Cyber-diplomacy: the theory and the practice

2 – 6 November, Pristina

Workshop Structure

Day 1 – Understanding cyberspace and defining cyber diplomacy

The training starts from the 'basics', to provide an underpinning conceptual framework on which the following days are built. In particular, the course begins by **examining the multifaceted concept of cyberspace, followed by an analysis of cyber diplomacy**. In the **afternoon**, the focus moves to the **cyber threat landscape**, considering in particular **hybrid campaigns, hacktivist groups** and **Advanced Persistent Threats (APTs).** The first day concludes with a dedicated session on Emerging Disruptive Technologies (EDTs) including AI and quantum technologies, which will significantly shape our digital future.

09:00 – 09:30	*Accreditations and welcome coffee*
09:30 – 10:00	**Institutional Remarks and Introduction to the Workshop** - Representative from the Ministry of Foreign Affairs and Diaspora (**TBD**) - Ambassador Maurizio **Antonini**, Italian Ministry of Foreign Affairs and International Cooperation - Representative from the Ministry of Foreign Affairs and Diaspora (**TBD**) - Counsellor Nicolò **Costantini**, Italian Ministry of Foreign Affairs and International Cooperation
10:00 – 10:50	**The Cyber Diplomat's Work** - Counselor Nicolò **Costantini**, Italian Ministry of Foreign Affairs and International Cooperation - Representative from the Ministry of Foreign Affairs and Diaspora (**TBD**)
10:50 – 11:20	*Coffee break*
11:20 – 12:00	**Contextualizing Cyber Diplomacy and the Italian Approach** - Mr. Giacomo **Zampieri**, Italian Ministry of Foreign Affairs and International Cooperation - Mr. Matteo **Pastorella**, Italian Ministry of Foreign Affairs and International Cooperation
12:00 – 13:30	*Lunch*

13:30 – 15:00	**Understanding Hybrid Campaigns, Hacktivist Groups and APTs** - Prof. Mattia **Siciliano**, LUISS University
15:00 – 15:30	*Coffee break*
15:30 – 16:30	**Emerging Disruptive Technologies** - Prof. Mattia **Siciliano**, LUISS University

Day 2 – International law and cyberspace

The second day of the course focuses of the **legal aspects related to cyberspace**. To do so, the program starts by providing an overview of the application of **international law** in cyberspace, looking in particular at some basic principles of international law. Then, a dedicated session delves into **International Humanitarian Law**. After that, a specific session will provide a collection of good practices and national experiences in developing a **national position on the interpretation of international law in cyberspace**. This second day ends with a hands-on workshop on the development of a national position on the interpretation of international law to cyberspace.

09:00 – 10:30	**International Law in Cyberspace** - Prof. Marco **Roscini**, University of Westminster
10:30 – 10:50	*Coffee break*
10:50 – 12:20	**International Humanitarian Law in Cyberspace** - Prof. Marco **Roscini**, University of Westminster
12:20 – 13:40	*Lunch*
13:40 – 15:10	**Developing a National Position on the Interpretation of International Law to Cyberspace** - Counselor Nicolò **Costantini**, Italian Ministry of Foreign Affairs and International Cooperation - Ms. Dominique **Steinbrecher**, United Nations Institute for Disarmament Research
15:10 – 15:30	*Coffee break*
15:30 – 16:30	**Workshop on Developing a National Position on the Interpretation of International Law to Cyberspace** - Ms. Dominique **Steinbrecher**, United Nations Institute for Disarmament Research

Day 3 – Kosovo in the international cyber arena

The focus of the third day is on the ongoing discussion and processes at the **international level**. Looking at these activities allows to appreciate the growing attention being afforded to cyber-related matters, as well as the role that states – and Kosovo – have *vis-à-vis* the normative and multilateral side of cyberspace. The first half of the day focuses on the **UN level**, deep-diving into the activities of the **Global Mechanism on ICTs in the Context of International Security** – looking at the first substantive plenary meetings and the works of the Dedicated Thematic Groups (DTGs). These sessions equip participants with the knowledge and practical tools needed to be able to meaningfully engage with this ecosystem. The second half of the day brings the **European Union** into the picture, looking at the actors, initiatives and dynamics that are relevant when dealing with cyber-related matters, and with cyber-diplomacy in particular. Indeed, at the EU level, there are several actors that are being active around cyber-diplomacy, and many initiatives and programs where Kosovo can fruitfully engage.

