EU Non-Proliferation and Disarmament Consortium

Promoting the European network of independent non-proliferation and disarmament think tanks

June 2021, Issue No 33
Subscribe:eunpdc@sipri.org
f.dallarche@iai.it

nonproliferation.eu

Genetic Engineering Technologies and Their Weaponisation Potential: Interview with Mirko Himmel

Mirko Himmel is a scientist at the University of Hamburg, Germany. His research focuses on biological and chemical arms control at the Centre for Science and Peace Research and on infection biology at the Department for Microbiology and Biotechnology. There, his laboratory-based studies focus on molecular mechanisms of infections caused by bacterial pathogens and the development of risk assessment strategies for new genome editing technologies. Furthermore, in a pilot study he investigates Technical Confidence Building Measures for the Bioweapons Convention. He also lectures on biomedical ethics at the university and provides biosecurity advice to students and governmental authorities.

In your work as a Scientist at the Bio laboratory at the University of Hamburg, you cover bioethics, biosecurity and preventive biological and chemical arms control. Specifically, what type of work does the laboratory conduct in the arms control and non-proliferation field?

Laboratory work related to arms control performed at the Department for Microbiology and Biotechnology include the development of Technical Confidence Building Measures usable within the Bioweapons Convention regime and the establishment of strategies for the risk assessment of emerging biotechnologies. The first approach is based on proposals made in 1993 by a group of verification experts. Inspection and compliance monitoring measures were identified which could be optimised using modern technologies. Our aim is to spark discussions about improved transparency building rather than coming up with a one and only verification method. The second approach is focused on risk assessments of new genome editing technologies. Here, we benefit from being embedded in a department performing both basic and applied research. Hands-on knowledge about pros and cons of these techniques provides us with a better understanding of misuse potentials resulting in a balanced view about risks and benefits of emerging biotechnologies.

In a recent publication, you explore the issue of genetic engineering technologies, stressing that they have a threatening misuse potential. Examples are synthetic biology and genome editing (i.e. CRISPR/Cas9). Could you tell us more about these technologies? Can they be weaponised? To what extent do they pose a proliferation risk?

Synthetic biology (SynBio) as opposed to conventional biotechnologies, aims to create novel artificial biological pathways (e.g. to produce pharmaceuticals), organisms or biological devices (e.g. controllable nano-devices). New genome editing technologies such as CRISPR/Cas do have many beneficial uses in biomedicine and in SynBio.

From the perspective of preventing arms control, SynBio methods are categorised as enabling techniques which could be misused for the development of weapons of mass destruction. Of course, this phenomenon is not new, again highlighting the existence of dual-use potentials in many if not all scientific disciplines. Proliferation risks associated with SynBio include technologies, products and knowledge transfer. In theory, all this could make it easier to develop biological warfare agents, but there are still experimental obstacles to their direct use for non-peaceful purposes. Given these technological difficulties related to genetic engineering technologies, the use of conventional biotechnologies for generating weaponised biological agents might still be attractive to malicious actors.

How can the EU respond to the arms control and non-proliferation challenges deriving from these technologies?

Emerging technologies require enhanced flexibility in the way the EU conducts non-proliferation and export control activities. Especially, catch-all control measures require a deep understanding of the proliferation risks associated with emerging technologies. Therefore, non-proliferation measures should focus more on the context of use of biotechnologies rather than on individual technologies. Electronic dual-use assessment tools plus e-learning module could assist exporters in academia and help create an environment close to the vision of a CBRN security culture proposed by the EU. Harmonisation of national export control measures and extended information exchange would help EU member states to fulfil their duties. Awareness raising activities should focus on industry and academia and include researchers, students but also technical personnel. But we should keep in mind how important freedom of research is. The right balance between non-proliferation activities and international scientific cooperation that overcomes mistrust will provide most benefits to the EU.

EXPORT CONTROLS ON CYBER-SURVEILLANCE ITEMS

With the long discussed and recently adopted Dual-Use regulation, the EU has finally taken an important step to better connect human rights and export control regimes. Considering the ever-growing digital nature of our communications and social interactions - creating huge stockpiles of digital traces and individual fingerprints - this move was long overdue.
Given the experience of a similar adjustment of the Wassenaar Arrangement in 2013, the "catch-all" approach should be suitable to keep pace with the constant challenge of new technological developments. Yet, while the new controls on "technical assistance" close certain gaps, other loopholes remain.
First and foremost, the new regulation delegates a major part of the decision of what is required to get licensed to the exporter, leaving room for interpretations and legal disputes. Whereas the questionable incentive for compliance of exporters will require joint measures to monitor exports, sanction unlawful activities and set standards for appropriate due diligence, these measures are prone to become subject to national economic, security and political interests. The same is true for the EU wide annual report on exports, which requires national notifications to be carried out extensively and regularly in order to work as a measure of transparency. Even the possibility for additional national licensing requirements holds the potential for separate, diverging approaches. While frequent events show that the military application of cyber tools can directly harm civilian IT systems – like critical infrastructures – it is difficult to understand why this is regulated under "technical assistance" but not part of the actual definition of regulated goods. Finally, the problem of controlling software and its proliferation still persists. This is too easily subverted, proving the proposed end-uses and end-users internal compliance programmes (ICPs) to be paper tigers if not supported by controlling cooperation at an international scale. In the end, the updated regulation is a necessary measure and important political signal, but it can only be the first step towards establishing an effective export control regime that holds up to the rapid pace of technological development.

