**International Cyber Diplomacy, Law and Norms**

**Basic course**

Training for officials from OAS Member States

21-23 February 2023

|  |  |
| --- | --- |
| **21 February 2023** | |
| Morning session | |
| 09:30-12:00 | *Introductory remarks by OAS and ICT4Peace*   * Welcome and introduction by OAS * Introduction to Course by ICT4Peace * Introductions of participants and speakers   *Overview of the Framework of Responsible Behaviour in Cyberspace*   * History * Structure * Main issues & challenges * International formats (GGE & OEWG) |
| Lunch Break (2h) | |
| Afternoon session | |
| 14:00-16:30 | *Putting international law into practice part I*   * Why does international law apply in cyberspace? * What obligations do States have under international law with respect to cyber operations? * When is a State internationally responsible for a malicious cyber operation? |
| **22 February 2023** | |
| Morning session | |
| 09:30-12:00 | *Putting international law into practice part II*   * What response options do States have when being targeted by malicious cyber operations? * Which rules apply to cyber operations during armed conflicts? * Guest speaker: Jonathan Horowitz, ICRC (TBC) |
| Lunch Break (2h) | |
| Afternoon session | |
| 14:00-16:30 | *Cyber norms*   * What is the difference between law and norms? * Which cyber norms does the international community endorse? * How is cyber due diligence regulated by law and norms? * Which norms apply in the context of network security? |
| **23 February 2023** | |
| Morning session | |
| 09:30-12:00 | *Cybercrime in Focus*   * How does the international community tackle cybercrime? * Budapest Convention – overview * Work of the Ad Hoc Committee on a new cybercrime treaty – overview   *Multistakeholderism* |
| Lunch Break (2h) | |
| Afternoon session | |
| 14:00-16:30 | *Putting theory into practice – a simulation of OEWG proceedings* (Group exercise) |