Overview of existing capacity building initiatives

International cybersecurity norms, confidence building measures (CBMs) and cyberdiplomacy

version: 23/03/2020

Cyber Diplomacy

In-Person Training

CSIS course on international security in cyberspace

This initiative is intended to strengthen understanding and engagement on topics related to international security in cyberspace across the world. It has been built in recognition of the growing need for capacity building in cybersecurity policymaking. It aims to ensure that more nations are able to participate fully and contribute to international and multilateral discussions on this topic.

Who can apply:
Government representatives looking to engage on discussions on topics relating to international security in cyberspace.

Who to contact:
James Lewis, jalewis@csis.org

Organizers:
The Center for Strategic and International Studies (CSIS), with funding from United States

More information:
https://www.csis.org/

In-Person Training

Cyber bootcamp project

The Cyber bootcamp project aims to build cyber capacity across a full breadth of cyber affairs, enabling countries across the Indo-Pacific region address cyber challenges and build cyber capacity at the national and regional level by learning directly from Australian cyber policy and operational specialists across government, academia and the private sector.

Who can apply:
Government representatives selected ASEAN and Pacific countries

Who to contact:
CyberAffairs@dfat.gov.au

Organizers:
Australian National University's Cyber Institute and National Security College, with funding from Australian government

More information:
https://dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/Pages/cyber-bootcamp-project.aspx

In-Person Training

DiploFoundation course with focus on small and developing nations

The DiploFoundation organizes series of trainings that cover internet governance, cybersecurity norms, confidence building measures, and international law of cyberspace. The focus of the training are government officials from small and developing countries, which face particular resourcing challenges. The trainings also seek to bring industry and civil society voices into conversation.

Who can apply:
Government officials from small and developing nations

Who to contact:
diplo@diplomacy.edu

Organizers:
DiploFoundation, with support from partners

More information:
https://www.diplomacy.edu/

Online Training

DiploFoundation course on Internet technology and policy

This course, conducted online over a period of ten weeks, focuses on technology and core infrastructure issues in the context of public policy. It touches on issues as wide-ranging as internet names and the internet of things. It is targeted at technical experts who are keen to learn more about digital policy; and at policy people who wish to learn more about technology.

Who can apply:
Government officials, academics, journalists, civil society representatives, postgraduates

Who to contact:
admissions@diplomacy.edu

Organizers:
DiploFoundation

More information:
https://www.diplomacy.edu/courses/ITP#detail

Online Training

DiploFoundation course on introduction to cybersecurity

Today's headlines often feature the word 'cyber', reporting on threats related to the virtual world: online child abuse, stolen credit cards and virtual identities, malware and viruses, botnets and denial-of-service attacks on corporate or government servers, cyber-espionage, and cyber-attacks on critical infrastructure including nuclear facilities and power supply networks. The 10-week advanced thematic course in cybersecurity covers policy challenges, actors, and initiatives related to cybersecurity, and specifically to cybercrime, security of the core infrastructure, cyberwarfare and cyberterrorism, and Internet safety.

Who can apply:
Government officials, academics, journalists, civil society representatives, postgraduates

Who to contact:
admissions@diplomacy.edu

Organizers:
DiploFoundation

More information:
https://www.diplomacy.edu/courses/cybersecurity#details

Online Training

Global Partners Digital materials on human rights

Global Partners Digital has developed a number of forum specific resources, such as toolkits, and webinars that support greater understanding of international cybersecurity, and in particular its relation to human rights.

Who can apply:
No restrictions

Who to contact:
sheetal@gp-digital.org

Organizers:
Global Partners Digital

More information:
https://www.gp-digital.org/insight/cybersecurity/

In-Person Training

ICT4Peace workshops on cybersecurity policy and diplomacy

ICT4Peace Foundation has since 2014 offered cybersecurity policy and diplomacy capacity building workshops for governments, international organizations, as well as business and civil society. The workshops focus on international law of cyberspace, international humanitarian law, international cybersecurity norms, confidence building measures, as well as national cybersecurity strategy and legislation.

Who can apply:
Government, business, and civil society representatives

Who to contact:
annahofmann@ict4peace.org

Organizers:
ICT4Peace Foundation

More information:
https://ict4peace.org/wp-content/uploads/2019/10/Cybersecurity-Policy-and-Diplomacy-Capacity-Building-17-October-2019.pdf

In-Person Training

Tallinn Summer School of CyberDiplomacy

The Tallinn Summer School of CyberDiplomacy offers insights into how international institutions, such as the United Nations (UN, European Union (EU), North Atlantic Treaty Organization (NATO) deal with cybersecurity. It also seeks to provide an overview of the history of cyber conflict and provide an overview of the latest trends of malicious cyber activities.

Who can apply:
Young diplomats from around the world

Who to contact:
TallinnSummerschool@mfa.ee

Organizers:
Estonian Ministry of Foreign Affairs

More information:
https://vm.ee/et/summerschool

In-Person Training

UK government focused events in support of United Nations (UN) discussions

In support of the dual-track UN discussions on responsible state behavior in cyberspace, the UK government is supporting a series of outreach events with the aim of increasing and informing states' engagement with the UN processes. The first roundtable discussion was held in Addis Ababa in October 2019 for Commonwealth African countries. A second roundtable discussion in Africa is planned for March 2020.

