

EU Non-Proliferation and Disarmament Next Generation Follow-Up Meeting

Virtual Event, 13 April 2021
by Federica Dall'Arche and Alice Fill¹

Due to the current COVID-19 pandemic, there are currently few opportunities for the Next Generation to meet around the world and think together about the great challenges of our times. With these words, **Elena Sokova**, Executive Director of the Vienna Center for Disarmament and Non-Proliferation (VCDNP), opened the 2021 "*EU Non-Proliferation and Disarmament Next Generation Follow-Up Meeting*".

The event - jointly organized by the VCDNP and the Istituto Affari Internazionali (IAI) within the framework of the [EU Non-Proliferation and Disarmament Consortium](#) - follows the [Next Generation Workshop](#) on non-proliferation and disarmament, an initiative held annually that brings together outstanding young scholars, students and professionals to present fresh ideas and solutions to current non-proliferation and disarmament challenges.

As stressed by **Ettore Greco**, the Executive Vice President of IAI, it is indeed essential to substantially involve the younger generation on these issues in order to not only identify gaps and barriers in the existing policies, but also to let fresh ideas and new perspectives help to promote innovative forms of cooperation in an era of daunting challenges for multilateralism. Under the same auspices, the [Young Women in Non-Proliferation and Disarmament Mentorship Programme](#) was launched during the same week.

The Follow-Up Meeting was attended by more than 120 participants, including women and girls from all over the world and with the most diverse backgrounds. The event was organised in two tracks: a first track was highly informative, during which two prominent experts addressed respectively bio-security challenges related to the COVID-19 pandemic and the most current cyber security concerns in relation to non-proliferation. The second track of the event was dedicated to a “networking” activity. Noting that the COVID-19 pandemic has left many young individuals isolated and detached from ongoing activities and has severely limited academic exchanges and training opportunities, the goal of the second track was to provide a framework for young people to meet, exchange ideas and promote their work.

View the meeting agenda.

The Impact of COVID-19 and other Bio-Security Challenges

The first topic was addressed by **Filippa Lentzos**, Senior Research Fellow at the King's College London. As pointed by **Federica Dall'Arche**, Researcher at IAI and moderator of the panel, the topic was particularly timely due to recent discussions on the origin of the virus. In order to reach an assessment of the health and societal impacts caused by COVID-19, Filippa Lentzos walked the participants through an accurate and anguished timeline of the pandemic stressing, in particular, the evolution of the Chinese government's narrative on the spread of the virus, the role of the World Health Organisation and the progressive recognition of the modalities of human-to-human transmission. As the pandemic escalated, however, even today many questions remain unanswered, according to Lentzos. The direct impact of the virus on health is still poorly understood and the extent of the indirect and long-term consequences will only fully emerge with time. The enormous socio-economic effects of the virus, however, are already

¹ Alice Fill is a Spring 2021 intern at the Istituto Affari Internazionali;

Federica Dall'Arche is the Non-Proliferation and Disarmament Researcher at the Istituto Affari Internazionali

pretty clear. Lentzos noted how the virus led to the disappearance of 225 million full-time jobs around the world and has exacerbated long-standing economic, racial and gender divides. Women, in particular, are paying the highest price, comprising 70% of global health and social care personnel. In addition to the consequently increased exposure to risk, women are also victims of what UN Women has called “the shadow pandemic”, *i.e.* a worrying increase in gender-based violence and domestic violence.

