

International Cyber Security Policy and Diplomacy Capacity Building Program



ICT4Peace Academy offers custom-tailored courses to meet your organization's needs in learning more about today's challenges in Information and Communications Technologies (ICTs), including cyber diplomacy, cyber peacebuilding and cyber (human) security. Drawing from an extensive network of expert practitioners, including diplomats, technologists and civil society experts, each customized course offers the latest in up-to-date information which is tailored to your organization's particular context and presented in a live and interactive format.

<https://academy.ict4peace.org>

Who is it For?

ICT4Peace Academy offers custom-designed courses for organizations who want to improve their understanding of today's most pressing challenges of new technologies. Each course is custom-designed and adapted to the context and needs of your organization and may last from half a day to a full week or more.

Courses on the Cutting Edge

ICT4Peace Academy is currently offering courses on the following topics:

International Cyber Norms	Applying International Law to Cyberspace	Cybercrime and Data Protection
Public-Private Partnerships and Cyber	Misinformation / Disinformation Online	ICTs and Gender
Confidence Building Measures (CBMs)	Preventing Violent Extremism Online	Computer Security Incidence Response Teams

Introduction

States bear primary responsibility for the safety and security of their citizens, including in the ICT environment. Many states, especially developing countries and LDCs however, still lack sufficient capacity to protect their ICT networks and to engage in bilateral, regional and global cooperation at the technical and diplomatic level and to learn about concrete threats and respond effectively to them.

The lack of such capacity can make national institutions, critical infrastructures such as power, Telecom, hospitals, transport and financial sector of a country or the citizens and the private sector at large vulnerable and can hamper economic and social development. It can make a country even an unwitting haven for malicious actors, which negatively impacts the global ICT network on the whole, thus also in the industrial world. It is often said, that the global ICT network “is only as strong as its weakest link”.

Support to capacity building in cyber security policy, strategy and diplomacy is playing an essential role in (1) States engaging in international cooperation and negotiations (as outlined in the 2013 and 2015 GGE reports on norms and CBMs), (2) enabling States, in cooperation with the private sector, academia and think tanks and civil society to secure its ICT infrastructure for economic and social development and (3) to strengthen the global ICT network and to ensure their peaceful use for economic and social development.

Since 2014 and with the support of the Governments of the UK, Germany, Switzerland, Netherlands, Colombia, Kenya, Singapore, Australia and New Zealand, the ICT4Peace Foundation has carried out a series of Capacity Building workshops for Latin American Countries (in Bogota in cooperation with OAS), for African Countries (AU, Addis Ababa), for East African Countries (Nairobi, in cooperation with the Government of Kenya), for francophone African Countries in cooperation with l’Ecole Nationale Cybersécurité à Vocation Régionale (ENCVR) à Dakar, Sénégal, for ASEAN Countries (Singapore), Europe (GCSP, Geneva), for OSCE Field staff (Vienna), for Cambodia, Laos, Myanmar, Vietnam (CLMV countries) in Laos, Vientiane; Hanoi, Vietnam, Siem Reap, Cambodia, Naypidaw, Myanmar, for all ASEAN Countries in Thailand and in Singapore (2x). Several capacity building workshops for African Diplomats in New York and Geneva, ahead of the OEWG and UN GGE negotiations was carried out in cooperation with ODA and the Swiss Government.

We cooperate with the UN GGE and UN OEWG experts on refining and delivering the next round of workshops to support the goals and tasks outlined in the GGE reports and the specific needs of the countries in the Regions.

General Objectives of the Workshops

1. Better awareness of issues of international cyber security by public officials and diplomats (international law and norms, CBMs and international cooperation as outlined in the UN GGE and UN OEWG Reports, by ASEAN, OSCE, AU, OAS etc.);
2. Preparation of staff in Capitals and Country Delegations for the upcoming negotiations on Cybersecurity in the context of the UN OEWG in 2022 to 2025 in New York, Geneva;
3. Preparation of staff in Capitals and Country Delegations to engage in bilateral, regional and global negotiations in Cybersecurity Confidence Building Measures (CBMs);
4. Better understanding of the respective role of States, International Organizations, Business, Academia and Civil Society in maintaining peace and Security in Cyberspace;
5. Feedback from the Regions to the international cyber security dialogue and discourse.
6. Better mutual understanding of related concepts, norms and measures, strengthened and possibly institutionalized cooperation among participating countries;
7. Exchange of concerns, best practices, policies and institutional arrangements in the field of cyber security;
8. A network of alumni, lecturers and experts familiar with the international cyber security challenges and processes and willing to support the goals of implementing and universally promoting inter alia the UN GGE UN OEWG guidance on norms and CBMs.

