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:

<table>
<thead>
<tr>
<th>International Cyber Norms</th>
<th>Applying International Law to Cyberspace</th>
<th>Cybercrime and Data Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public-Private Partnerships and Cyber</td>
<td>Misinformation / Disinformation Online</td>
<td>ICTs and Gender</td>
</tr>
<tr>
<td>Confidence Building Measures (CBMs)</td>
<td>Preventing Violent Extremism Online</td>
<td>Computer Security Incidence Response Teams</td>
</tr>
</tbody>
</table>
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);
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 Bogota with OAS: http://ict4peace.org/?p=3563


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


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


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

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

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

2017 Singapore 1st Cybersecurity Norms Workshop for ASEAN Countries: https://ict4peace.org/activities/promoting-norms-of-responsible-behaviour-in-cyberspace/
2017 Hanoi Cybersecurity Policy and Diplomacy for CLMV Countries: http://ict4peace.org/?p=5095

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


diplomacy-capability-building/online-training-for-government-officials-from-southern-african-countries-22-26-november-2021/


2022 Three days Training Program on Mis-, Disinformation and Hate Speech (February 2022)

Links to selected ICT4Peace publications:


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

ICT4Peace Proposed “States Cyber Peer Review Mechanism” for state-conducted foreign cyber operations (2020)

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

ICT4Peace and the UN Opend Ended Working Group on Cybersecurity (2019 – 2021)

For additional information, cooperation or other requests please contact:

Ms. Anne-Marie Buzatu
Vice-President and COO
ICT4Peace Foundation
anne-mariebuzatu@ict4peace.org