While the effects of the pandemic still remain at least partially unknown, this is even more true for its origin. As essential as it is to reconstruct a clear picture of what happened to reduce the risk of the introduction of new viruses to the human population, we still know little about the time, place and causes that led to the break out of COVID-19. “What should have been a routine science question” Filippa Lentzos argued, “has instead become extremely politically charged”. In early April 2021, a WHO-China Joint Mission on COVID-19 released a study listing four different possibilities on the origins of the outbreak of the pandemic: the first hypothesis listed is that the virus jumped from an animal directly to a human; the second, that the virus jumped from an animal to an intermediate host and then to a human; the third hypothesis is that the virus was imported to China via frozen food; the last hypothesis is that it spread because of a lab-leak. While, according to the report, the second theory seems to be the most likely, the joint nature of the report raises significant doubts on its mandate and independence. Additionally, the lack of adequately grounded evidence to favour one hypothesis over the other is also a cause of particular concern, according to Lentzos. Yet, understanding the origin of COVID-19 would be essential to strategize on how to prepare for future pandemics.

Lentzos concluded her remarks noting that biological threats are not limited to the current pandemic. Among others, she included: the potential accidents in Biosafety laboratories - currently under-monitored and under-regulated; deliberate biothreats caused by a growing technical capacity to modify pathogen and transfer them to the human body; and biological information warfare possibly targeting specific individuals or groups. Remarkably, the effects of biological information warfare are substantially indifferent from those of real, internationally prohibited biological warfare: this makes disarmament efforts particularly difficult.

Cyber Security and Implications for Non-Proliferation

The relevance of cyber security, as reminded by *Mara Zarka*, Project/Events Manager and Research Associate at the VCDNP and moderator of the second panel, has recently been brought into the spotlight because of the alleged cyber-attack to the Natanz nuclear plant, in Iran. Although cybersecurity has been on the policymaking eye for over a decade, these events show that the answers we have come up with still remain largely unsatisfactory. According to *Alexi Drew*, Postdoctoral Research Associate at the Policy Institute at King's College London, “most of the cyber issues that we see in international security arise out of a lingering series of misperceptions about what cyber security actually is, and who does it”, she argues. The actors involved are indeed changing rapidly with drastic consequences within the arms control arena: what was traditionally negotiated between States and within international institutions, is now addressed in far more complex negotiations because of the growing role of the so-called cyber emerging technologies. As a consequence, continued Drew, today private industries are the new predominant group of actors shaping the cyber security field, with a variable-geometry role left to the States. Remarkably, both private actors and States are increasingly aware of the new balance of power and of who can really set the standards: cutting-edge technology is no longer directed solely by States’ interests, with enormous consequences on international governance dynamics. In fact, according to Drew, while technology might seem neutral and apolitical, it is the result of ethical and political choices: the kind of decisions now happening are about the importance of privacy in the next-generation technologies and algorithms, or about how domestic and international standards should be set. And these standards are increasingly set by private actors.

Another crucial and often underestimated aspect of cyber security has to do with supply chains that contribute to creating broader attack surfaces, linking private and public digital infrastructures. However, as Alexi Drew explained, not everything that takes place in the cyber space can or should be considered as a form of warfare: in the large majority of cases, it is about cyber espionage, never intended to cause damages. This difference is widespread and yet difficult to explain, since it is incidents such as the one that happened at the Natanz nuclear plant – actually intended to cause damages – that make the headlines. The consequent general failure in grasping these nuances between espionage and attacks remains one of the main barriers to effective policymaking on cyber security. The key of the instability risk that should be addressed by cyber security is indeed the possibility of escalation due to lack of knowledge, a lack resulting from a deliberate policy on the side of both States or institutions involved in the cyber event. For instance, NATO members have never defined the standard beyond which a cyber incident can be considered a full-fledged attack, thus expanding the deterrent potential: however, this makes it hard to establish where the line is and represents a critical risk of escalation or “splash effect”. Drew concluded her remarks noting that cyber capability is rapidly proliferating, both in terms of defence and attack capabilities.

Networking session

During this session, participants were divided in groups and provided with ice-breaking questions. The discussion in the different groups covered both the main pressing challenges to non-proliferation and disarmament as well as ways in which the EUNPDC and its members could do to better engage the next generation and young women in the field.

The main takeaways of the sessions are compiled in the document “*Networking Session Takeaways*”