Workshop Modules

1. Introduction to the international peace and security goals related to uses of ICTs;
2. Links between national and international cyber security efforts, processes and actors;
3. Introduction to international cyber security consultations and dialogues (UN GGE, UN OEWG, ASEAN, ARF, OSCE, AU, OAS, London Process etc.);
4. Applicability of the international law as outlined in the UN GGE reports;
5. Norms of responsible state behavior as outlined in the UN GGE reports;
6. CBMs and international cooperation in the cyberspace (as outlined in the UN GGE, OSCE, ARF etc. reports);

7. Best practices in national cyber security strategy building, policy development and legislation;
8. Best practices in Cert building and Cert-Cert cooperation;
9. Presentations and panel discussions on regional and national cyber security concerns, perspectives and policy options;
10. Table-top exercises tailored to the target audience priorities and requirements.
11. Emerging threats to peace and security, human dignity, social cohesion and democratic processes by Mis-, Disinformation and Hate Speech (MDH);

Additional courses and seminars upon request

1. Better understanding of the emerging threats to peace and security, human dignity, social cohesion and democratic processes by Mis-, Disinformation and Hate Speech (MDH) and an emerging governance framework;
2. Workshops and consultations on best practices of National Cyber Security Strategy (NCSS) building;
3. Workshops and consultations on developing and implementing national legislation;
4. Workshops on establishing CERTs, CERT- CERT cooperation;
5. Workshops for special target audiences (parliamentarians, judiciary, regulatory authorities etc.)

Participation

These workshops are of particular interest to government officials involved or interested in foreign cyber policy development and/or cyber security diplomacy but offer useful background knowledge to decision-makers and advisers in the field of national cyber security strategy development and implementation. Senior staff of technical cybersecurity units such as CERTs and the Private Sector will be included wherever possible.

A ceiling of approximately 35 participants per workshop is recommended to facilitate discussion.

Lecturers and facilitators of the workshop

The lecturers and facilitators of the workshop consist of senior diplomats having participated in the processes of UN GGE, UN OEWG OSCE or ARF CBMs, and senior experts with business civil society/academic background and first-hand experience with the topic.

List of Cyber Security Policy and Diplomacy Workshops already carried out on: International Law, Norms and CBMs, Cybersecurity Strategies and Legislation, CERT-Building and CERT-CERT Co-operation etc.:

2014 OAS Organisation of American States Cybersecurity Policy and Diplomacy Course in Bogota: <http://ict4peace.org/?p=3563>

2015 The Hague Global Conference on Cyberspace 2015 preparatory workshop: <http://ict4peace.org/?p=3693>

2015 Kenya Cybersecurity Diplomacy and Policy Course for 12 East African countries: <http://ict4peace.org/?p=3674>

2015 ASEAN Singapore Cybersecurity Diplomacy Workshop for ASEAN Countries: <http://ict4peace.org/?p=3969>

2016 African Union Addis Ababa Cybersecurity Diplomacy workshop with AU Commission: <http://ict4peace.org/?p=4079>

2016 CLMV Countries Vientiane Cybersecurity Policy and Diplomacy Workshop for CLMV Countries: <http://ict4peace.org/?p=4304>

2016 GCSP, Cybersecurity Workshop for Geneva based diplomats, business and civil society: <http://ict4peace.org/?p=4095>

2016 OSCE Cybersecurity Policy and Diplomacy Workshop for field staff: <http://ict4peace.org/?p=4781>

2016 ASEANBangkok Cybersecurity Policy and Diplomacy Workshop for ASEAN countries: <http://ict4peace.org/?p=4849>

2017 UN ODA Geneva workshop for the UN GGE Experts: Existing and Future Norms on International ICT Infrastructure and Data Integrity: <http://ict4peace.org/?p=4804>

2017 ASEAN Singapore 1st Cybersecurity Norms Workshop for ASEAN Countries:

<https://ict4peace.org/activities/promoting-norms-of-responsible-behaviour-in-cyberspace/>

2017 CLMV Hanoi Cybersecurity Policy and Diplomacy for CLMV Countries:
<http://ict4peace.org/?p=5095>

2018 ASEAN Brunei Cybersecurity Policy and Diplomacy Workshop for ASEAN Countries: <http://ict4peace.org/?p=5285>

2018 UN ODA New York Workshop on Implementing UN Norms of Responsible State Behavior in Cyberspace in New York <https://ict4peace.org/activities/ict4peace-workshop-on-implementing-un-norms-on-responsible-state-behaviour-in-cyberspace-in-new-york/>

2018 ASEAN Singapore 2nd Cybersecurity Norms workshop for ASEAN Countries: <https://ict4peace.org/activities/2nd-asean-cyber-norms-workshop-in-singapore-supported-by-ict4peace/>

