# EU-JAPAN JOINT RESPONSES TO MALICIOUS CYBER ACTIVITIES

# EU-JAPAN CYBER WORKSHOP

**10 December 2019**

The East Research Building, Mita Campus, Keio University Global Research Institute, Tokyo

EU-Japan cooperation on resilience, confidence building, and international norms in cyberspace is based on shared values and matching threat perception. The EU and Japan have implemented different actions to prevent, detect, and react to malicious cyber activities and having embedded those measures in overall cybersecurity and defence strategies (i.e. the EU Cyber Diplomacy Toolbox, the Blueprint for cyber crisis response, or Japan's updated defence and cybersecurity strategy). The Strategic Partnership Agreement between the EU and Japan which concluded in December 2018 identified cybersecurity as one of the areas for deeper security cooperation. While both sides recognize the risks posed by malicious activities in cyberspace the discussions about possible joint responses in the case of high impact cyber incidents affecting Japan, the EU or both are in their nascence. Consequently, this workshop will focus on discussing modalities for possible joint EU-Japan responses and testing them based on the experiences learnt from "WannaCry". The guiding question for the cyber workshop is "How can the EU and Japan jointly respond to malicious cyber activities?". Specific objectives include:

- To increase understanding of responses to prevent, detect and react to malicious cyber activities that are available to the EU and Japan;
- To identify common concerns, goals of responses, response mechanisms and challenges for joint EU and Japan response;
- To discuss joint responses and their possible effects and limitation using different scenarios

Additional issues that will be addressed during the meeting include threat landscape, goals, mechanisms, roles and central challenges of joint responses. Each session will be built around interventions of two input speakers from European and Japan respectively.

## About EU Cyber Direct

The EU Cyber Direct project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rights-based international order in cyberspace through extensive dialogues with strategic partners from Brazil, China, India, Japan, South Korea, the United States, as well as regions of Latin America and the Asia-Pacific. The project brings together governments and non-governmental actors to explore the main issues surrounding international law in cyberspace, norms of responsible state behaviour and Confidence Building Measures. EU Cyber Direct is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

This event is co-organised with

Implementing organisations

This project is funded by the European Union.

# Agenda

## 9:00-9:30 Registration and welcome coffee

## 9:30-9:45 Opening remarks

**Jiro Kokuryo**
Professor and Vice-President, Keio University

**Rosa Balfour**
Senior Fellow, The German Marshall Fund of the United States, Belgium and Project Manager of EU Cyber Direct

**Isamu Yamaguchi**
Director, New Security Challenges Division, Ministry of Foreign Affairs

*Moderation*
**Ken Katayama**
Keio University Global Research Institute

## 9:45-10:45 Finding common concerns

1) What are the EU's and Japan's main concerns when looking at the current threat landscape of malicious cyber activities?
2) What do you think are the major common concerns the European Union and Japan have regarding malicious cyber activities?

Inputs by governmental speakers from Japan and the European Union
**Jun Osawa (TBC)**
Nakasone Peace Institute
**Michael Gams**
Senior Analyst Cyber Issues at European External Action Service (EEAS), EU Intelligence and Situation Centre (EU INTCEN), Intelligence Analysis Division / Hybrid Fusion Cell

*Moderation*
**Julia Schuetze**
Project Manager, Stiftung Neue Verantwortung
**Sven Herpig**
Project Director for International Cyber Security Policy, Stiftung Neue Verantwortung

## 10:45-11:30 Identifying joint goals

1) What are the EU's and Japan's main goals when responding to malicious cyber activities?
2) What are goals that Japan and the European Union have in common when responding to malicious cyber activities?

Inputs by governmental speakers from Japan and the European Union
**Wiktor Staniecki**
Head of Cyber Sector, Security and Defence Policy Division, EEAS
**Isamu Yamaguchi**
Director, New Security Challenges Division, Ministry of Foreign Affairs

*Moderation*
**Julia Schuetze**
Project Manager, Stiftung Neue Verantwortung
**Sven Herpig**
Project Director for International Cyber Security Policy, Stiftung Neue Verantwortung

## 11:30-11:45 Coffee/tea break

## 11:45-13:00 Discussing Joint Response

1) What are the EU's and Japan's main responses to prevent, detect and react to malicious cyber activities?
2) What are responses that the EU and Japan should implement together to prevent, detect and react to malicious cyber activities?

Inputs by experts from Japan and the European Union
**Ken Katayama**
Keio University Global Research Institute
**Patryk Pawlak**
Brussels Executive Officer, the European Union Institute for Security Studies

*Moderation*
**Julia Schuetze**
Project Manager, Stiftung Neue Verantwortung
**Sven Herpig**
Project Director for International Cyber Security Policy, Stiftung Neue Verantwortung

## 13:00-14:00 Lunch break

## 14:45-16:00 Scenario based discussion "WannaCry"

The participants will be presented with a realistic scenario that has affected Japan and the European Union in the past - "WannaCry". In groups, participants will discuss the following questions

- Would responses look differently today?
- What joint responses could and should be taken in the future?

*Moderation*
**Ken Katayama**
Keio University Global Research Institute
**Yukako Uchida**
JPCERT/CC
**Julia Schuetze**
Project Manager, Stiftung Neue Verantwortung
**Sven Herpig**
Project Director for International Cyber Security Policy, Stiftung Neue Verantwortung

16:00-16:30 Presentation of Group Work

16:30-17:00 Coffee/Tea break

17:00-18:00 Development in Cyber Diplomacy (Organized by Mitsubishi Research Institute)

1) What is the political feasibility of ideas discussed in the workshop?
2) How can the public and private sector contribute to cyber diplomacy?
3) How has cyberspace affected international security environment?
4) What does state practice reveal about diplomacy in cyberspace?

*Moderator*
**Dai Mochinaga**
Senior Researcher, Keio Research Institute at SFC

18:00-18:30 Conclusion

19:00-21:00 Dinner

Faculty club, Keio Mita campus, 2-15-45 Mita, Tokyo 108-8345, Japan