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 GGE reports on norms and CBMs), (2) enabling countries 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), East African Countries (Nairobi), ASEAN Countries (Singapore), Europe (GCSP, Geneva), Cambodia, Laos, Myanmar, Vietnam (CLMV countries) (Laos, Vientiane) and Thailand (Bangkok).

We hope to cooperate with the GGE experts on refining and delivering the next round of workshops to support the goals and tasks outlined in the 2016/17 GGE report.
General Objectives of the Workshops

1. Better awareness of issues of international cyber security by public officials and diplomats (international norms, CBMs and international cooperation as outlined in the UN GGE Report, by OSCE, AU, OAS etc.);
2. Feedback to the international cyber security dialogue and discourse;
3. Better mutual understanding of related concepts, norms and measures, strengthened and possibly institutionalized cooperation among participating countries;
4. Exchange of concerns, best practices, policies and institutional arrangements in the field of cyber security;
5. 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 the UN GGE guidance.

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, 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. Presentations and panel discussions on regional and national cyber security concerns, perspectives and policy options;
9. Table-top exercises tailored to the target audience priorities and requirements.

Additional courses and seminars upon request

1. Workshops and consultations on best practices of National Cyber Security Strategy (NCSS) building;
2. Workshops and consultations on developing and implementing national legislation;
3. Workshops on establishing CERTs, CERT- CERT cooperation;
4. Workshops for special target audiences (parliamentarians, judiciary, regulatory authorities etc.)
Participation

These workshops will be 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.

A ceiling of approximately 30 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; OSCE or ARF CBMs, and senior experts with civil society/academic background and first-hand experience with the topic.

Links to agendas

2014 Bogota with OAS: http://ict4peace.org/?p=3563
2015 Singapore for ASEAN Countries: http://ict4peace.org/?p=3969
2016 Vientiane for CLMV Countries: http://ict4peace.org/?p=4304
2016 OSCE, Vienna for OSCE field staff: http://ict4peace.org/?p=4781
2016 Bangkok, Royal Government of Thailand

Links to selected list of ICT4Peace publications

Dec 2011
Getting Down to Business: Realistic Goals for the Promotion of Peace in Cyber-Space (2011)
Developments in the Field of Information and Telecommunication in the Context of International Security (2012)
Cyber Security Affairs: Global and Regional Processes, Agendas and Instruments (2013)
Confidence Building Measures and International Cyber Security (2013)
Baseline Review of ICT-Related Processes and Events (2014)

For additional information, cooperation or other requests please contact:

Dr. Daniel Stauffacher
President
ICT4Peace Foundation
danielstauffacher@ict4peace.org