little weight. However, NGOs were able to influence the overall debate and introduce new topics by linking to more established discourses in the debate, such as legal or technical discourses.

# [7407] Stopping "killer robots": Cross-national experimental evidence on the relative strength of pro-regulation arguments

Ondřej Rosendorf (Institut für Friedensforschung und Sicherheitspolitik (IFSH) an der Universität Hamburg).

*Abstract*

The advent of autonomous weapons, also known as "killer robots", presents one of the most significant and controversial developments in contemporary military affairs. Previous studies suggest that there is considerable public opposition to these weapon systems, but our knowledge of what is driving these unfavorable attitudes remains limited. This poses a challenge for policymakers and disarmament advocates seeking to mobilize the public in favor of regulatory measures. Experts use a variety of arguments, including those based on the unethical nature of autonomous weapons, their negative implications for international security, problems with compliance with international humanitarian law, and technical limitations. At present, however, we do not know which of these arguments is most convincing to the public. This paper aims to explore cross-national differences in the perceived persuasiveness of various arguments in favor of regulating autonomous weapons through an experimental survey. To explore these differences, we will randomly assign our respondents to one of the commonly used ethical, security, legal, or technical arguments and then ask them how much they approve or disapprove of preventive regulation of autonomous weapons. The results can help policy-makers and disarmament advocates in crafting more effective pro-regulation messaging.

# IV (Civilian Infrastructure and Protest)

# [7630] Civil Protection in a State-Centric Risk Culture - The Role of Warning Apps in Germany

Jasmin Haunschild (PEASEC, TU Darmstadt).

*Abstract*

Warning apps offer a mobile crisis alert system with access to multi-media content, reliable agency information and options for personalization (Hauri et al., 2022; Reuter & Kaufhold, 2018). These apps aim to ensure situational awareness during crises and provide preventive and response advice. In contrast to everyday applications that are also used in crises (Tan et al., 2017), warning apps are specifically designed for disaster purposes and have specific design requirements, geared at simplicity, trustworthiness, timeliness and reliability (Bonaretti & Fischer, 2021; Tan et al., 2020). Despite their potential, low usage numbers across European countries (Hauri et al., 2022) indicate a lack of awareness or prioritisation, especially since warning apps are generally regarded as important and useful (Haunschild et al., 2022; Kaufhold et al., 2020). Regarding the individual contribution to crisis preparedness, Germany is repeatedly found to be an intriguing case where a general interest in crisis information can be found, while the readiness to prepare for disasters is low. Even though less than 90% of Germans feel informed or very informed about disasters and less than 80% feel prepared or well prepared, only 21% plan to prepare quite a lot or a lot (Appleby-Arnold & Brockdorff, 2018). Research indicates that in Germany, this may be due to a state-centric risk culture, in which people feel that the state takes care of emergency management and personal responsibility for preparedness is therefore small (Cornia et al., 2016; Reuter & Kaufhold, 2018). The analysis of German warning apps indicates that state agencies are fostering this state-centric risk culture. Here, preparedness information is side-lined and relegated to a non-interactive menu item. Topics and functions related to security are largely neglected. The presentation shows the state of research on warning apps and potentials for enhancing their utility for citizens and for security related crises. First, the results of representative and qualitative surveys, and usage trends over time are presented. Then, strategies for enhancing the usefulness of warning apps and increasing usage and results from experiments are shown. Finally, further potentials for enhancing the use of warning apps are discussed, with reference to the Finnish warning app and the Ukrainian app Diia, which has taken on unforeseen functions during the war. Overall, this research sheds light on the potential of warning apps for civil protection and crisis preparedness, providing valuable insights for their future development and implementation.

## Sources

Appleby-Arnold, S., & Brockdorff, N. (2018). Culture and disaster risk management—Synthesis of citizens' reactions and opinions during 6 Citizen Summits: Romania, Malta, Italy, Germany, Portugal and the Netherlands. CARISMAND Report.

Bonaretti, D., & Fischer, D. (2021). Timeliness, trustworthiness, and situational awareness: Three design goals for warning with emergency apps. Forty-Second International Conference on Information Systems, 1–17.

Cornia, A., Dressel, K., & Pfeil, P. (2016). Risk cultures and dominant approaches towards disasters in seven European countries. Journal of Risk Research, 19(3), 288–304. https://doi.org/10.1080/13669877.2014.961520

Haunschild, J., Kaufhold, M.-A., & Reuter, C. (2022). Perceptions and Use of Warning Apps—Did Recent Crises Lead to Changes in Germany? Proceedings of Mensch Und Computer 2022, 25–40. https://doi.org/10.1145/3543758.3543770

Hauri, A., Kohler, K., & Scharte, B. (2022). A comparative assessment of mobile device-based multi-hazard warnings: Saving lives through public alerts in Europe. Risk and resilience Report, Center for Security Studies. https://doi.org/10.3929/ethz-b-000533908

Kaufhold, M.-A., Haunschild, J., & Reuter, C. (2020). Warning the public: A survey on attitudes, expectations and use of mobile crisis apps in Germany. Proceedings of the European Conference on Information Systems (ECIS). http://www.peasec.de/paper/2020/2020%5FKaufholdHaunschildReuter%5FWarningthePublic%5FECIS.pdf

Reuter, C., & Kaufhold, M.-A. (2018). Fifteen years of social media in emergencies: A retrospective review and future directions for crisis informatics. Journal of Contingencies and Crisis Management (JCCM), 26(1), 41–57. https://doi.org/10.1111/1468-5973.12196

Tan, M. L., Prasanna, R., Stock, K., Doyle, E. E. H., Leonard, G., & Johnston, D. (2020). Modified usability framework for disaster apps: A qualitative thematic analysis of user reviews. International Journal of Disaster Risk Science, 11(5), 615–629. https://doi.org/10.1007/s13753-020-00282-x

Tan, M. L., Prasanna, R., Stock, K., Hudson-Doyle, E., Leonard, G., & Johnston, D. (2017). Mobile applications in crisis informatics literature: A systematic review. International Journal of Disaster Risk Reduction, 24, 297–311. https://doi.org/10.1016/j.ijdrr.2017.06.009

# [1095] Protest and technology in the national strike of 2021 in Cali, Colombia through an intersectional perspective

Miyerlandy Cabanzo (Universidad Tecnológica del Chocó).

*Abstract*

One of the biggest and longest strikes in recent years in Colombia occurred between April and June, 2021. Cali, in the southwest of Colombia, was the main focus of the violent protests around the country. Technology was used under two perspectives: first, to organize and support people who protested or were against protests. Secondly, to sabotage the mobilizations. In this context, the feminist, women's and LGBTIQ+ movement of Cali spread a wide range of actions to protest. In consequence, the questions that guide this research proposal is how women and LGBTIQ+ persons used technology to protest? Did they use it to produce a pacific or a violent protest? How other women and LGBTIQ+ persons supported or were against to both protest? What is the meaning of technology? What happened to the technology used after the national strike ended? These questions will be answered with a qualitative approach through interviews and document and bibliographic review. Black women and trans women organizations such as Casa del Chontaduro and Twiggy Fundación who protested in favor of the national strike and against the police violence, and female inhabitants from the southwest of Cali, who protested against the national strike will be considered in the research process. They all were key in this period. This concrete mobilization in Cali may explain the relationship between protest, technology and intersectionality.

# [1410] Inside China‘s Cyber System – Ambitions, Actors, Instruments

Helene Pleil (Digital Society Institute, ESMT Berlin).

*Abstract*

China's increasing influence is having a profound impact on global security and democracy (Stoltenberg, 2022): The U.S. National Security Strategy identifies China as a systemic rival in the context of strategic competition (White House, 2022a). At this time, Germany is working on a new China strategy - it is suspected that the tone toward China will become more critical. Currently, however, depending on the policy area, China is simultaneously a cooperation partner, negotiating partner, economic competitor, and systemic rival for European countries (European Commission, 2019).

In the digital era, geopolitical conflicts are shifting to cyberspace. Consequently, new technologies and the digital realm have become a significant arena of competition between the United States and China as major world powers, as exemplified by the U.S. "Chips Act" (White House, 2022b). Technology is no longer merely a domain of opportunities and possibilities; it has evolved into a "battleground for control, values, and influence" (Gallardo/Fleming, 2022).

