INTERNATIONAL CYBER CRISIS MANAGEMENT WORKSHOP

An online workshop co-hosted by the European Union Institute for Security Studies (EUISS) and the United Nations Institute for Disarmament Research (UNIDIR) to discuss the relationship between the technical and political crisis management necessary in the cyber realm; cybersecurity efforts of Member States including through the implementation of norms and Member States' expectations on the role of the UN in how regional organizations address cyber insecurity and prevent and manage cyber crisis.

Summary report

Significant cyber incidents across the globe have been rapidly increasing at an exponential rate, proliferating not only in terms of volume but also in terms of gravity. Malicious cyber actors have steadily targeted critical state infrastructure, defence telecommunications, and social media accounts of prominent government figures. As recent examples show, the cyber component is omnipresent in modern conflict: before, during, and in the aftermath of kinetic action. In the face of this challenge, we must raise the necessary first line of defence. Regionally, we have seen the adaptation of relevant legislative frameworks, but also more radical attempts to increase resilience and tackle this problem operationally. It is becoming increasingly obvious that these efforts should be complimented and further supported by the multilateral system. The UN Common Agenda is permeated by a firm ambition to increase engagement with and amongst Member States, to help foster a culture of accountability and adherence to principles of responsible state behaviour in cyberspace. The challenge today is to give practical relevance to these principles. How could a regional cyber crisis be triggered? When does an incident become a crisis? What kind of regional tools or mechanisms would be applicable?

Panel 1, moderated by **Dr Samuele DOMINIONI**, discussed the EU perspective on confidence-building measures (CBMs) and the operationalization of the normative framework for responsible state behaviour currently established on a UN level. **Ms Joanneke BALFOORT** considered available diplomatic responses to malicious cyber activity, including the Cyber Diplomacy Toolbox (CDT). It is important that the EU continues to seek enhanced cooperation with international partners, both in bilateral and multilateral settings. **Ms Lorena BOIX ALONSO** addressed the systematic and cross-sectorial nature of cyberattacks, while emphasizing how the EU's policy framework on cybersecurity (including the 2020 EU Cybersecurity Strategy and the Blueprint) gives great prominence to cyber readiness and coordination mechanisms amongst cyber communities to ensure the implementation of collective responses. **Ambassador Tadeusz CHOMICKI** noted that cybersecurity is the most transnational and most transectorial area of security, which renders international cooperation instrumental for ensuring collective responses and mitigating measures to these complex threats. While the cyber policy domain is generally pervaded by a 'silo' attitude, we need to establish links across the technical, operational, legal, political, and international dimensions.

Panel 2, moderated by **Ms Moliehi MAKUMANE**, looked at the EU's regional approach to cyber crisis management and investigated the EU's added value in supporting resilience and coordination amongst different actors and stakeholders. **Dr Patryk PAWLAK** outlined the EU's existing policy framework, identifying different response mechanisms and corresponding actors. The complexity of cybersecurity challenges calls for a comprehensive strategy that would provide an overarching direction to regulatory action and could act as a multiplier of the impact of national strategies. At the same time, it is important to develop a robust institutional ecosystem through information exchanges and joint exercises, as well as to foster cooperation amongst agencies at different levels through directories and standard operating procedures. **Mr. Philipp AMANN** discussed the role of law enforcement in developing holistic response mechanisms to cyber crises. He explained

how large-scale cyberattacks NotPetya and WannaCry triggered the adoption of the EU Law Enforcement Emergency Response Protocol, which represents a key basis for coordinating the law enforcement response to cyber crises in line with the Blueprint. It is important to formalise this coordination and ensure that we have communication channels, standardized taxonomies, and shared institutional assessments together with other partners within the EU institutional ecosystem and potentially beyond.

Panel 3, moderated by **Dr Andraz KASTELIC**, assessed EU-UN cooperation in tackling cyber crises. **Dr Camino KAVANAGH** outlined the general expectations of Member States from the UN, both prior to the emergence of a crisis (e.g. continuing to facilitate discussions on how ICTs could be used as disrupters of international peace and security, promoting regular dialogue with and between regional/sub-regional organisations, developing tabletop exercises and similar mechanisms to test existing tools) and in response to a crisis (e.g. involving the Security Council, calling for briefings to provide insight into certain situations, deploying good offices to de-escalate tensions). At the end of the day, the UN can only do whatever its Member States allow it to do; in that sense, the EU can offer a lot of added value. **MrGert AUVÄÄRT** recounted the Estonian experience at the UN Security Council and explained how this institutional body can meaningfully contribute to setting the rules of the road on what is acceptable and what is not. Those who wish to push these discussions forward need to adopt an ambitious, principled, and open mindset, as well as to recognize the potency of setting precedents. Participants also discussed the need to streamline cybersecurity and cyber hygiene policies across all areas of the UN's work, given that any UN mission or mandate nowadays involves the use of ICT solutions, and any breakdown can have an immediate impact on the delivery of the UN's mandate.

The workshop's concluding remarks, delivered by **Dr Giacomo PERSI PAOLI,** identified two thematic clusters. The first concerned preparedness (i.e., in the development of CBMs and policy frameworks), while the second concerned response and crisis management. The EU is clearly a leading actor, especially within the thematic reach of the first cluster, in that it has created a strong preparedness bubble. This bubble, however, is not always impermeable. When it comes to responding, there are plenty of possibilities and solutions available, which are nevertheless largely subject to political assessment and therefore to national prerogative. To what extent is the EU learning from its past and exploring how regional mechanisms could be challenged by internal divergences? How could the assessment of a cyber incident vary within the frame of a heightened political context? Finally, participants overwhelmingly saw a need for further EU-UN collaboration on an operational level, especially in conducting joint exercises that may provide solutions to possible real-life scenarios.