09:00 – 10:30	**The Activities at the UN-level and the Global Mechanism** - Prof. Alberto **Oddenino**, University of Turin
10:30 – 10:50	*Coffee break*
10:50 – 12:20	**Engaging with the UN: modalities and scope** - Dr. Claudia **Schettini**, Italian Institute for International Political Studies
12:20 – 13:40	*Lunch*
13:40 – 15:10	**European Cybersecurity and Cyber Diplomacy: From Theory to Practice in Securing Cyberspace** - Prof. Annita Larissa **Sciacovelli**, University of Bari
15:10 – 15:30	*Coffee break*
15:30 – 16:30	**Engaging with the EU** - Ms. Lilian **Georgieva-Weiche**, European External Action Service *online* - Prof. Annita Larissa **Sciacovelli**, University of Bari

Day 4 – Multistakeholder approach & the "practice" of cyber-diplomacy

This module highlights the importance of a **multistakeholder approach**. During this day of training, the participants engage with the role of the private sector, civil society, and academia present in the **Kosovar and Italian ecosystems**, to understand their role in shaping national cybersecurity strategies and participating in global forums. The second half of the day will shift the perspective from the *theory* related to cyber-diplomacy to its *practice*. Indeed, throughout the four days of the training the participants are expected to have gained a solid understanding of the theoretical side of cyber-diplomacy. Building on this, the afternoon's sessions consider how the theory is translated into the practice of the diplomatic work. This is done by looking in particular at **cyber deterrence and cyber resilience**. Lastly, a specific session is dedicated to **Cyber Capacity Building**. This provides an interesting use-case to see how the different objectives, strategies, and working modalities described in the initial part of the course are "put into practice" when carrying out concrete activities of CCB.

09:00 – 10:30	**Multi-Stakeholder and Whole-of-Government Approaches** - Dr. Marta **Stroppa**, University of Milan - Ms. Luanda **Domi**, German Development Agency (GIZ) Kosovo
10:30 – 10:50	*Coffee break*
10:50 – 12:20	**Public-Private Partnerships and Best Practices in Coordination** - Dr. Marta **Stroppa**, University of Milan - Mr. Drinor **Selmanaj**, Sentry and Cyber Academy
12:20 – 13:40	*Lunch*
13:40 – 15:10	**Cyber Deterrence and Cyber Resilience** - Dr. Marta **Stroppa**, University of Milan
15:10 – 15:30	*Coffee break*
15:30 – 16:30	**Cyber Capacity Building** - Mr. Matteo **Pastorella**, Italian Ministry of Foreign Affairs and International Cooperation - Mr. Giacomo **Zampieri**, Italian Ministry of Foreign Affairs and International Cooperation

Day 5 – Diplomatic cyber range

In an evolving operational landscape, digitalization is providing new opportunities for development and progress, but also **creating new challenges**. It is therefore crucial to focus on increasing cyber awareness and literacy, upskilling the workforce, enhancing resilience and strengthening cyber capabilities.

Measures to enhance **cyber resilience and security include cyber ranges and other training exercise**. A cyber range is a controlled, interactive virtual environment where teams can safely simulate a cyber crisis to practice and develop their crisis preparedness and response capacities. This kind of exercise requires participants to carry out strategic activities in a **fictional cyber crisis scenario**, where they are tasked with assessing the severity of a certain situation, identify key relevant actors, assess their roles in cyber incidents, as well as to analyse the robustness of national documents and normative frameworks and understand whether and, if so, what elements to publicly disclose.

The exercise proposed during the last day of this training takes the form of a **diplomatic cyber range**, where the participants are put in the role of the **Kosovar's public administration personnel responsible for cyber malicious activities**. The aim is to foster awareness of the multidimensional impact of cyber operations in the **inter-institutional Kosovar** milieu, and to raise participants' awareness of the difficulties faced when dealing with one of them. In addition, this exercise enables participants to gain hands-on experience and improve their cybersecurity awareness and readiness, as well as their incident response capabilities.

09:00 – 10:30	**Setting the Stage and Analysis of the Scenario** - Dr. Andrea **Calderaro**, EU Institute for Security Studies
10:30 – 10:50	*Coffee break*
10:50 – 12:20	**Decision-Making Stage and Conclusions** - Dr. Andrea **Calderaro**, EU Institute for Security Studies - Mr. Matteo **Pastorella**, Italian Ministry of Foreign Affairs and International Cooperation - Mr. Giacomo **Zampieri**, Italian Ministry of Foreign Affairs and International Cooperation
12:20 – 13:40	**Lunch and Conclusion of the Workshop**

Presentation of the Experts

Mattia Siciliano – LUISS University



Mattia Siciliano is an Adjunct Faculty Member at Luiss Business School and an expert in cybersecurity and digital innovation with over 15 years of experience. Holding a degree in Telecommunications Engineering, he has developed strong expertise in cybersecurity management. He currently serves as a Strategic Advisor to the Italian Ministry of Defense – General Office for Innovation (UGID) and as President of the Cyber Threat Intelligence and Cyber Warfare Commission at the Italian Society of Intelligence (SOCINT). He is also a member of the Digital Policy Committee at Business at OECD. Throughout his career, he has worked with major international consulting firms such as EY and KPMG and is a co-founder of innovative startups in the cybersecurity and artificial intelligence sectors.