Thomas Reinhold
Science, Science and Technology for Peace and Security (PEASEC) / EU Non-Proliferation and Disarmament Network

Latest Publications

Autonomous Weapon Systems and International Humanitarian Law: Identifying Limits and The Required Type and Degree of Human-Machine Interaction, Vincent Boulanin, Laura Bruun and Netta Goussac, Stockholm International Peace Research Institute (SIPRI), 2021

Cyber Capabilities and National Power: A Net Assessment, the International Institute for Strategic Studies (IISS), 2021

The Next 50 Years of Missile Proliferation, Xu Tianran, Melissa Hanham, One Earth Future, 2021

Stealing Precious Steel: Firearms Theft in the European Union, Quitterie de Labbey, Nils Duquet, Lore Smets, the Flemish Peace Institute, 2021

Network Calls

FULL TIME RESEARCHER

The Institute for Peace Research and Security Policy at the University of Hamburg (IFSH) is seeking to hire a researcher. The position falls under the IFSH research area European Peace and Security Orders and the Centre for OSCE Research (CORE).

Deadline: 28 July 2021
More info: **here** or contact
Dr. Habil Cornelius Friesendorf

RESEARCHER, DOCTORAL AND POST-DOCTORAL POSITIONS

The Institute of Strategic and Defense Studies (IESD) is offering six positions as Researcher, Doctoral and Post-Doctoral.

Deadline: 13 July 2021
Positions to be filled by:
1 September 2021
More info: here

CONSORTIUM NEWS

The EU Non-Proliferation and Disarmament Papers Series

As part of its mandate, defined in Council Decision (CFSP) 2018/299 of 26 February 2018, the EU Non-Proliferation Consortium is publishing a new series of Non-Proliferation and Disarmament Policy Papers. One of the latest papers is co-authored by Dr Tatyana Novossiolova and Prof. Maurizio Martellini.

Effective and Comprehensive CBRN Security Risk Management in the 21st Century

Summary

The multifaceted nature of security concerns related to the proliferation of weapons of mass destruction (WMD) in the 21st century requires a novel organising principle for the international multilateral efforts focusing on the prevention of the hostile misuse of chemical, biological, radiological and nuclear (CBRN) knowledge and materials. At the heart of this security paradigm is the need to strengthen established international norms against the development, spread and use of WMD, and ensure the comprehensive in-depth implementation of relevant regulatory instruments through the internalisation of safety and security practices, procedures and behaviours among relevant professional communities. This paper argues that effective CBRN security risk management requires the integration of national, regional and international strategic approaches that promote and uphold the norms of WMD non-proliferation and disarmament.

Read the full paper here
Previous papers can be found here

NETWORK NEWS

CYBER-SECURITY, NUCLEAR WEAPON SYSTEMS AND STRATEGIC STABILITY

On 27 May 2021, the Interdisciplinary Group on Science, Technology and Society (GISTS) of the Pisa Campus of the Italian National Research Council (CNR), in collaboration with several other academic and scientific institutes, organised a webinar on Cyber-security, Nuclear Weapon Systems and Strategic Stability.

The webinar has addressed issues related to the Cyber-security of Critical Infrastructures and the implications of Cyber and Space dependency on Nuclear Assets and Strategic Stability. Information technologies play a fundamental role in both civilian and military systems. Vulnerabilities caused by malfunctions and errors in the design or implementation of digital systems are exploited for attacks on them, with consequences that sometimes also result in physical damage. The level of insecurity and uncertainty that this situation entails is particularly dangerous, especially in relation to nuclear systems and nuclear weapons, and can have important negative repercussions on crisis management and strategic stability.

Dr. Domenico Laforenza (CNR) has elaborated on the EU strategy for ensuring cyber-security as well as the formal, normative steps taken in Italy to that purpose. Subsequently, Dr. Beyza Unal (Chatham House) addressed issues concerned with risk analysis on the impact of cyber on national infrastructures and nuclear weapons systems, emphasising the criticalities and discussing possible approaches to mitigation. The potential impact on crisis management of the instability created by cyber-attacks, or computer malfunctions have also been addressed and thoroughly discussed.

More information can be found below:
Cyber-security, Nuclear Weapon Systems and Strategic Stability
Interdisciplinary Group on Science, Technology and Society (GISTS)
Italian National Research Council

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the EU NPD Network and do not necessarily reflect the views of the European Union