In President Xi's vision for China, cyberspace plays an essential strategic role: China aspires to become a cyber (great) power and to take technological leadership (Creemers, 2021; Voo/Creemers, 2021; Rühlig et al., 2022). The ambitions in this context span over the full spectrum of political, economic, and social issues, motivated by a variety of reasons (Chang, 2014). To achieve these objectives, China employs various strategies: Technological standardization and dominance in new technologies, e.g., AI and 5G, are strategically instrumentalized, to influence actors and promote international norms that serve Chinas interests (Fischione et al., 2022; Björk/Rühlig, 2022). In addition, technological self-reliance is sought to minimize own vulnerabilities (Cary, 2021). Various global platforms, including the UN, as well as major economic projects, such as the "digital silk road," also serve as venues to expand one's own influence and promote alternative narratives to foster a more China-centric global digital order (Dekker/Okano-Heijmans, 2022; Creemers, 2020). This vision, which is based on a state-centric, westphalian understanding of sovereignty in cyberspace, contrasts with the currently dominant Western notion of a free Internet (Creemers, 2020). All this is supported by strong political will and extensive institutional restructuring in the cyber governance landscape (Creemers, 2021; Chang, 2014).

Gaining a comprehensive understanding of cyberspace developments is imperative for informed policy-making e.g., for the continued organization of a coherent international cyber diplomacy, which is central to protecting and strengthening Europe's digital sovereignty. In this context, China represents a pivotal actor with the potential to disrupt the current international order and stability in cyberspace. However, there is a significant knowledge gap concerning Chinese cyber policy. Therefore, it is crucial to identify and comprehend China's aspirations in cyberspace, fostering dialogue and knowledge sharing on this topic. This presentation seeks to shed light on China's cyber system by providing an overview of its ambitions in cyberspace, the

motivations driving them, and the different strategies, means, structures, and stakeholders involved in this system.

## Sources


Björk, M. & Rühlig, T. (2022): Power competition and China's technical standardization. In: Rühlig, T. (2022): China's Digital Power. Assessing the Implications for the EU. In: Rühlig, T. (Ed.). China's Digital Power Assessing the Implications for the EU.Berlin: CDP.

Cary, D. (2019): China's National Cybersecurity Center. A Base for Military-Civil Fusion in the Cyber Domain. Washington: CSET.

Chang, A. (2014): Warring State China's Cybersecurity Strategy. Washington: Center for a New American Security.

Creemers, R. (2021): China's Cyber Governance Institutions. Leiden: Universiteit Leiden.

Creemers, R. (2020): China's Approach to Cyber Sovereignty. Berlin: Konrad-Adenauer-Stiftung.

Dekker, B. & Okano-Heijmans, A. (2022): Projecting digital power internationally: Europe's digital China challenge. In: Rühlig, T. (Ed.). China's Digital Power Assessing the Implications for the EU. Berlin: CDP.

European Commission (2019): EU-China – A strategic outlook.Brussel: European Commission.

Fischione, C.; van der Lugt, S. & van der Putten, F.-P. (2022): AI and IoT Developments in China and the Relevance for EU Policy – a scoping study.In: Rühlig, T. (Ed.). China's Digital Power Assessing the Implications for the EU. Berlin: CDP.

Gallardo, C. (2022): UK spy chief: Britain must invest more to counter China's tech dominance.Online:https://www.politico.eu/article/uk-must-invest-more-to-see-off-chinas-tech-dominance-spy-chief-says/utm_source=blognotification&utm_medium=email&utm_campaign=Blog%20Post%20Notification%20Net%20Politics&utm_term=NetPolitics (last accessed: 3.3.2023).

Voo, J. & Creemers, R. (2021): China's Role in Digital Standards for Emerging Technologies – Impacts on the Netherlands and Europe.Leiden: Universiteit Leiden.

White House (2022a): National Security Strategy. Washington: White House.

White House (2022b): FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China. Online:https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/ (last accessed: 3.3.2023).

# Poster

# [2355] Unmasking Digital Threats in the Pursuit of Human Rights and Environmental Defense in La Guajira and Cesar, North Colombia

Laura Guntrum (PEASEC, Technical University of Darmstadt) and Verena Lasso Mena (International Relations, Technical University of Darmstadt).

*Abstract*

During decades of armed conflict between guerrillas, state armed forces, and paramilitaries in Colombia, minimal attention has been paid to the protection of digital rights. Furthermore, it is reported that during the armed conflict a surveillance apparatus to spy on citizens without judicial order was set up in Colombia (Erb, 2019).

This paper investigates the alarming (digital) human rights violations committed against social leaders in La Guajira and Cesar, North Colombia, who advocate for human rights and against environmental destruction caused by, amongst others, one of the biggest coal mines in Latin America (El Cerrejón) and numerous wind farms (Osorio García de Oteyza et al., 2021; Schwartz, 2020). According to Villalba (2021) in the national newspaper El Espectador, “threats are part of the daily life of social leaders in Colombia. And social networks and instant messaging services have also been a channel used by violent individuals to intimidate communities”. Based on qualitative interviews, the paper examines how digital threats are perceived by social leaders and whether and how digital security issues contribute to further violence. The research findings reveal that digital violence and digital death threats through (WhatsApp) calls, Facebook (Messenger), and SMS are prevalent in the region and are likely attributed to a variety of actors, including illegal armed groups and private companies operating in the region. In addition, social leaders encounter further challenges arising from internal divisions within their communities, exemplified by digital threats posed against them by own community members. In reaction, certain measures, like refraining from sharing their live location, are being implemented. However, secure applications such as Signal are seldomly used, confirming the overall perception that digital security issues play a predominantly subordinate role in their defense. Besides digital threats, numerous leaders experience that their accounts are being hacked, and they also often experience hate speech through social media platforms. Additionally, there is a pervasive sense of digital surveillance, adding to the challenges they encounter while using information and communication technologies (ICTs) for their defense.

The interviews reveal that while the majority of social leaders maintain their own security protocols, these protocols often neglect to adequately address the risks posed in the digital realm. The paper underscores the importance of equipping social leaders with the necessary knowledge and resources to effectively use ICTs in a secure manner. Furthermore, ensuring the availability of user-friendly, secure, and offline applications that can function efficiently in areas with limited connectivity is of high importance. The precarious nature of connectivity, particularly in rural parts of the region, accentuates the need for adaptive and resilient ICT solutions. This highlights the approach required to strengthen the crucial work of promoting human

rights and environmental defense in this field, by empowering social leaders with the necessary expertise and access to suitable ICTs.

## Sources

Erb, S. (2019, February 26). Colombia's sprawling spy network a threat to freedom.DW Akademie. https://akademie.dw.com/en/colombias-sprawling-spy-network-a-threat-to-freedom/a-47691828

Osorio García de Oteyza, M., Estupiñán Estupiñán, Ó. J., & Fuentes-Lara, M. C. (2021). Retos de paz y derechos humanos en la comunidad Wayúu en la Alta Guajira (Colombia). Revista de Paz y Conflictos, 13(2), 25–51. https://doi.org/10.30827/revpaz.v13i2.11247

Schwartz, S. (2020). Wind extraction? Gifts, reciprocity, and renewability in Colombia's energy frontier.Economic Anthropology, 8(1), 116–132. https://doi.org/10.1002/sea2.12192

Villalba, V. C. (2021). Lo bueno, lo malo y lo feo de las redes sociales para los y las líderes en Colombia| EL ESPECTADOR.https://www.elespectador.com/colombia-20/paz-y-memoria/lo-bueno-lo-malo-y-lo-feo-de-las-redes-sociales-para-los-y-las-lideres-en-colombia-article/

# [1195] NewSpace and proliferation risks – mapping the regulation of commercial space activities

Lauriane Heau (SIPRI).

*Abstract*

The dual-use character of many space technologies and concerns over the trade in such technologies are not new. However, with the rise of the NewSpace industry the range of possible missile proliferation risks has broadened. A multitude of new private actors are emerging in a growing number of countries, often with a lack of awareness about the regulatory environment in place, and resulting gaps in their compliance procedures which could be exploited. Recent technological developments in the space industry also increase proliferation risks, not least due to the growing similarities between small and micro launchers and ballistic missiles.

The global regulation of NewSpace industry activities is essential to address these proliferation risks. It takes place in part through international space treaties, which establish legally-binding obligations for States parties to take responsibility for objects launched into orbit, and to engage with their national space industry, thus creating a framework for national oversight of the industry. Multilateral export control regimes also have a key role to play. They count many of the states developing their NewSpace industry as members, and their control lists largely cover dual-use missile and SLV technology. In addition, other multilateral tools are relevant to prevent the sharing of sensitive technologies related to missiles in the context of NewSpace, such as foreign direct investment screening mechanisms. As a whole, these instruments make up a complex regulatory environment for new entrants in the sector – whether these are states or private actors.