Marco Roscini – University of Westminster



Marco Roscini is Professor of International Law at the University of Westminster in London and Senior Fellow at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. He holds a PhD from Sapienza University of Rome and has published extensively on international law. His publications include numerous journal articles and book chapters, as well as three monographs, including Cyber Operations and the Use of Force in International Law, and International Law and the Principle of Non-Intervention, both published by Oxford University Press. In 2025, he served as Director of Studies at the Hague Academy of International Law's Centre for Studies and Research, devoted to artificial intelligence and international law.

Dominique Steinbrecher – United Nations Institute for Disarmament Research



Dominique Steinbrecher is a Researcher with the Security and Technology Programme at the United Nations Institute for Disarmament Research (UNIDIR). UNIDIR is an autonomous institution within the United Nations that conducts independent research on disarmament and international security, and supports Member States and other stakeholders through analysis, dialogue and capacity-building. Ms. Steinbrecher is part of the International Cyber Stability Workstream, working on cybersecurity with a particular focus on research and capacity-building on international law. Her areas of expertise include international law, international humanitarian law and human rights, international security, and disarmament issues. Prior to joining UNIDIR,

Dominique worked at the International Committee of the Red Cross in Geneva, the Cooperative Cyber Defence Centre of Excellence, the Non-Proliferation for Global Security Foundation, and the Civil Association for Equality and Justice. She holds an LL.M. from the Geneva Academy of International Humanitarian Law and Human Rights, a postgraduate degree in Security, Disarmament and Non-Proliferation, and a Law Degree from the University of Buenos Aires.

Claudia Schettini – Italian Institute for International Political Studies



Claudia Schettini is the Head of the Digitalization Program at ISPI, Italy's leading think tank on international affairs' research and policy analysis on global geopolitical and economic trends. At ISPI, she leads research on the geopolitical, economic and security implications of digital technologies, with a particular focus on artificial intelligence, cybersecurity, digital governance and technological competition. She holds a Bachelor's degree in Political Science from LUISS Guido Carli University, a Master's degree in International Security from Sciences Po Paris, and a PhD in Global Politics and Human Rights from the Sant'Anna School of Advanced Studies, Pisa. Her doctoral research examined technology-facilitated abuse through adaptive threat modelling. Claudia Schettini previously worked with the Atlantic Treaty Association and Swiss consultancy Horizon Groups, where she conducted strategic analyses on digital technologies and advised international clients on cybersecurity policies and standards. She speaks English, French and Spanish.

Alberto Oddenino – University of Turin



Alberto Oddenino is a Professor of International law at the Department of Law at the University of Turin, he also teaches the course on International Law and New Technologies. He is the coordinator of the Diploma in Law and Technology at the same department and serves as Secretary-General of the Italian Society for International Organisation (SIOI – Piedmont and Aosta Valley Section). He is a member of the Co-ordinating Committee of the Interest Group on International Law and New Technologies of the Italian Society of International Law and the European Union, and a member, amongst other things, of the Advisory Board of the Journal of Law, Market and Innovation. He is a member of the 'New Technologies, Cybersecurity and Artificial Intelligence' Commission of the Reale Mutua Insurance Group. He is the author of two monographs and over sixty publications on topics relating to international law and EU law, with particular reference to the relationship between international law, EU law, the Internet, Big Data and artificial intelligence. An international lawyer, he has been registered with the Turin Bar since 2001.

Marta Stroppa – University of Milan



Marta Stroppa is a Postdoctoral Research Fellow in International Law at the Department of International, Legal, Historical and Political Studies of the University of Milan, where she serves as Principal Investigator of the research project "The Use of Autonomous Cyber Capabilities in Military Operations: An International Law Perspective (AI-M)," funded by Fondazione Cariplo. Previously, she was a Postdoctoral Research Fellow at the Sant'Anna School of Advanced Studies, where she also earned her PhD. During her doctoral studies, she was a Visiting Researcher at the NATO Cooperative Cyber Defence Centre of Excellence and the University of Westminster. She has also worked in the Legal Affairs Office of the Permanent Mission of Italy to the United Nations in New York and with the Global Maritime Crime Programme of the United Nations Office on Drugs and Crime.

