EU-U.S. EXPERT WORKSHOP

JOINT RESPONSES TO MALICIOUS CYBER ACTIVITIES

Organized by the EU Cyber Direct Project
October 8-9, 2019 (Dinner & Track 2.0 workshop)
Washington, DC, the United States

In recent years, the European Union (EU) and the United States (U.S.) have found responses to malicious cyber activities seeking to undermine their political integrity, national security and economic competitiveness, with the eventual risk of conflict. In order to respond to those malicious cyber activities, the EU has established a set of response mechanisms, including most prominently the so-called EU Cyber Diplomacy Toolbox and the EU Joint Communication on "Resilience, Deterrence, and Defence: Building Strong Cybersecurity for the EU". Adopted in June 2017, the EU Cyber Diplomacy Toolbox includes measures suitable for an immediate response to incidents as well as elements to encourage cooperation, facilitate the mitigation of immediate and long-term threats, and influence the behavior of potential aggressors in the long term. These measures range from diplomatic and political to economic actions to prevent, detect or react to malicious cyber activities, including those that do not rise to the level of internationally 'wrongful acts' but are considered as 'unfriendly acts'. The United States has developed strategies and policies as well as defined domestic stakeholders that would engage in response actions, for instance the U.S. recommendations on deterrence and international engagement pursuant to the U.S. Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure".

For both partners, responses to malicious cyber activities have an international component. In the EU, the General Secretariat of the Council stated in its "Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities" that "appropriate coordination with like-minded partners and international organizations should be envisaged." The U.S. government stated in its 2018 Recommendations to the President on Protecting American Cyber Interests Through International Engagement that the "imposition of consequences would be more impactful and send a stronger deterrent message if it were carried out in concert with partner states. Partners could, on a voluntary basis, support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken following an incident, and/or actual participation in the imposition of consequences against perpetrator governments". In addition, the EU and the U.S. underlined the need for coordination and cooperation on joint responses in the 2018 and 2019 Cyber Dialogues.

This workshop, organized by the EU Cyber Direct, brings together cybersecurity and foreign policy experts from the EU and the U.S. to assess the current state of joint EU-U.S. responses to to prevent, detect and react to malicious cyber activities and determine options of further advancing joint responses along various dimensions as was envisioned by diplomats in the EU-U.S. Cyber Dialogues from 2018 and 2019.

Objectives

- Increase the understanding of responses to malicious cyber activities that are available to the EU and U.S.
- Identify mechanisms, roles, and challenges for a joint EU and U.S. response to malicious cyber activities
- Putting ideas into practice by talking through scenarios "WannaCry" and "NotPetya"

Implementing organisations

The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Stiftung Neue Verantwortung

This project is funded by the European Union.

Agenda

October 8 Dinner

20:00 Dinner Discussion "Is a Schengen Accord for the Internet possible?"

Location: Floriana, 1602 17th St NW, Washington, DC 20009

Keynote

Robert K. Knake
Whitney Shepardson Senior Fellow

Moderator

Julia Schuetze
Project Manager, Stiftung Neue Verantwortung

October 9 EU-U.S. expert workshop "Joint Responses to Malicious Cyber Activities"

Location: The German Marshall Fund, 1700 18th St NW, Washington, DC 20009

The guiding question for the workshop is "How can the EU and U.S. jointly respond to malicious cyber activities?". We will identify common strategic goals, joint instruments achieve those goals, as well as limitations of responses. We will then put ideas into practice by engaging in a scenario exercise involving major cyber attacks with high impact, namely "WannaCry" and "NotPetya".

09:00-09.30 Registration and welcome coffee

09:30-10:00 Introductions and workshop goals

Welcome

Rosa Balfour
The German Marshall Fund of the United States

Introduction

Julia Schuetze & Sven Herpig
Stiftung Neue Verantwortung

10:00-11:00 Common strategic goals

11:00-11:15 Coffee/tea break

11:15-12:30 Joint instruments

12:30-13:15 Lunch break

13:15-14:30 Limitations of joint instruments

14:30-15:45 Scenario-based discussions on concrete cyber incidents with high impact "WannaCry" and "NotPeyta"

The participants will be presented with scenarios that entails cyber incidents with high impact. The following questions will guide the group work and subsequent discussions.

1. What responses have been adopted and and implemented, and how effective have they been?
2. Taking into account the status quo, what joint responses could be taken?
3. What new joint responses can be applied?

15:45-16:15 Scenario presentations

16:15-16:45 Role of diplomats

16:45-17:00 Wrap up

About the EU Cyber Direct project

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 behavior and Confidence Building Measures. Workshops, conferences, and meetings organized in the framework of EU Cyber Direct contribute to a better understanding of EU cyber diplomacy and cyber resilience policies worldwide. EU Cyber Direct is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.