Evangelische Akademie Loccum

Cyberwarfare – Cyberpeacebuilding
On a Search for a Cooperative Security Architecture in Cyberspace
April - May 2021
Virtual Discussion Serie, Protestant Academy Loccum

The cyberspace is increasingly marked by a digital arms race. The number of states that run active military cyber programs has grown in recent years. Cyber-attacks and digital disinformation campaigns have become more sophisticated and numerous. With the COVID-19 pandemic and the accelerated digitalization in almost all areas of life, the destructive potentials of cyber conflicts seem to have grown even further.

The international rules-based order is clearly showing various signs of erosion and great power competition is on the rise. The cyberspace is not exempted from this global trend. However, taking the conclusion of two multi-annual UN experts forums on cyber security in Spring 2021 (the OWEG and the UNGEE) as an occasion – we would nevertheless like to brainstorm proposals on how to move closer to a more cooperative security architecture in cyberspace. By this virtual discussion series, we aim to explore the different dimensions of cyber conflicts and elaborate on ideas of how the digital realm could become more stable and secure with the help of international cooperation.

Contact:
Dr. Thomas Müller-Färber, Program Director International Affairs, Protestant Academy Loccum
Tel: +49 5766 81-109 • Mobile: +49 162 75 12 • E-Mail: Thomas.Müller-Färber@evlka.de

28 April
4 - 5:45 p.m. (CET)

Sabotage, Espionage, Subversion – Exploring the Evolving Nature of Cyber Attacks

In recent years, the digital realm has become more violent. There is a constant stream of media reports about detected cyber-attacks and unveiled disinformation campaigns. Due to the COVID-19 pandemic, the digitalization of nearly all areas of life has worldwide taken a big leap forward. Consequently, the future potentials for malicious manipulations of information and communication technology (ICT) have further grown during the recent year. A closer look at this general trend reveals, however, a diffuse situation. The nature of cyber conflicts appears to be composed of a wide range of varying offensive cyber activities ranging from cyber sabotage, over digital subversion to ICT-based espionage. This complexity combined with the clandestine character of cyberattacks makes it difficult to gain a clear picture of the current situation. Against this background, it is the purpose of this session to elaborate on the current and future trends of cyberattacks.

Sven Herpig, Director, International Cybersecurity Policy, Stiftung Neue Verantwortung (SNV), Berlin [confirmed]

Robert Koch, Commander, Scientists, and General Staff Officer, German Federal Armed Forces, Federal Ministry of Defence, Berlin [confirmed]

Eneken Tikk, Cyber Policy Institute (CPI) and Senior Research at the Institute of Software Science at Tallinn University of Technology, Jyyäskylä/Tallin [confirmed]

3 May
4 - 5:45 p.m. (CET)

Escalation All the Way Down? – Exploring the Evolving Nature of Cyber Conflicts

Are we moving in the digital domain steadily towards escalation? Is a cyber armament race inevitable and already unfolding? In recent years, more and more states have launched military cyber activities. It is estimated that about 140 military cyber programs operate today around the world. While these indicators point towards a growing intensity of cyber conflicts, it is important to note that the behavioral pattern in cyberspace is nevertheless marked by a relatively high degree of variety. For example, the nature of military cyber programs differs largely between offensive and defensive agendas. Moreover, the key players in the field seem to follow different goals, strategies, and tactics when it comes to cyber conflicts. The purpose of this session is to elaborate on the changing nature of cyber conflicts and the behavioral patterns show be key players of the digital domain.

Wyatt Hoffman, Research Fellow at Georgetown's Center for Security and Emerging Technology (CSET), Washington D.C. [confirmed]

Monica Kaminska, Postdoctoral Researcher, The Hague Program for Cyber Norms at Leiden University – Institute of Security and Global Affairs, Leiden [confirmed]

Matthias Schulze, Deputy Head, International Security Research Division, German Institute for International and Security Affairs (SWP), Berlin [confirmed]

5 May 2021
4 - 5:45 p.m. (CET)

Needed but Unachievable? Possibilities and Limits of Cooperative Security in Cyberspace

Cyberspace is increasingly marked by a digital arms race. The number of states that run active military cyber programs has grown in recent years. Cyber-attacks and digital disinformation campaigns have become more sophisticated and numerous. Considering these developments, international efforts to regulate the digital domain aiming for de-escalation and stabilization are lacking behind. Since cyber conflicts are inherently transnational and cross-border phenomena, it is difficult to envision long-term mitigation without some degree of international cooperation. But although the UNGGE recommendations of 2015 and several other high-ranking initiatives working on cyber norms have provided in recent years a solid framework for future cooperative efforts, an international arrangement that would at least rudimentarily resemble an arms control agreement is nowhere at sight in the cyber domain. The purpose of this workshop session is to elaborate on the limits and the potentials of a future cooperative security architecture in the digital domain with a particular focus on the lack of political will.