2018 CLMV Countries Siem Reap Cybersecurity Policy and Diplomacy Workshop for CLMV Countries: <https://ict4peace.org/activities/capacity-building/capacity-building-cs/ict4peace-3rd-senior-level-cybersecurity-policy-and-diplomacy-workshop-for-clmv-countries-held-in-siem-reap-cambodia/>

2019 CLMV Countries NayPyitaw Cybersecurity Policy and Diplomacy Workshop for CLMV Countries: <https://ict4peace.org/activities/4th-ict4peace-senior-level-cybersecurity-policy-and-diplomacy-workshop-for-clmv-countries-held-in-naypyitaw-myanmar/>

2019 OAS Organisation of American States, Cybersecurity Policy and Diplomacy Workshop in Washington DC for Latin American Diplomats, for Upcoming OEWG and UN GGE processes: <https://ict4peace.org/activities/un-gge-and-un-oewg-on-cybersecurity-ict4peace-supporting-oas-regional-consultations/>

2019 UN, New York, ODA, Cybersecurity Policy and Diplomacy Workshop for African Diplomats for Upcoming UN OEWG and UN GGE processes: <https://ict4peace.org/activities/un-oewg-un-gge-preparatory-workshop-with-africa-diplomats-successfully-completed/>

2020 UN, New York, ODA, 2nd Cybersecurity Policy and Diplomacy Workshop for African Diplomats for ongoing and upcoming UN OEWG and UN GGE processes:
<https://ict4peace.org/activities/2nd-capacity-building-workshop-on-cybersecurity-policy-and-diplomacy-with-african-diplomatic-delegations-to-the-un-in-new-york-in-preparation-of-the-un-oewg-on-cybersecurity/>

2020 UN, Geneva, ODA, 3rd Cybersecurity Policy and Diplomacy Workshop for African Diplomats for ongoing and UN OEWG and UN GGE processes:
<https://ict4peace.org/activities/3rd-capacity-building-workshop-on-cybersecurity-policy-and-diplomacy-with-african-diplomatic-delegations/>

2020 Government of Kenya, Pilot 5 Days Online Course on Cybersecurity Policy for East African Countries. <https://ict4peace.org/activities/new-5-days-online-course-on-cybersecurity-policy-for-east-african-countries-completed/>

2020 OAS Organization of American States, International Cyber Diplomacy, Law and Norms, 5 Days OAS Online Training Course for Government Officials
<https://ict4peace.org/activities/oas-5-days-international-cyber-diplomacy-course-completed/>

2021 OAS Organization of American States, International Cyber Diplomacy, Law and Norms, Second 5 Days OAS Online Training Course for Government Officials (15 to 19 April 2021) <https://ict4peace.org/activities/oas-ict4peace-second-5-days-online-cybersecurity-policy-diplomacy-workshop-completed/>

2021 ICT4Peace Academy launched <https://ict4peace.org/activities/cybersecurity-policy-and-diplomacy-capacity-building/ict4peace-academy-launched/>

2021 OAS – ICT4Peace Academy 5 Days Online Course on International Cyber Diplomacy, Law and Norms (8 to 12 November 2021)
<https://ict4peace.org/activities/cybersecurity-policy-and-diplomacy-capacity-building/third-oas-ict4peace-academy-5-days-online-course-on-international-cyber-diplomacy-law-and-norms/>

2021 East African States Level 2 Five Days Online Training for Government Officials from East African Countries (15 to 19 November 2021)
<https://ict4peace.org/activities/cybersecurity-policy-and-diplomacy-capacity-building/online-training-for-government-officials-from-east-african-countries-level-2-completed/>

2021 Southern African States ICT4Peace Five Days Online Certificate Course on International Cyber Diplomacy, Law and Norms for Government Officials from Southern African States (22 to 26 November 2021)

<https://ict4peace.org/activities/cybersecurity-policy-and-diplomacy-capacity-building/online-training-for-government-officials-from-southern-african-countries-22-26-november-2021/>

2021 Francophonie (OIF) Programme de certificat en ligne de cinq jours pour les représentants des pays africains francophones: Cyber diplomatie, droit international et cyber normes (6 au 10 Décembre 2021)

<https://ict4peace.org/activities/cybersecurity-policy-and-diplomacy-capacity-building/ict4peace-programme-en-ligne-de-cinq-jours-cyber-diplomatie-droit-international-et-cyber-normes/>

2022 ICRC Three days Training Course on Mis-, Disinformation and Hate Speech for ICRC staff (February 2022)

2022 OAS Five Days Training Course on Cyber Diplomacy and Norms (February 2022)

2022 ICRC Three Days Course on Mis-, and Disinformation and Hate Speech for ICRC staff (October 2022)

2022 GIZ Three Days Course on Cyber Diplomacy and Norms (October 2022)

2022 GIZ Three Days Course on Misinformation and Social Media (November 2022)

2022 OAS Masterclass on Cooperation and Confidence Building Measures (CBMs) in Cyberspace (December 2022)

2023 OAS Cyber-Diplomacy, Law and Norms, (February 2022) in Washington DC

2023 OAS Application of International Humanitarian Law to Cyber Operations (March 2023) in Washington DC

Links to selected ICT4Peace publications:

