Cyberspace, and in particular the global, open Internet, has become one of the backbones of our societies. An open, free, stable and secure cyberspace is important for continued global development and prosperity. Cybersecurity is therefore a global challenge, which requires international engagement, collaboration and coordination amongst all stakeholders to preserve a functioning and stable cyberspace, supporting access to and unhindered, uncensored and non-discriminatory use of open and secure information and communication technologies (ICTs), fostering open societies and enabling economic growth and social development globally, in line with the UN’s Sustainable Development Goals.

The role of cyber capacity building is central to contribute to the above-mentioned goals. Such efforts should focus on assisting countries to develop the skills and capacities necessary to address cyber threats adequately and thereby to advance peace and security. With this in mind, the EU and its Member States presently focus external cyber capacity building initiatives on addressing cybercrime and increasing cybersecurity in partner countries and regions, with an emphasis on reforms across the main dimensions of cyber resilience, namely by supporting an overarching strategic framework, promoting legislative reforms and increasing the capacities of the criminal justice system, developing and increasing incident management capabilities, developing education, professional training and expertise in this field and promoting cyber hygiene and awareness as well as culture of security assessment of digital products, processes and services in compliance with European and international standards and best practices.

In turn, this capacity building approach incorporates a number of key principles. Notably:

- the understanding that existing international law and norms apply in cyberspace;

- rights-based and gender-sensitive by design, with safeguards to protect fundamental rights and freedoms;

- in line with the democratic and efficient multi-stakeholder internet governance model;

- supports the principles of open access to the Internet for all, and not undermine the integrity of infrastructure, hardware and services;

- supports a shared responsibility approach that entails involvement and partnership across public authorities, the private sector and citizens and promotes international cooperation.

Furthermore, wider lessons from development cooperation should be taken into account in external cyber capacity building efforts in order to enhance effectiveness and sustainability. Notably, we aim to:

- ensure that partner countries enjoy full ownership of the development priorities in relation to cyber resilience;

- focus on sustainable results through the promotion of broader policy, legal and technical reform processes instead of ad-hoc, one-off activities;
- ensure that trust, transparency, accountability and shared responsibility are the driving force behind assistance.

The EU and its Member States support further engagement with key international and regional partners and organizations as well as with civil society, academia and the private sector in this field with the aim of avoiding duplication of effort, and looking for opportunities for synergies and burden-sharing, in order to support coordination and coherence in our collective efforts. In that regard, the EU welcomes the coordination role of the Global Forum of Cyber Expertise, as well as efforts to elevate the issue including at the World Economic Forum, the Internet Governance Forum, and through the Paris Call. The EU and its Member States strongly support initiatives enabling the exchange of best practices on the development of capacities to address cyber incidents.

The EU and its Member States recognize that cyber capacity building efforts are important in order to develop minimum capacities necessary for the implementation of regional cybersecurity confidence building measures such as those led by the OSCE, the ASEAN Regional Forum and the OAS, as well as for the implementation of rules, norms and principles of responsible State behaviour as set out in the 2013 and 2015 reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE).

In accordance with the need to focus our collective efforts on developing the skills and capacities to address cyber threats adequately and to advance peace and stability through effective implementation of the norms, rules and principles of responsible state behaviour and the application of international law in cyberspace, the EU will continue the prioritisation and exchange of information on cyber capacity building activities in bilateral dialogues with partners as well as at relevant international and regional fora.

Furthermore, the EU has developed operational guidance for EU-financed cyber capacity building in order to provide a comprehensive practical framework when designing and implementing the EU’s external actions against cybercrime and for promoting cybersecurity and cyber resilience¹.

The EU supports cyber capacity building work through its External Financing Instruments, which encompass a range of programmes with a global reach including actions being implemented in Africa, Asia and Latin America, as well as the Western-Balkans. Concretely, the EU is currently investing more than €100 million in cyber capacity building activities worldwide, to support their implementation, in cooperation with its implementing partners, through projects such as EU’s Cyber-Resilience for Development, Glacy+ and EU Cyber Direct. The EU looks forward to deepening its cooperation with UN member states with the aim of extending this work.