The poster will map the existing regulatory environment and highlight possible remaining gaps, after briefly introducing why NewSpace poses specific proliferation risks, and which space technologies and activities are of particular concern. In doing so, it aims to clarify and increase understanding about applicable regulations over NewSpace activities involving dual-use space technology, and about possible ways forward in addressing developments within the NewSpace industry.

# [7497] Global Critical Infrastructures

Daniel Lambach (Goethe-Universität Frankfurt).

*Abstract*

Critical infrastructure (CRITIS) is “an asset or system which is essential for the maintenance of vital societal functions”. In other words, CRITIS are essential for the supply of populations, but the concept is only ever applied to the national scale. But what are the critical infrastructures of humanity as a whole? In the face of accelerating environmental change, this contribution asks whether humanity’s infrastructures are prepared for supplying all of humankind while adapting to more sustainable modes of governing essential functions. Its main aim is a reconceptualization and a rescaling of the CRITIS concept to a global scale. To that end, it first identifies “core” CRITIS sectors from a comparison of national taxonomies based on CIPedia’s survey (https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector).

As a next step, the potential for a global approach towards these sectors and their services is assessed with a view towards a sustainable transformation of critical infrastructures, e.g. by prioritizing access to mass transit over individualized car traffic, or by preferring renewable energy generation over fossil fuels. The contribution then sketches a theoretical framework how such global critical infrastructures are currently governed. Drawing on the literatures on global governance and global public goods, it takes a relational approach and focuses on agents and interactions due to the relatively low degree of institutionalization and greater prevalence of market mechanisms compared to other governance fields. Based on this theoretical approach, the contribution offers scope for a normative assessment how global critical infrastructures should be governed to improve access for all of humanity while making infrastructures more ecologically sustainable.

# [6777] Information Warfare on Twitter: Disinformation in the Russo-Ukrainian War

Stefka Schmid (PEASEC, TU Darmstadt), Maren Köhler (PEASEC, TU Darmstadt), Jonas Franken (PEASEC, TU Darmstadt) and Christian Reuter (PEASEC, TU Darmstadt).

*Abstract*

Social media has become a place for information operations, in particular in the context of warfare. The aim of this work is to identify factors that influence the spread of disinformation in the Russo-Ukrainian war on social media. Based on a data collection on the microblogging service Twitter, from March to April 2022, factors that could have an impact on the sharing of disinformation among Ukrainian and Russian-speaking social media users were investigated: political attitude, physical location, social media user type, trustworthiness of sources, and type of media. The quantitative analysis included 3,000 tweets and showed that especially pro-Russian social media users spread disinformation. Using an untrustworthy source (in the form of an article, image or video) in a tweet or misjudging the truth of a source also positively influences the sharing of disinformation for both Ukrainian- and Russian-speaking social media users. Thus, a strong ``media literacy'' is important for identifying both Ukrainian and Russian disinformation. As online and offline spheres are increasingly intertwined while intensified dynamics of ``tech nationalism'' reflect efforts to construe virtual spaces along national borders, we are particularly interested in how the physical localization of users affects their sharing behavior. In this regard, we find that localization can indirectly affect political attitudes among Russian-speaking social media users and thereby contribute to the generation of disinformation. Building on the insight that the impact of physical developments (in war) and different physically-bounded media ecosystems is outweighed by the effects of political attitude and consumption of untrustworthy (digital) media, we formulate design-oriented implications with the goal to foster media literacy across national contexts.

# [8883] Supporting Victims of Hate Speech: The Role of German Reporting Centers as Intermediaries with Counseling Centers, Authorities and Digital Platforms

Julian Bäumler (PEASEC, TU Darmstadt), Thea Riebe (PEASEC, TU Darmstadt), Marc-André Kaufhold (PEASEC, TU Darmstadt) and Christian Reuter (PEASEC, TU Darmstadt).

*Abstract*

The relationship between online hate speech and physical political violence has come to the attention of German policymakers, not least following the far-right motivated murder of Walther Lübcke, the regional district president of Kassel. To counter online hate speech, socio-technical measures have already been proposed that address the level of content, individual internet users, communities of users, civil society, or platforms. While all German states and the federal government have taken countermeasures, major differences can be observed. This applies in particular to the provision of or cooperation with reporting centers. As previous work has only peripherally addressed such organizations, this poster aims to explore the role of reporting centers in combating online hate speech in Germany and the emerging research gaps in this context. Drawing on a review of relevant academic literature as well as civil society publications and policy documents, the poster (1) provides an initial overview of the German reporting center landscape, (2) presents a preliminary model of how reporting centers act as intermediaries between victims and counseling centers, authorities, and platforms, (3) outlines initial opportunities for technology support, and (4) finally identifies a need for more in-depth research on the collaborative work processes in reporting centers.

# [4906] Political Violence, Populism and Social Media in Brazil

Kaya de Wolff (Goethe University Frankfurt, TraCe).

*Abstract*

This paper addresses the interrelations of political violence, populism and social media, using the striking case of the recent tense and eventful Brazilian presidential election process in 2022/23. It looks into new forms of digital populism in Brazil. It argues that the emergence of social media transforms the nature of political violence, as the invasion in Brasília on January 8 demonstrates. On this example, it discusses the role of social media platforms and centers the discussion on the interpretation that the attacks of the national congress were staged as "a coup for the Instagram age".

# [1533] Chemical Weapons Investigation Mechanisms in Syria: Scientific Methods and Standard of Proof

Almuntaser Albalawi (Peace Research Institute Frankfurt) and Kristoffer Burck (Justus-Liebig-University Giessen).

*Abstract*

The use of chemical weapons is comprehensively banned under the Chemical Weapons Convention (CWC) and customary international law. This comprehensive prohibition does not only apply to states but also to individuals. While the CWC does foresee procedures for ascertaining chemical weapons use and identifying perpetrators in Article IX (Consultations, Cooperation, and Fact-Finding) and Verification Annex Part XI (Investigations in Cases of Alleged Use of Chemical Weapons), these articles were not employed in the first cases of chemical weapons use by a CWC state party, i.e., in the context of the Syrian civil war.

Instead, several ad-hoc mechanisms were established with either the objective of fact-finding or attributing responsibility based on varying legal frameworks. This contribution aims to engage four of these mechanisms, namely, the early United Nations Mission through the United Nations Secretary-General's Mechanism (UNSGM), the Organization for the Prohibition of Chemical Weapons (OPCW) Fact-Finding Mission (FFM), the Joint Investigative Mechanism (JIM), and the Investigation and Identification Team (IIT).

With distinctive mandates, the mechanisms followed different scientific methods in meeting varying standards of proof depending on the objectives pursued. For instance, in investigating allegations, UNSGM and FFM primarily relied on methods of biomedical and environmental sample analysis. On the other hand, the JIM and IIT utilized further scientific methods to conclude attribution, including chemical forensics, analysis of meteorological data and satellite images, ballistics analysis, munition analysis, and toxicology analysis.

This work compares the mandates and legal foundations of the four mechanisms and the respective scientific methods utilized in evidence finding and attribution. This systematic comparison provides the basis for further discussions on how legal circumstances constitute scientific methodology and vice-versa. As such, the objective is to provide a better understanding of the relationship between legal objectives and related standards of proof with the different scientific methods used in investigation mechanisms

# [2914] Briar: Secure Messaging for Citizens and Activists during Internet Shutdowns

Nico Alt (The Briar Project / PEASEC, TU Darmstadt).

*Abstract*

A pattern commonly observed in situations of protests and crises is limited Internet connectivity due to either forced Internet shutdowns or infrastructure outages. While many popular instant messaging systems these days, like Signal and WhatsApp, offer sound cryptographic protection of messages' contents, they all require a working connection to some sort of server infrastructure in order to function. Briar is a free and open-source software messaging system that solves these problems by using a novel peer-to-peer approach. Depending on the Internet's availability, it uses the Tor network to directly deliver messages between communicating peers. However, if the Internet connection is cut, it can fall back to communication via Bluetooth, the local network, or communication via memory cards, enabling so-called sneakernets. All messages exchanged are end-to-end encrypted and due to the peer-to-peer nature metadata is protected as well. By these means, Briar enables self-organization of citizens and activists and allows them to keep communicating even in hostile environments.

# [8459] The 70:20:10 framework for regulatory compliance trainings. An opportunity for CBRN-WMD awareness trainings?

Tom De Schryver (Dutch Defence Academy (NLDA)).