Information and Communication Technology for Peace – The Role of ICT in Preventing, Responding and Recovering from Conflict (2005)

<https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2005-Information-and-Communication-Technology-for-Peace.pdf>

Getting Down to Business: Realistic Goals for the Promotion of Peace in Cyber-Space (2011) <https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2011-Getting-Down-to-Business.pdf>

Developments in the Field of Information and telecommunication in the context of international security: Work of the UN first Committee 1998-2012 <https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2012-GGE-Work-Of-First-Committee .pdf>

Cyber Security Affairs: Global and Regional Processes, Agendas and Instruments (2013) <https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2013-Global-And-Regional-Processes-Agenda-And-Instruments.pdf>

Confidence Building Measures and International Cyber Security (2013) <https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2013-Confidence-Building-Measure-And Intern-Cybersecurity.pdf>

A Role for Civil Society? ICTs, Norms and Confidence Building Measures in the Context of International Security (2014) <https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2104-A-Role-For-Civil-Society.pdf>

Baseline Review of ICT-Related Processes and Events (2014) <https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2014-Baseline-Review-ICT-Processes.pdf>

The G7 and Cyberspace: “Give Peace a Chance (2016) <https://ict4peace.org/wp-content/uploads/2020/03/Cyber-G7May2016OpEd-Commentary-on-G7-2016-1.pdf>

WannaCry, the Geneva Digital Convention and the urgent need for Cyber Peace A commentary by ICT4Peace (2017) <https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2017-Wannacry-GenevaDigitalConvention.pdf>

Voluntary, Non-Binding, Norms for Responsible State Behavior in the Use of Information and Communications Technology – A Commentary (Published by UNODA, New York) (2017) <https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2017-Civil-Society-And-Disarmament.pdf>

The Struggle for Cyber Peace: Norms of responsible state behavior (2018) <https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2018-Cyber-Peace-Struggle.pdf>

2018 The Year that Cyber Peace became Non-Binding (2018)

https://ict4peace.org/wp-content/uploads/2020/03/ICT4PeaceFoundation_The_year_that_cyber-peace_became_non-binding2018-12-31-1-1.pdf

Global Cyber Security Norms: A Proliferation Problem? (2018)

<https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2018-Global-Cyber-Security-Norms.pdf>

OEWG and UN GGE: How to live with two concurrent UN Cybersecurity Processes

(2019) <https://ict4peace.org/wp-content/uploads/2019/11/ICT4Peace-2019-OEWG-UN-GGE-How-to-live-with-two-UN-processes.pdf>

Trust and Attribution in Cyberspace: A Proposal for an Independent Network of Organizations engaging in Attribution Peer Review (2018) <https://ict4peace.org/wp-content/uploads/2019/07/ICT4Peace-2019-Trust-and-Attribution-in-Cyberspace.pdf>

Meeting Report: Workshop on Trusted Attribution in Cyberspace (2019)

https://ict4peace.org/wp-content/uploads/2019/10/ICT4Peace_AttributionWorkshop_Meeting-Report_final.pdf

ICT4Peace Submission to UN Open Ended Working Group on ICT and International Security (2019)

<https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2019-Submission-UN-Open-Ended-Working-Group.pdf>

Critical Infrastructure and Offensive Cyber Operations A Call to Governments (2019)

https://ict4peace.org/wp-content/uploads/2019/11/ICT4P_CriticalInfrastructure_Call_Final_21102019.pdf

ICT4Peace Proposed “States Cyber Peer Review Mechanism” for state-conducted

foreign cyber operations (2020) <https://ict4peace.org/wp-content/uploads/2020/03/ICT4Peace-Proposed-States-Cyber-Peer-Review-2.pdf>

Self-Defence against Cyberattacks? Digital and kinetic Defence in Light of Article 51 UN-Charter (2021)

<https://ict4peace.org/wp-content/uploads/2021/03/ICT4Peace-2021-Cyberattacks-and-Article51-1.pdf>

ICT4Peace and the UN Open Ended Working Group on Cybersecurity (2019 – 2021)
<https://ict4peace.org/wp-content/uploads/2021/04/ICT4Peace-2021-OEWG-Final-Report.pdf>

For additional information, cooperation or other requests please contact:

Ms. Anne-Marie Buzatu
Executive Director
ICT4Peace Foundation
anne-mariebuzatu@ict4peace.org