Annita Larissa Sciacovelli – University of Bari



Annita Larissa Sciacovelli, Ph.D., is an Associate Professor of International Law at the Department of Law of the University of Bari Aldo Moro, Italy, a specialist in cybersecurity, and a practising lawyer admitted to the Bari Bar. Representing the University of Bari, she participates as a non-governmental stakeholder in the United Nations Global Mechanism on ICT security. She is Advisor to the Governance Risk and Compliance-GRC Summit organised by the Luxembourg House of Cybersecurity (LHC) and the National Cybersecurity Competence Center of Luxembourg, and she is member of the Global Cyber and Security Policy expert panel at the Geneva Centre for Security Policy (GCSP). She is Scientific Director of both the Executive Programme "Cybersecurity, Emerging Technologies, and Advanced Defense" and Signa, the cybersecurity and information security journal of the Centre for Higher Defence Studies (CASD), Italian Ministry of Defence. She also lectures on "Information and Communication Technologies II" within the Executive Course of the Economic and Financial Police (Guardia di Finanza) in Rome. From 2023 to 2025, she served as a member of the Advisory Group of the European Union Agency for Cybersecurity (ENISA), and as Scientific Co-Director of the Cybersecurity Course for the Cybernetic Security Operations Centres (COSC), organised by the Directorate of the Italian Postal and Cyber Police. She has also been Legal Consultant to the Italian Cyber Operations Command (COR). She is Vice President of Global Professional for Artificial Intelligence (GP4AI), and in 2024, she received the prestigious "Professional Woman in Cybersecurity Europe" award from CEFCYS in Paris.

Andrea Calderaro – EU Institute for Security Studies



Dr. Andrea Calderaro is Director of Cyber Diplomacy at the EU Institute for Security Studies (EUISS), leading the EU Cyber Direct - EU Cyber Diplomacy Initiative programme. His work focuses on technology and foreign policy, particularly cybersecurity, cyber diplomacy, and the transnational governance of emerging technologies. He has contributed to bilateral and multilateral cyber dialogues including the UN OEWG, the UN Global Mechanism, the IGF, and WSIS, and has supported cyber capacity-building initiatives across Africa, Asia, the Middle East, and Latin America and the Caribbean. He has served on advisory boards for the European Union, the Global Forum on Cyber Expertise (GFCE), the UK FCDO, UNESCO, and the OECD. His publications include articles in Third World Quarterly, Policy & Internet, and European Security, and volumes including "Internet Diplomacy: Shaping the Global Politics of Cyberspace" (2022). Currently on leave from Cardiff University, he has previously held positions at Caltech, Humboldt University, FGV Rio de Janeiro, LUISS, and the European University Institute, from which he holds a PhD and MRes in Social and Political Sciences.

Luanda Domi – GIZ's Regional CyberPolicy Advisor for the WB



Luanda Domi is a cybersecurity policy and governance expert with over a decade of experience in cyber governance, critical infrastructure resilience and international capacity building. She currently serves as GIZ's Regional Cyber Policy Advisor for the Western Balkans, supporting cyber capacity building, strengthening partnerships in cybersecurity and advancing multilateral engagement in cyber diplomacy across the Western Balkans region. Her expertise includes strengthening national cybersecurity frameworks, critical infrastructure resilience and cybersecurity culture. Previously, at the Global Forum on Cyber Expertise (GFCE), she managed a global portfolio on gender mainstreaming and cyber skills, led the Women in Cyber Capacity Building Network and facilitated global working groups on critical infrastructure protection, cyber workforce development and cybersecurity awareness. She also served as Deputy Country Director for USAID's Critical Infrastructure Digitization and Resilience Program, alongside earlier work with UNDP, DCAF and the Unitarian Universalist United Nations Office in New York. She is a non-resident EU Cyber Direct fellow at EUISS, focusing on cyber diplomacy, and Responsible AI Governor for Kosovo at the Global Council for Responsible AI. Her international recognition includes Cybersecurity Woman of the Year 2025 (Supporter category) and selection among the world's Top 25 Women in Cybersecurity in 2025 and 2026.

Drinor Selmanaj – Founder of Sentry and Cyber Academy



Drinor Selmanaj is a cybersecurity frontiersman with over a decade of experience in penetration testing, cyberterrorism combat, and global privacy. He has worked with NATO representatives, multinational corporations, tech giants, and heads of state. Drinor is an award-winning cybersecurity professional, lecturer, public speaker, and executive aspiring to boost innovation while perpetually pursuing excellence and keeping one step ahead of cyber threats. He has founded numerous businesses and initiatives focusing on cybersecurity services and education. At Sentry Cybersecurity & Defense, Drinor leads an advanced team of cybersecurity professionals, overseeing the delivery of advanced penetration testing and consultancy services to major corporations, including those classified as unicorn entities and some of the Big Four.

Lilian Georgieva-Weiche – European External Action Service



Lilian Georgieva-Weiche works as a policy officer in the Cyber and Hybrids Threats Division of the European External Action Service (EEAS), where she is focusing on the Africa and Multilateral portfolio. She is a seconded national expert from the German Federal Foreign Office (FFO) as well as the German Development Agency (GIZ), where she previously worked on cyber diplomacy and the intersection of technology and human rights.