*Abstract*

Training about regulatory compliance is most urgent in contexts where you expect it the least. This applies for sure in a dual-use context. Business and their supply chains dealing with dual-use goods; i.e. goods, software and technology that can be used for both civilian and military applications; need to invest in training because the customers of these goods and services can disguise their true intended end-use. Because of the ambivalence and risks, the international laws and regulation for to the exchange of dual-use goods and services in commercial and research settings is complex. It has become increasingly important to assess whether business transactions are driven by commercial, academic versus national security/defense interests. L& D professionals working in these dual use contexts face a huge challenge. On the one hand, it is clear that dual-use trainings should help professionals to increase awareness about the security and dual-use risks and to combine wise ethical judgement with professional competence. On the other hand, the ways to design and to deliver these dual use training in contexts that matter are less understood. Regulatory compliance trainings are often considered for most participants to be a dull moment of time.

The main problem is that most regulatory compliance trainings are designed without any consideration of the learning needs of staff. The trainings are simply imposed top-down. In order to accommodate the trainings more to the workforce, Hauser (2020) has diversified the roles of trainers and increased the options for the design of compliance trainings. He argues that instead of always putting their compliance knowledge or educational tools to the fore, trainers should evolve into guides and tutors for their trainees. The contribution of Hauser (2020) is a good start to make regulatory trainings more relevant. Moreover, this framework has strong parallels with the popular 70:20:10 framework in L& D community.

I argue here that the model can be extended further by means of a more trainee centered approach. Hauser (2020) focusses mainly on what the trainer ought to do. Much can be gained by flipping the corporate classroom and focusing more radically on the trainee in the design of regulatory compliance trainings. Not only the learning goals of the trainer, but also the dilemmas of the trainee deserve time and attention. The focus of this poster is on how to design a regulatory compliance training that takes into account the diverse learning needs. Lessons learnt from the 70:20:10 framework lead me to focus on conditions for good communication: how to make sense of stories where both trainees and trainers are both experts and laymen.

## Sources

Hauser, C. (2020). From preaching to behavioral change: Fostering ethics and compliance learning in the workplace. Journal of Business Ethics, 162(4), 835-855. https://doi.org/10.1007/s10551-019-04364-9

De Schryver, T. (2023) Designing Dilemma Trainings As Liminal Spaces For Behavioral Change. 2022 EAPRIL conference proceedings. https://tinyurl.com/yheadcwn

# [6245] Critical infrastructure and outer space: geopolitics, vulnerability, risk reduction and arms control

Jürgen Scheffran (Professor in Geography at Universität Hamburg).

*Abstract*

Outer space is considered as part of the world's critical infrastructure, both in the civilian and security sector. Satellites conduct numerous tasks, often dual-use, for reconnaissance, early warning, monitoring, weather observation, communications, navigation, environmental protection and research which support multiple infrastructures on earth for the economy and society, energy and resources, political stability and security, health and climate, among others. While the global market for space-related activities and investments is multiplying in the coming years, competition and cooperation are increasing among a growing number of governmental and non-governmental actors in North and South. When outer space is becoming an arena for geopolitical conflict, the infrastructure in orbit and on earth is becoming more vulnerable to cascading risk: interruption of communication by accidents, jamming or ground attacks; collision with other space objects and space debris; physical attack by explosive devices, cyber, nuclear, kinetic or directed energy weapons; sensor blinding; hacking, deception or hijacking. The survivability of space objects can be improved by passive or active protection and risk reduction measures, including physical hardening and shielding, manoeuvring capability, dummies, or active countermeasures. A code of conduct for responsible space behaviour can contribute to confidence-building, rules of the road, risk reduction and stabilization. With the proliferation of space launchers and missiles, missile defense and anti-satellite weapons, threats to space infrastructure would considerably increase, jeopardizing international stability. An arms race in space can be prevented through preventive arms control and disarmament which reduces the risk to the infrastructure on earth and in space.

# [2136] Oculta: Hidden Secure Communication via WhatsApp and Co.

Nico Alt (PEASEC, TU Darmstadt) and Laura Guntrum (PEASEC, TU Darmstadt).

*Abstract*

In tense situations, often there are requirements to communication current messaging systems aren't able to meet. While systems like Signal offer sound cryptographic protections to ensure confidentiality, authenticity, and more, using a separate messaging system often is not possible. Those systems might be censored in a given region, it might be illegal to have their apps installed (and one could get into trouble in road checks), or communication via, e.g., WhatsApp is preferred, because using it is free in that country and all contacts are there. WhatsApp officially states that it is using end-to-end encryption, but this can't be confirmed independently.

In addition to that, some high-risk users need additional protections against physical attacks on their devices. To someone inspecting their devices, it should not be visible at the first glance that some secret communication is happening.

Oculta (Spanish for “hidden”) is an Android application that allows to have cryptographically protected communication that is exchanged in a hidden manner via existing messaging systems like WhatsApp, Telegram, or email. For this, messages are protected using state-of-the art cryptography and hidden inside text or images using techniques from steganography.

# [1311] On the Origin of Gender Bias in Face Recognition

Paul Jonas Kurz (TU Darmstadt), Philipp Terhörst (Universität Paderborn) and Arjan Kuijper (Fraunhofer IGD & TU Darmstadt).

*Abstract*

Biometrics is defined as the automated recognition of individuals based on their behavioral or physical characteristics. Unintentional gender bias in the corresponding systems has significant consequences. Individuals, especially females, are systematically discriminated against since the algorithms experience higher error rates on these demographics. For this reason, gender bias is one of the pivotal unsolved problems in biometrics and face recognition in particular. Its impact is evident in various everyday application scenarios using facial recognition systems. These include the authentication on modern smartphones and laptops, the authorization of financial transactions, or even the identification for border control. Especially in situations relevant to criminal law, the unintentional malfunction of the algorithms has potentially severe consequences, such as the imprisonment of innocent individuals. Such occurrences critically impact the daily life of those affected and, thus, foster public mistrust in facial recognition systems in general. Legislators also intensively debate the use of face recognition in practice, despite its clear advantages over password- or token-based authentication. To find an effective fix for this deficiency, the underlying causes of gender bias must be identified, analyzed, and ultimately understood. Previous works have primarily focused on the unequal distribution of genders in training data as a possible origin. Despite their efforts, the actual impact of this circumstance on bias has recently been proven insignificant. This finding has instigated a paradigm shift in research, with studies from the near past now mainly evaluating the role of facial features in the broader issue. However, these works apply complicated analysis methods that use low-scale, low-variance face annotations and image databases, as well as evaluation techniques that can induce unwanted variations in the results. Additionally, they do not take correlations of facial features into account. These deficits limit the results' expressiveness and generalizability. In this thesis, the effects of non-demographic facial characteristics on gender bias are comprehensively evaluated. The presented methodology exploits the advantages of the tree data structure to efficiently generate multiple combinations of attributes, which represent the presence or absence of relevant characteristics. Subsequently, annotated large-scale image databases with high variance are filtered for faces of males and females in which the desired attribute combinations are featured. Thus, the images' performance and, hence, the characteristics' impact on fairness can be reliably assessed using two state-of-the-art face recognition models. Crucially, the proposed approach can also account for correlating facial features by clustering and thus combining them such that they can effortlessly be treated as a single attribute. Overall, these properties make the proposed approach simple yet effective, with its results achieving high informational value and generalizability. Applying the presented methodology reveals that gender bias entirely disappears when the presence or absence of combinations of specific characteristics is equalized across the considered genders. Those include attributes related to facial hair,

hairstyles, and particular occluding accessories. These outcomes are consistent across all considered experimental settings. This strongly indicates the role of the revealed facial features as the true origin of gender bias. Consequently, future works can leverage those findings. One viable strategy would be to develop recognition models agnostic to the respective characteristics during training and operation. Another possible approach is the introduction of bias mitigation techniques that limit the effect of these specific characteristics in the recognition process. Ultimately, the results of this thesis should notably aid in more effectively and precisely researching remedies for gender bias and, thus, critically reducing the unfair treatment of individuals.

# [5009] Investigating the contribution of website operators to the emergence and remediation of privacy risks

Alina Stöver (TU Darmstadt).

*Abstract*

Privacy risks on websites are a pervasive issue that impacts user privacy. Although much existing research has focused on understanding the user's perspective and offering solutions, the role of website operators is often overlooked. These operators make critical decisions that can either create or mitigate privacy risks online. This dissertation shifts focus to explore the viewpoint of website operators, aiming to shed light on their role in the emergence and remediation of online privacy risks.

A multi-part study involving operators of 4,594 websites uncovers gaps in awareness, technical understanding, and the organizational resources necessary for remediating privacy issues. Another study, which investigates the design of cookie consent notices among 376 users and 195 operators, reveals a disjunction between user preferences for privacy-friendly designs and the choices that operators make. The research further shows that Consent Management Platforms (CMPs), which offer commonly-used templates for these notices, often provide inadequate options for privacy-friendly designs.