Elena Chernenko, Special Correspondent for Cybersecurity, Non-Proliferation and Arms Control, Kommersant Newspaper and Board Member of the Council on Foreign and Defense Relations and the Council of the PIR-Center, Moscow [confirmed]

Regine Grienberger, Ambassador for Cyber Foreign Policy, German Foreign Office, Berlin [confirmed]

Christopher Painter, President, Global Forum on Cyber Expertise, Member of the Global Commission on the Stability of Cyberspace, and Associate Fellow at Chatham House and the Australian Strategic Policy Institute (ASPI), Washington D.C. [confirmed]

Christian Reuter, Professor for Computer Science, Technical University of Darmstadt and Head of PEASEC (Science and Technology for Peace and Security), Darmstadt [confirmed]

12 May 2021
4 - 5:45 p.m. (CET)

Make Cyber Norms Work: How to Increase Awareness, Augment Adherence, and Bolster Implementation with the Emerging Normative Standards in Cyberspace

In December 2015, the UN General Assembly adopted the Report of the Governmental Experts on cyber norms, rules, principles, and confidence-building measures and thereby established an internationally agreed framework that would make the digital realm more stable, secure, and peaceful. In addition, a consensus was reached that international law applies also to cyberspace – a bone of contention during previous years. Since then, the ecosystem of cyber norms has further grown and have led to more UN groups, expert commissions, industry coalitions, and multistakeholder collectives – for example, the UNGGE, the OEWG, the Paris Call, the Tech Accord, the Charter of Trust, the GCSC, or the Joint Statement on Advancing Responsible State Behavior in Cyberspace. All these different fora and formats have contributed to the emergence of a normative standard of appropriate behavior for states and/or non-state actors in cyberspace. There is certainly room for improvement of the cyber norms that were developed so far. The major challenges, however, lie in improving the actual impact of this emerging normative standard on real-world behavioral patterns in cyberspace. The purpose of this session is to review and deliberate ways and means through which the emerging framework on responsible cyber behavior could exert influence in the future.

Kaja Ciglic, Senior Director, Digital Diplomacy at Microsoft, Ljubljana [confirmed]

Mischa Hansel, Head, International Cybersecurity (ICS), Institute for Peace Research and Security at the University of Hamburg (IFSH), Hamburg [confirmed]

Alexander Klimburg, Director, Cyber Policy and Resilience Program at Hague Center for Strategic Studies and Director of the GCSC Initiative (Global Commission on the Stability of Cyberspace), The Hague [confirmed]

Kerstin Vignard, Head, Support Team to UN General Assembly, UNIDIR (United Nations Institute for Disarmament Research), Geneva [confirmed]

18 May 2021
4 - 5:45 p.m. (CET)

Confidence & Trust – How to Build it in the Digital Domain

Confidence Building Measures (CBMS) were in particular prominent between nuclear powers during the Cold War era. CBMS are meant to address, prevent, or resolve uncertainties among rivals in order to avert unwanted escalations and preserve fragile stability in times of intensified power competition. In recent years, CBMS were introduced into the cyber domain and several organizations – such as the OSCE, the African Union, the G7 or the G20 – gained experience with trust and confidence-building initiatives. Future efforts to establish a cooperative security architecture in cyberspace, will therefore most likely grant CBMS a prominent role. Against this background, it is the purpose of this workshop session to take stock of the CBMS lessons that were made in the past and elaborate on ideas on how these measures could be improved in the future within the cyber domain.

Jürgen Altmann, Lecturer/Researcher, Department of Physics at Technische Universität Dortmund, Co-Founder of the German Research Association for Science, Disarmament and International Security (FONAS), Dortmund/Germany [confirmed]

Erica Borghard, Senior Fellow at the Atlantic Council and Senior Director of the Cyberspace Solarium Commission, New York [confirmed]

Andreas Kuehn, Senior Fellow, Cyberspace Cooperation Initiative, Observer Research Foundation America (ORF America), San Francisco [confirmed]

Szilvia Tóth, Cyber Security Officer, Secretariat of the Organization for Security and Co-operation in Europe (OSCE), Vienna [confirmed]

20 May 2021
4 - 5:45 p.m. (CET)

No Bigger Problem Than Cyber Attribution? How to Increase Transparency and Improve Monitoring in the Digital Realm

A working cooperative security architecture does require a certain level of transparency between the involved actors. An agreed transparency scheme decreases the level of mistrust and provides a fundament for taking joint actions against irresponsible behavior. In cyberspace, independent, reliable, and non-politicized monitoring and verification are widely lacking. What we witness instead is a relatively high degree of finger-pointing and naming-and-shaming. It is often said that the so-called attribution problem is the most important obstacle to transparency in the digital domain as it lowers substantially the chance to ascribe cyber-attacks and disinformation campaigns to the responsible actors. Therefore, conventional monitoring and verification methods – such as on-site inspections, sensor installations, or areal images – that are used with regard to other military technologies and weapon categories are unlikely to operate properly in cyberspace. However, in recent years several ideas were floated and proposed how to increase transparency in the digital domain and to handle the attribution problem. The purpose of this session is to elaborate and evaluate these proposals and sketch out an outlook about the future development of the debate on cyber monitoring.

Erin D. Dumbacher, Senior Program Officer, Scientific and Technical Affairs, Nuclear Threat Initiative (NTI), Washington D.C. [confirmed]

Serge Droz, President of the Forum of Incident Response and Security Teams (FIRST), Senior Advisor of ICT4Peace, and Senior Security Engineer at ProtonMail, Zürich [confirmed]

Ivan Kwiatkowski, Senior Security Researcher at Global Research and Analysis Team (GReAT), Kaspersky, Paris [confirmed]

Jonathan William Welburn, Operations Research at RAND and Professor at Pardee RAND Graduate School, Santa Monica [confirmed]