**Masterclass on State responsibility and response options to
cyber operations**

Training for officials from OAS Member States

1-3 February 2023 (online)

|  |
| --- |
| **1 February 2023** |
| 09:30-12:30 ET (15:30-18:30 CET) | *Introductory remarks by OAS and ICT4Peace* * Welcome and introduction by OAS
* Introduction to Course by ICT4Peace
* Introductions of participants and speakers
* Keynote: ***Ms. Elina Noor***, Director, Political-Security Affairs, Asia Society Policy Institute

*State Responsibility** Introduction to the concept of State responsibility
* What is an internationally wrongful act?
* Consequences of State responsibility
* Classification/response matrix

*Attribution** What is attribution?
* Standards of attribution under International Law
* Standards of proof and evidence under International Law
* Is there a duty to provide evidence for attribution?
 |
| **2 February 2023** |
| 09:30-12:30 ET (15:30-18:30 CET | *Overview of response options**Diplomatic response options** Cyber diplomacy
* Restrictive measures / sanctions
* Keynote: ***Ms. Manon Le Blanc***, Head of Sector Cyber Security, European External Action Service (TBC)

*Response options within the national legal framework**Countermeasures Part I** What constitutes a countermeasure (and what doesn’t)?
* Substantive legal requirements for the taking of countermeasures
* Procedural requirements for the taking of countermeasures
 |
| **3 February 2023** |
| 09:30-12:30 ET (15:30-18:30 CET | *Countermeasures Part II** Necessity and proportionality of countermeasures
* Collective countermeasures

*Aid and assistance, Neutrality, Co-belligerency** Limits of aid and assistance in countering cyberattacks in peacetime
* Providing aid and assistance to a country involved in an armed conflict (between neutrality and co-belligerency)

*Group assignment* (case study) |