The findings emphasize the need for targeted interventions to support website operators in enhancing online privacy. Addressing this often-overlooked group can help relieve the burden on users to navigate privacy risks and contribute to a more privacy-friendly online environment. Tailored solutions must be developed to suit the varied technical and organizational contexts in which these operators work.

# [2024] Technology Assessment of Dual-use ICTs – How to Assess Diffusion, Governance and Design

Thea Riebe (PEASEC, TU Darmstadt).

*Abstract*

The dissertation employs the epistemological framework of Technology Assessment (TA), integrating concepts from Critical Security Studies (CSS) and Human-Computer Interaction (HCI) to evaluate and design dual-use technologies. First, looking into cases of spillover effects, it examines the early-stage diffusion of dual-use innovations in expert networks and AI patents, revealing limited diffusion. Second, the dissertation delves into the governance of dual-use technologies through two case studies, including the regulation of AWS with a focus on Meaningful Human Control (MHC) and the evolving regulations surrounding strong cryptography and mass surveillance programs in the U.S., involving private companies as central actors. Third, focusing on the aspect of including dual-use assessment into technology design, the research investigates dual-use case of Open Source Intelligence System (OSINT) for cybersecurity while deriving design implications within the Value-Sensitive Design (VSD) framework. Findings emphasize the importance of participatory approaches to mitigate risks for indirect stakeholders. Overall, this interdisciplinary and multi-method dissertation contributes to understanding the specific risks associated with dual-use technologies in areas such as AI, AWS, cryptography, and OSINT, offering insights for regulation, design, and security considerations.

# Dialogue Panel: ICT4Peace - The Role of Information and Communication Technology in (Digital) Peacebuilding

# [7623] Digital Peacebuilding – Potentials and Challenges of ICTs in Peacebuilding Efforts

Laura Guntrum (PEASEC, TU Darmstadt).

*Abstract*

Digital peacebuilding presents a myriad of opportunities and challenges that need to be addressed to optimize its potential for conflict transformation. On the one hand, ICTs can help to overcome physical barriers and reach marginalized communities, facilitate data management, and promote interactivity in peacebuilding. On the other hand, digital threats such as hacking, privacy violations, and cyberbullying can jeopardize the safety of individuals and organizations involved in peacebuilding. Furthermore, access to technology and digital literacy is not universal, which can lead to inequalities in participation and engagement. Furthermore, the use of technology in peacebuilding may face cultural or political resistance, particularly in contexts where, for example, authoritarian governments seek to control information and discourse. This panel discussion will explore the opportunities and challenges of digital peacebuilding by looking at specific case studies and highlighting best practices, key lessons learned, and strategies for addressing digital risks and promoting inclusivity in peacebuilding.

# [2258] Postcolonial Perspectives on Digital Peacebuilding: Moving from «Inclusion» to «Agency»

Julia-Silvana Hofstetter (ICT4Peace Foundation).

*Abstract*

Digital technologies promise to innovate peacebuilding and enhance inclusivity by facilitating the participation of local civil society in decision-making processes. However, the current approach to participatory digital peacebuilding has a limited definition of «inclusion» and is often rather extractive in nature, where the local population is treated as a mere source of data. The paper critically analyses the implications of «digital inclusion» in peacebuilding, particularly in terms of its limitations and risks, using a postcolonial lens. Moreover, in this context, the paper sheds light on the gendered risks of digital peacebuilding initiatives, such as misrepresentation in data sets and cyberviolence. The paper argues that citizens' participation in digital peacebuilding should go beyond collecting data on their needs and opinions and ensure their agency and ownership of digital peacebuilding programs and collected data. To this end, the paper argues for a reconceptualization of «digital inclusion» as «digital agency».

# [2657] Digitalization and e-government in the lives of urban migrants: Evidence from Bogotá

Charles Martin-Shields (German Institute of Development and Sustainability).

*Abstract*

Research on the role of information and communication technologies (ICT) to improve the lives of displaced people is a growing field. However, studies in this area have been conducted mainly in wealthy countries, with municipalities that are capable of supporting migrants or refugees. There is less evidence from middle-income host countries and how ICTs can help migrants in their resettlement efforts. To address this gap, this study examines ICT access and the use of e-government services by Venezuelan displaced people in Colombia and compares this group with short- and long-term residents of Bogotá. The descriptive analysis of the data reveals that, after controlling for demographic and socioeconomic characteristics, foreign displaced people are less likely to own ICT devices compared to short- and long-term residents, but over time do acquire ICT access. In addition, Venezuelan displaced people are less likely to use e-government services than their local peers even after controlling for demographic characteristics and internet access, with the exception of address registration. While this paper originally focused on post-displacement contexts, the talk will highlight how the results apply to a variety of post-conflict settings where digital solutions are deployed to meet collective social and economic needs.

# [4159] The Ethics of PeaceTech: Ownership and Outsourcing of Risk in Distributed Systems

Andreas Hirblinger (Geneva Graduate Institute), Fabian Hofmann (Geneva Graduate Institute) and Kristoffer Lidén (PRIO).

*Abstract*

The growing use of digital technologies in efforts to end violent conflicts and build peace has triggered an increased concern with their associated risks and ethical challenges, which is well visible in the growing number of policy- and practice-oriented publications. Digital peacebuilding efforts have enabled remote and decentered approaches executed through human-machine networks in which agency emerges as a distributed effect. Often, these networks entail global partnerships involving technology and peacebuilding professionals in digital infrastructures that stretch from Silicon Valley, over the headquarters of international organizations, to local peacebuilding initiatives. This means that the impacts of digital peacebuilding interventions and their potential adverse effects can usually not be directly controlled. However, the contours of this newly emerging “ethics of PeaceTech” discourse and the specific distribution of risks and responsibilities it entails have received scant scholarly attention so far. To address this gap, the paper presents a qualitative analysis of the most pertinent policy- and practice guidelines on digital peacebuilding and sheds light on their underlying ethics perspectives and risk management strategies. It argues that duty-based, consequentialist, and virtue ethics perspectives on PeaceTech serve as vectors that individualize and decenter the responsibility for the adverse effects of digital peacebuilding. By explicitly or implicitly framing these adverse effects as „risks” and outsourcing them to virtuous end-users or third parties, discourses on the ethics of digital peacebuilding advertently or inadvertently push responsibility on those parts of the networks that are least resilient.

# [1470] An intersectional feminist lens on digital peacebuilding

Kerem Tugberk Capraz (Berghof Foundation).

*Abstract*

From social media activism to minority surveillance: New technologies are having a profound impact on the field of peacebuilding. The hope that digitalisation would promote inclusion and equality is contrasted with the sobering reality that mechanisms of marginalisation are often reproduced in the digital sphere. The Berghof Foundation and the Platform for Peaceful Conflict Transformation have commissioned a studythat fills a gap in existing literature and practice where intersectional feminist approaches to technology meet intersectional feminist approaches to peacebuilding.The study explores how intersectionality can help increase the opportunities and reduce the risks of digital peacebuilding. The authors argue that incorporating an intersectional feminist lens into peacebuilding helps to start from a better understanding of privilege and discrimination to address recurring challenges to effective, inclusive peace processes. The paper also shows that the strategic goal of approaching digital technology through an intersectional feminist lens is to mitigate the discrimination built into technology design and use.

# V (Dual-use and Technology Assessment)

# [4387] Adjusting the Wheel: Ethical Deliberation as a Method for Dual-Use Assessment in the ICT Development Process

Thea Riebe (PEASEC, TU Darmstadt) and Christian Reuter (PEASEC, TU Darmstadt).

*Abstract*

ICT development methods have changed from the linear water-fall model towards faster iterations which can even include ethical design approaches, such as Value Sensitive Design (VSD). To ensure such standards, principles, and Codes of Conduct have been formulated and operationalized. In the case of AI, sets of principles have been collected as "AI4People" (Floridi et al., 2018) or "Trustworthy AI" (EU Commission, 2019). In the case of AI, the frameworks help to include relevant aspects, to develop in a lawful, ethical, and robust way, but need to be translated into the application of the R&D projects. These frameworks are based on a set of norms, which are deliberately abstract and need translation for a particular context. On the other side, there are participatory design methods, such as VSD, which help to include values, which are important to the participants, and might fit a certain context well, but do not guarantee that certain norms are met. Thus, the question remains if dual-use risks can be fully addressed by these frameworks and methods, or if dual-use risks occur, even when ethical standards are met, and all stakeholder values are included. Thus, this paper summarizes the discourse on ethical ICT development frameworks, and participatory design methods, mapping the dual-use definitions, risk scenarios and stakeholders (Riebe, 2023) on them. Doing so, the paper asks if these frameworks and participatory methods already address ICT dual-use risks (Tucker, 2012), and if so, which of them. The results help to understand, how dual-use assessment can be done as a form of ethical deliberation as a combination of norms and a participatory and deliberate process (Gogoll, 2021), or if there is a methodological research gap.

