# TOWARDS A GLOBAL CYBER RESILIENCE FRAMEWORK

EU CYBER DIRECT

**Brainstorming session**

14 November 2019, Justus Lipsius, EUISS meeting room 00-FG-10

## Rationale

Several key EU documents, such as *A Global Strategy for the European Union's Foreign and Security Policy and EU Cyber Security Strategies (2013 and 2017)* recognise the importance of resilience, including in the international context. In all those documents the EU's dependence on the resilience of IT systems and infrastructure is one of the key challenges the EU faces nowadays. Resilience is built through both internal and external initiatives, including through close cooperation with international partners. Moreover, supporting efforts to build national resilience in third countries will increase the level of cybersecurity globally, with positive consequences for the EU. This is why since 2013, the EU has been leading on international cybersecurity capacity building and systematically linking these efforts with its development cooperation. Furthermore, joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced need to be taken into account.

Promoting cooperation in a whole-of-society model, capacity building and increasing cyber resilience are as well part of the overarching objective to maintain an open, stable and secure cyberspace and to build bridges between all actors. In this respect, a global cyber resilience framework/regime could contribute to a strategic framework for conflict prevention, cooperation and stability in cyberspace that is based on the application of existing international law, in particular of the UN Charter in its entirety, the development and implementation of universal norms of responsible state behaviour, and regional confidence building measures between States. Strengthening resilience is a way to increase the EU's capacity to deal with the negative consequences of cyber-attacks and consequently to reduce the risk of overreaction, miscalculation and conflict.

This is why there is a need to have a holistic reflection into what a global cyber resilience framework could look like. Building on the initial workshop on resilience held in October 2018, this brainstorming session/workshop will aim to:

- Identify key objectives that a global cyber regime/framework should aim to achieve.
- Identify key elements of the global cyber regime/framework.
- Identify key actors of the global cyber regime/framework.
- Design the process and mechanisms to achieve set objectives.

Implementing organisations

ISS European Union Institute for Security Studies

G|M|F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Stiftung Neue Verantwortung

This project is funded by the European Union.

# Objectives

The goal of the workshop is to define a common European approach towards a global cyber resilience regime through:

- Listing and prioritising EU's strategic interest in building a global cyber resilience framework;
- Mapping the existing international and national initiatives through which these interests are already pursued as well as identifying the existing gaps in the global governance of cyber resilience
- Identifying most effective way to achieve those priorities, either through existing platforms or the new ones.

The meeting will take the form of an informal moderated discussion. Each session will include short presentations by input givers.