Sources:

EU Commission (2019). Ethics guidelines for trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Floridi, Luciano, et al. (2021). An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Ethics, governance, and policies in artificial intelligence, 19-39.

Gogoll, Jan et al. (2021). Ethics in the software development process: from codes of conduct to ethical deliberation. Philosophy & Technology, 1-24.

Riebe, Thea (2023). Technology Assessment of Dual-Use ICTs – How to assess Diffusion, Governance and Design. Darmstadt, Germany: Springer Vieweg.

Tucker, Jonathan B. (Ed.). (2012). Innovation, dual use, and security: managing the risks of emerging biological and chemical technologies. MIT press.

# [9033] Missile Defenses for Europe: Computer Modeling and Analysis

Timur Kadyshev (IFSH).

*Abstract*

After the end of the Intermediate-Range Nuclear Forces Treaty (INF), there is a growing threat from intermediate- and shorter-range missiles. Russia is deploying a new intermediate-range system, the US is developing one. Even before the treaty's demise, China has been developing and fielding conventional and nuclear intermediate-range missiles in the Western Pacific. To counter this threat, along with political efforts, countries consider development and deployment of ballistic missile defenses. Detailed technical knowledge is required to support the debate on the effectiveness of such systems. In this contribution we will present a new computer model for the calculation and comparison of missile defense footprints. The model builds upon work from Jürgen Altmann in the 1980's, takes into account technical characteristics of missiles and interceptors, and calculates and displays footprints corresponding to various scenarios of engagement. Using this computer program we analyze existing missile defense systems and their quantitative deployment parameters depending on the requirements set forth with regard to their effectiveness.

# [4198] The Impact Of Quantum Technologies On Deterrence, Arms Control, Nonproliferation, and Verification

Ferenc Dalnoki-Veress (James Martin Center for Nonproliferation Studies (CNS)), Grant Christopher (VERTIC), Allison Burke (James Martin Center for Nonproliferation Studies (CNS)) and Miles Pomper (James Martin Center for Nonproliferation Studies (CNS)).

*Abstract*

Quantum information science and technologies (QIST) will have myriad impacts on deterrence, arms control, nonproliferation, and verification. Quantum computing and quantum communications will disrupt current protocols for secure data transfer and storage. Quantum simulations of chemical and biological processes are expected to cause additional challenges and opportunities for WMD risk reduction. Developments in quantum sensing and metrology are in an advanced status of development and will impact and disrupt current verification activities by enabling the development of new sensors. Quantum sensing could make it easier for military forces to track nuclear-armed submarines and mobile missiles, threatening a deterrence pillar. This paper will address the current status of these technologies, the expected development timeline, and the impact on security, with a focus on deterrence, arms control, nonproliferation, and verification. This project is funded by the United States Department of State.

# VI (Cyber Operations)

# [3174] The Normative Power of the Factual: How State Practice Shapes Understandings About Direct Public Political Attribution of Cyber Operations

Christina Rupp (Project Manager Cybersecurity Policy and Resilience, Stiftung Neue Verantwortung) and Alexandra Paulus (Project Director Cybersecurity Policy and Resilience, Stiftung Neue Verantwortung).

*Abstract*

An increasing number of states use direct public political attribution to call out inappropriate behavior in cyberspace attributable to another state. Shared understandings about conducting and communicating political attribution practices are essential to avoid misunderstandings and mitigate the risk of potential escalation between states. However, attribution remains only marginally addressed in the context of diplomatically negotiated cyber norms so far. This makes this field well suited to explore the formation of normative ideas through state practice as it leaves ample room for practical interpretation by states. Based on a selection of four case studies (Australia, Germany, Japan, and the United States), this paper identifies which cyber operations the selected states have publicly attributed, how the attribution was communicated and justified, to what extent other states were involved in the process, and how other states perceived the attribution. This analysis of established and emerging individual as well as collective state practice will permit new insights into how States currently perceive the respective normative framework, that is, formalized cyber norms, and conclusions as to what extent the observed State practice gives rise to new shared understandings about appropriate state behavior - practiced cyber norms - when it comes to direct public political attribution of cyber operations.

# [514] The Role of Cyber Ranges within European Cybersecurity Strategy: A Primer

Dwyer Andrew (Royal Holloway University of London), Mischa Hansel (Institute for Peace Research and Security Policy at the University of Hamburg (IFSH)), Jantje Silomon (Institute for Peace Research and Security Policy at the University of Hamburg (IFSH)) and Kathrin Moog (Institute for Peace Research and Security Policy at the University of Hamburg (IFSH)).

*Abstract*

Over the course of the last decade, the European Union has emerged as an important player within the field of international cybersecurity. While regulatory policies are arguably the prime vehicle for implementing the EU's cybersecurity strategy, other policy instruments such as cyber sanctions, information sharing and infrastructure development also offer important contributions. Cyber ranges (CRs) are another such tool that could facilitate greater cooperation and influence European policy debates, yet there has been little assessment of their strategic utility. The majority of CRs are run by, and for, research or commercial purposes, with a focus on meeting training and educational needs. Yet, CRs could further a cyber-skilled workforce more broadly, helping to build resilience within business as part of the EU's strategy of enabling a cyber-skilled workforce, or bolstering defensive capabilities more broadly. CRs could also support such endeavours beyond operational and technical coordination, fostering that cooperation with partners and the multi-stakeholder community – another vital element of EU's strategy – as a small number of states have already begun to do so. Lastly, CRs are being used to advance sovereign capabilities, offering challenges but also opportunities. For example, CRs could be used to substantiate and advance principles of responsible state behaviour within cyberspace, which would align with the proposed EU leadership on standards, norms, and frameworks in cyber matters. Our work gives an overview of how CRs are used, followed by a survey of those existing at the national level before delving into EU efforts to enable joint uses at the regional level. We then assess potential uses of CRs to achieve four core objectives of the EU's cybersecurity strategy: bolstering a cyber-skilled workforce, ensuring high levels of cyber resilience across the continent, encouraging responsible behaviour in cyberspace, and extending solidarity to international partners and allies.

# [8638] International Cybersecurity and Peace Research: Challenges at the Interception of Peace and Conflict Research and Cyber Security Research

Christian Reuter (PEASEC, TU Darmstadt).

*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 talk 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 the variety of state and non-state actors and the difficulty of verification and attribution are outlined. Furthermore, an overview about current research in this area is given.

# VII (Biological, Chemical and Conventional Weapons)

# [7088] Biological Weapons: A Harm Potential Assessment

Dunja M. Sabra (Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg), Anna Krin (Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg), Johannes L. Frieß (Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg), Ana B. Romeral (Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg) and Gunnar Jeremias (Carl Friedrich von Weizsäcker-Centre for Science and Peace Research (ZNF), University of Hamburg).

*Abstract*

Bioterrorist attacks belong to the class of low probability, high-impact events. Therefore, measuring the likelihood of a bioweapon attack is unfeasible due to the lack of comparable events. Effective and sustainable preparedness is thus an indispensable component of an impactful biosecurity management. Hence, we propose a tool to analyze and assess the expected harm potential of diverse biological agents. The here proposed Harm Potential Assessment is a qualitative and semi-quantitative assessment tool based on a questionnaire subdivided into seven sections. These sections consist of thirty-seven questions addressing technical characteristics of a specific bioweapon covering the aspects of the bioweapon agent development, bioagent release, and mitigation of the biological agent. Beyond this, its biological characteristics, human health, societal, economic and environmental impact are explored in this assessment. The goal of the Harm Potential Assessment is to calculate the harm potential of biological agents used in diverse scenarios, allowing relevant stakeholders, such as politicians, economists, healthcare professionals and emergency response teams, to effectively coordinate and allocate their resources.

# [551] Taking biological security education forward and building up an international biological security education network

Lijun Shang (London Metropolitan University) and Malcolm Dando (Bradford University).

*Abstract*

The recent 9th Review Conference of the Biological and Toxin Weapons Convention (BTWC) in 2022 concluded that a radical change in how science and technology is dealt with under the Convention must be a major issue for decision during the current intersessional period up to the 10th Review Conference. As part of this rethink much more attention will be paid to the implementation of the Biological and Toxin Weapons Convention, and as part of that process there should be a focus on correcting the present less known of most life scientists (and life science-associated scientists) of the dangers of biological security in general and of dual use in particular. The Tianjin Guidelines for National and Institutional Codes of Conduct under the Convention and the World Health Organisation's new Global Guidance Framework for the Responsible Use of the Life Sciences make it plain that a major effort designed to educate life scientists about biological security will be needed in coming years. In this presentation, we would like to talk about our initiative of setting up an International Biological Security Education Network (IBSEN). We will start with our recent survey on globe biological security education projects in the last two decade, then our ongoing biological security education resource book, and move on to our new project of setting up an International Biological Security Education Network, which is in parallel to the International Nuclear Security Education Network (INSEN) run in conjunction with the International Atomic Energy Agency (IAEA). We hope to work in conjunction with colleagues around the world and State Parties to the BTWC and to lay the basis for the network eventually to be run from the BTWC itself.

# [4167] Access to Information about Chemical Weapon Attacks: Increasing Resilience in Kurdistan

Zenobia Homan (Centre for Science and Security Studies, King's College London), Saman Omar (Center for Genocide studies, University of Duhok) and Jeanne Desurmont (King's College London).

*Abstract*

This project documents the threat of chemical weapon use in the Kurdistan region of Iraq (KRG), with the aim to contribute to prevention and mitigation of such crimes. The work particularly focusses on the digital information landscape and online knowledge exchange, including the influence of social media as a resource, censorship, bias, disinformation and misinformation.

The aim of an exploratory study (September 2021-January 2022) was to map present-day knowledge: through in-person interviews and surveys accounts were gathered that reflected on public awareness and current security concerns. The scope of the research covered the Anfal campaigns, the use of chemical weapons during the Syrian civil war, and chemical attacks launched by so-called Islamic State (IS). This study found that there was a strong lack of knowledge about the effects and impact of chemical weapons at the time of the Anfal attacks, with little change during the attacks by IS almost 30 years later. It also showed that people fear further chemical attacks – yet they do not believe there is sufficient awareness, or an acceptable plan for emergency response.

That study led to several new research questions, especially relating to the availability and reliability of published information – which is a notoriously complex subject in the KRG. Accordingly, the next step in our project was to consider news media – focussing on how and by who chemical weapon attacks are reported in the region. What are the sources, how are these verified, and what is the message that is coming across? What is the state of investigative journalism in the KRG – particularly, in Kurdish media itself? And from the point of view of the public, how do local media affect their knowledge, awareness and preparedness when it comes to potential chemical attacks?

Between May 2022 and May 2023, we shared a targeted online survey with journalists working in the KRG (local and foreign, 15 total) and conducted interviews with journalists (local, 10 total). Despite their extensive experience in the region, including reporting on chemical attacks, many provided comments such as “the quality (of reporting) is not good, but there is an essential issue that journalists lack the resources to investigate thoroughly” and “better access to experts on chemical attacks, and training on this topic, is needed”. As barriers they highlighted issues with press freedom, absence of media ethics, political bias, partisan pressure from editors, bans on certain topics, fear of prosecution or arrest, corruption, religious challenges, source reliability, and lack of statistics.

Next, we wanted to map the information landscape and gain a better understanding of the quality of available media reports. During June 2023 we analysed local online news media archives – in both English and Sorani Kurdish. We gathered 643 articles reporting on (alleged) chemical attacks, comparing between 2017 (73 items)

and 2022 (570 items). These mentioned possible incidents in over 50 locations, of which 60% in the KRG. The collected articles included news items, official and political statements, interviews and testimonies, protest reports, and, notably, many commemorations and mentions of martyrdom. Depending on political affiliation of the media outlet, we found clear patterns in tone and vocabulary-use. While some outlets released multiple articles on certain events, others did not report on them at all. This makes it difficult to verify reports, to judge what is true, and to decide what information to trust.

With this data, we intend to explore the role of media in raising awareness against chemical weapon attacks in the KRG. Specifically, we want to utilise this study to enhance access to information, education, and emergency response. Through development of educational materials as well as in-person training and online mentoring we hope to increase resilience and preparedness in the KRG.

# [325] Small space launch vehicle technology in the NewSpace era: A new challenge for missile non-proliferation?

Kolja Brockmann (SIPRI).

*Abstract*

## Abstract

The development of small and micro launch vehicles by the NewSpace industry, driven by the demand for additional launch options for ever smaller and cheaper satellites and multi-satellite constellations, is significantly increasing the number of dual-use missile technology holders beyond current missile possessors (Brockmann and Raju, 2022). 'Small launchers' are roughly defined as those space launch vehicles able to carry a payload of up to 2000 kilograms to at least low Earth orbit, while 'micro launchers' can do so with payloads of up to 500 kg (Wekerle et al., 2017). Some small and micro launchers are increasingly resembling ballistic missiles (Maitre and Moreau-Brillatz, 2022). These commercial launch vehicles are configured to use solid-fuelled rocket motors for rapid deployment and are road-mobile. For example, Chinese companies Landspace and ExPace are both working on such road-mobile solid-fuelled quick reaction launch vehicles.

The growth of the commercial space launch vehicle market and associated international transfers of technology and know-how raise serious missile proliferation concerns. Therefore, It is important to improve understanding of the missile-related dual-use technologies pursued by small and micro launch vehicle manufacturers and the applicability of existing export control frameworks, including the Missile Technology Control Regime. Many NewSpace companies, including launch vehicle manufacturers, are start-ups, small, or medium-sized enterprises and lack awareness of proliferation risks and effective internal compliance programmes. It is crucial for states to improve outreach to the industry, strengthen resilience and compliance and explore how national developments in this sector should be reported in relevant transparency and confidence-building measures, in particular the Hague Code of Conduct against Ballistic Missile Proliferation.

Sources

Brockmann, K. & Raju, N. (2022). NewSpace and the Commercialization of the Space Industry: Challenges for the Missile Technology Control Regime. SIPRI. https://doi.org/10.55163/YRPY6524

Wekerle, T., et al. (2017). Status and trends of smallsats and their launch vehicles—An up-to-date review.Journal of Aerospace Technology and Management, 9(3), 270. https://doi.org/10.5028/jatm.v9i3.853

Maitre, E. & Moreau-Brillatz, S. (2022). The Hague Code of Conduct and space. HCoC Research Papers, 10. Fondation pour la Recherche Stratégique. https://www.nonproliferation.eu/hcoc/the-hague-code-of-conduct-and-space-2/

# VIII (Technology Politics and Strategies)

# [5183] Narratives of "Tech Wars": Technological Competition, Power Shifts and Conflict Dynamics Between the US, China and the EU

Daniel Lambach (Goethe-Universität Frankfurt), Jakob Landwehr-Matlé (TU Chemnitz) and Kai Oppermann (TU Chemnitz).

*Abstract*

In the context of digitalization, technological change and competition are deeply entwined with questions of international security and power. In particular, leadership in digital technologies has become a key parameter of the growing geopolitical and geo-economic great power competition between the US, China, and the EU. The securitisation of such technologies can be seen in the widespread perception of an intensifying *Tech War* between the three actors. Against this background, the paper takes a social constructivist perspective to draw out the dominant interpretations of the competition for digital technological leadership between the US, China, and the EU. It uses a method of narrative analysis to explore the different meanings that are intersubjectively attributed to the technological competition and its implications for the power relationship between the three actors. The paper examines Artificial Intelligence (AI) as a paradigmatic case in which narratives of an “AI arms race” have proliferated in recent years. The empirical focus is on official strategy documents from the US, China, and the EU, which are supplemented with expert interviews to reconstruct the narrative dynamics and shifts in this field. Ultimately, this serves to identify the scope for cooperation between the three actors and to minimise risks to international security.

# [2698] The Promise of Track-Two Diplomacy Amidst US-China Tech War

Guangyu Qiao-Franco (Radboud University).

*Abstract*

This paper considers the possible role of 'Track-Two' diplomacy in the wake of a US-China tech war. At a time when official diplomatic engagements between the two countries prove challenging, unofficial Track-Two interactions offer an alternative and promising venue for exploring coordination and cooperation options. We take stock of Chinese Track-Two actors' efforts in resolving growing confrontations with the US in cyber security and AI weaponisation – two fields unique in their greater focus on technical dimensions and the diversity of expertise. Building on insights from practice theory, communities of practice, and boundary work, we understand Track-Two diplomacy as a site of boundary work and those actors involved as 'boundary workers'. An extensive analysis of documentary evidence and interviews with Chinese participants demonstrate that Track-Two actors engage in a complex process of inclusive (e.g., exploring common ground, transmitting insights, and boundary-spanning) and divisive (e.g., establishing differences, drawing boundaries, and strengthening prior beliefs) practices when interacting with their counterparts on the other side. These practices, while both bridging and establishing differences between the two sides, are conducive to fostering "Chinese" approaches to secure cyberspace and military AI applications. These approaches are essentially rooted in practical imperatives whose meanings are contextual-dependent, varying with actors' social experience at the boundaries between the US and China. This paper contributes a new conceptual model to Track-Two scholarship and illuminates the potential of Track-Two initiatives in contributing to US-China Track-One diplomatic efforts and policymaking.

# [2282] Trust in AI: Producing Ontological Security through Governmental Visions

Stefka Schmid (TU Darmstadt), Bao-Chau Pham (University of Vienna) and Anna-Katharina Ferl (Peace Research Institute Frankfurt (PRIF/HSFK)).

*Abstract*

With recent developments in artificial intelligence (AI) widely framed as a potential security threat both in the military and increasingly in the civilian realm, governments have turned their attention to devising regulation to govern AI, its development, and associated harms. In our comparative study of US, Chinese, and EU AI policies, we seek to go beyond purely instrumental understandings of AI as a technological capability, which serves nation states' self-interests and the maintenance of their (supra)national security. In particular we are interested in the mobilisations and enactments of 'trust'. Our specific interest therefore lies in the affective and emotional register that these policies tap into and elicit. Our analysis shows that across governmental documents, AI is perceived as a capability that enhances societal and geopolitical interests while its risks are framed as manageable. This echoes strands within the field of Human-Computer Interaction that draw on human-centered perceptions of technology and assumptions about human-AI relationships of trust, implying notions of interpretability and human control. Despite different innovation cultures and institutional settings, visions of future AI development in all three governmental visions are shaped by this (shared) understanding of human-AI interaction. Nonetheless, the policies differ and are reflective of each government's interest in guaranteeing physical as well as ontological security. We therefore draw on Critical Security Studies and Science and Technology Studies, to ask how different identities play into the production of governmental AI visions and how these visions in turn (co-)produce identities and innovation policies.

# [9728] Maritime Critical Infrastructures Protection: Technical and Political Approaches Beyond the Military

Jonas Franken (PEASEC, Technical University Darmstadt).

*Abstract*

"Lifelines", "Arteries", "Super-Highways", or "Backbone": Anyone researching maritime infrastructures is likely to be struck by the abundance of metaphors used to describe them. On the one hand, these metaphors suggest a lack of familiarity with the subject, although the maritime space currently serves as the essential transit sphere for physical goods and non-material data. On the other hand, they allow for highlighting the enormous societal dependency that has intensified over a long time in a globalized, interdependent world. Though interdependence brought with it the promise of a more peaceful world, there are signs that it is increasingly becoming a security policy lever in the context of geopolitical tensions. Critical infrastructures (CI), while serving the basic needs of societies, have not been prone to this development and have increasingly been used as a platform for geopolitical interaction. Maritime CI in the energy (wind farms, pipelines, oil rigs), ICT (data cables), and transport (cargo shipping) sectors have all suffered sabotages or failures recently, reinforcing the need for better protection of offshore and subsea infrastructures. Although most reactions to the latest events primarily include national navies, the poster will present and discuss various technical and political approaches to make maritime CI more resilient beyond simple military surveillance.

# Workshop and Closing Panel

# [1735] Thinking about the future: Nuclear verification in a complex world

Leonardo Bandarra (Institute of Political Science, University Duisburg-Essen), Stefan Böschen (Human Technology Center, RWTH Aachen University), Andreas Dürholt (International Relations, RWTH Aachen University), René Geiser (International Relations, RWTH Aachen University), Malte Göttsche (Nuclear Verification and Disarmament, RWTH Aachen University), Sophie Kretzschmar (Nuclear Verification and Disarmament, RWTH Aachen University), Irmgard Niemeyer (Nuclear Waste Management (IEK-6), Forschungszentrum Jülich), Linda Ostermann (Human Technology Center, RWTH Aachen University), Lukas Rademacher (Nuclear Verification and Disarmament, RWTH Aachen University), Ralph Rotte (International Relations, RWTH Aachen University), Julian Schäfers (Human Technology Center, RWTH Aachen University) and Carmen Wunderlich (Institute of Political Science, University Duisburg-Essen).

*Abstract*

Close cooperation between policymakers and experts from across sectors and disciplines is essential to successfully address global challenges to peace and security. This is particularly true in the current global context, where social, political, and technological factors are impacting each other and thus form key challenges, such as dealing with the consequences of escalating climate catastrophe or the race to develop and regulate dual-use technologies. However, this cooperation also requires the willingness and the ability for inter- and transdisciplinary engagement. Our workshop provides an opportunity to practice a multi-perspective discussion focussing on a potential future challenge to global security: nuclear non-proliferation and safeguards in crisis situations.

Nuclear safeguards are measures applied by the International Atomic Energy Agency (IAEA) to verify that States comply with their obligations to use their nuclear material and technology for peaceful purposes only. Those measures include, depending on the specific agreement, nuclear material accountancy, containment, and surveillance techniques, and, as a crucial part of the verification activities, on-site inspections. Global developments in recent years indicate that these on-site inspections may become increasingly challenging in the future: Environmental disasters, regional conflicts, or even a new pandemic could limit inspectors' access or even destroy the information needed to verify that no nuclear material has been diverted.

Our workshop will discuss a hypothetical scenario in which IAEA safeguards are applied to a State's nuclear facility under a crisis. Following an introduction to IAEA safeguards procedures, discussions will be held in an interactive world café format. Small groups, supported by facilitators from VeSPoTec, will explore a specific crisis that hinders safeguards activities and approach possible solutions from different perspectives.

Given the unique setting of this conference, we look forward to engaging with a diverse group of natural and social scientists to address questions such as: How can new technologies, such as autonomous systems or developments in satellite imagery, be used in or adapted for crisis situations? How can we ensure the security and reliability of these systems in the light of cyber threats? What is the role of non-state actors, or even civil society, to build confidence in the State not attempting to divert nuclear material? What can we learn from the discussions on resilience of

critical infrastructure to make also nuclear safeguards more resilient? What are opportunities for cooperation in the current geopolitical situation?

The workshop is limited to 40 participants. Prior knowledge on nuclear verification or IAEA safeguards is not required, as all relevant information will be provided in the workshop. For those keen to dive into the topic before the workshop, dedicated material will be made available a few weeks before the conference.

# [7486] New military technologies – fundamental challenges to the international system?

Jürgen Altmann (TU Dortmund University), Anna-Katharina Ferl (PRIF), Niklas Schörnig (PRIF) and Carmen Wunderlich (University of Münster).

*Abstract*

In military research and development important states are pursuing paths that will likely lead to arms races and new levels of destabilisation. Autonomous weapon systems and wider military uses of artificial intelligence as well as cyber-war preparations are seen as central means for maintaining or achieving military superiority, in particular by faster action and reaction. Such "fighting at machine speed" puts into question the capability of human control to prevent escalation. Synthetic biology or human enhancement pose other fundamental problems. Many generic technologies with dual use are becoming more widely accessible; weapons could be very small and be produced in small facilities. If there were a different political climate, many dangerous developments could be contained for the medium term by (preventive) arms control with adequate verification. But given the overall geopolitical landscape, military motives for increased combat strength from new technologies seem to trump arms control efforts. In addition, the new technologies themselves make verification more difficult than ever as a degree of intrusiveness would be needed that would be difficult to accept for armed forces as well as civil society. Both factors may render verified arms control impossible in the long-term future. So, is the old dictum, that arms control is impossible when needed, true after all?

At the end of the conference, the panel is to look back and discuss several fundamental problems, with a view toward tasks for natural-science as well as political-science peace research:

- Details of risks from various new military technologies, from arms races to military destabilisation and the human condition.
- Verification methods for various recommended prohibitions and limits, including required degrees of intrusiveness, directly in armed forces and for preventing misuse in civilian industry and research, and their acceptability in armed forces, in industry and in society at large.
- Norm development, strengthening an enlightened view of national security, that is, the insight that security cannot be guaranteed sustainably by military strength, let alone superiority, but needs to be embedded into international-security mechanisms.
- A longer view for the future of humankind, investigating more fundamental change in the international system – in the direction of a monopoly of legitimate violence in an overarching democratic institution, as it is common within civil societies.
- Intermediate steps on a way toward such an international institution with authority to set as well as enforce rules for the uses of new technology.