Who can apply:
No restrictions

Who to contact:
mdp-elearning@unitar.org

Organizers:
UNITAR

More information:
http://www.unitar.org/mdp

Online Training

UNITAR course on use of digital tools

United Nations Institute for Training and Research (UNITAR) offers an online course, which aims to equip participants with the practical skills to make the best use of digital tools in pursuing diplomatic objectives. It also helps them understand the challenges and difficulties digital technologies pose for diplomacy. At the same time, it focuses on the broad range of problems generated in cyberspace and how diplomacy can be applied to managing them.

Who can apply:
No restrictions

Who to contact:
mdp-elearning@unitar.org

Organizers:
UNITAR

More information:
http://www.unitar.org/mdp

Online Training

UNODA course on cyberdiplomacy

United Nations Office for Disarmament Affairs (UNODA) developed an online course that seek to enhance understanding of technology use, and its implications for international cybersecurity. In particular it investigates existing and emerging online threats, international law and its application to cyberspace, international cooperation and assistance in cybersecurity capacity building, confidence building measures, and norms, rules and principles

Who can apply:
Interested government officials

Who to contact:
gohg@un.org

Organizers:
United Nations Office for Disarmament Affairs (UNODA) with support from government of Singapore

More information:
https://cyberdiplomacy.disarmamenteducation.org/home/

Fellowship

Women and International Security

Women and International Security in Cyberspace Fellowship was launched to increase female representation at the United Nations negotiations concerning responsible state behavior in cyberspace. As part of this initiative, up to 20 women from African and South Asian countries will be funded to attend to attend cyber policy training, and forthcoming sessions of the Open-Ended Working Group.

Who can apply:
Female government officials from African and South Asian countries with support of their employer.

Who to contact:
cybercapacity.building@fco.gov.uk

Organizers:
UK government with support from Australia, Canada, and the Netherlands

More information:
cybercapacity.building@fco.gov.uk

Cybersecurity Norms

In-Person Training

UNGGE Norms implementation in the ASEAN

Australian Strategic Policy Institute (ASPI) is currently driving a multi-year capacity-building project to support member states of the Association of Southeast Asian Nations (ASEAN) with the implementation of the 11 norms agreed in the United Nations in 2015. The project is being delivered through regional workshops and in-country training.

Who can apply:
Representatives from ASEAN member governments

Who to contact:
barthogeveen@aspi.org.au

Organizers:
Australian Strategic Policy Institute (ASPI), with support from Australian and UK governments

More information:
https://www.aspi.org.au/program/international-cyber-policy-centre

Confidence Building Measures

In-Person Training

OSCE CBM
Scenario-based exercises

The OSCE facilitates the regular organization of scenario-based discussions for its participating States. The focus of this effort is to explore how the different participating States would work together in response to a cyber/ICT security incident and how the OSCE confidence building measures can be applied during the respective incident. Such Scenario-based discussions for all 57 OSCE participating States are held either in Vienna, or in the capital of the respective Chairmanship in Office of the respective year. The OSCE Secretariat supports the participating States during the preparation and implementation of the exercises. So far, the Netherlands, Italy, Slovakia, the United Kingdom, Hungary, Germany and Romania have held and/or facilitated a scenario-based discussion at the OSCE.

Who can apply:
OSCE participating States

Who to contact:
OSCE Cyber/ICT Security team: cybersec@osce.org

Organizers:
OSCE Secretariat and various OSCE participating States

More information:
For more information, contact the OSCE Cyber/ICT Security team

In-Person Training

OSCE provided international cyber/ICT security training

The Organization for Security and Co-operation in Europe (OSCE) Secretariat regularly organizes trainings in selected regions, which aim to equip policy makers, technical experts and private sector representatives with a sound understanding of international cyber/ICT security, international law as it relates to this field, norms of responsible state behavior in cyberspace, OSCE confidence building measures and their implementation, as well as national cyber/ICT security strategies.

Who can apply:
OSCE participating states and partners, on the invitation of the OSCE Secretariat

Who to contact:
OSCE Cyber/ICT Security team: cybersec@osce.org

Organizers:
Organization for Security and Cooperation in Europe (OSCE)

More information:
https://polis.osce.org/subregional-training-role-icts-context-regional-and-international-security

In-Person Training

OSCE CBM Points of Contact facilitated dialogue and visits

The Organization for Security and Co-operation in Europe (OSCE) Secretariat is organizing in-country bilateral and multilateral visits between policy and technical Points of Contact aimed at familiarizing them with each other's work and best practices, enhancing and/ or forging institutional links, raising awareness of CBMs and building confidence necessary to make the Point of Contact network more effective in reducing risks of conflict stemming from the use of ICTs.

Who can apply:
CBM 8 Points of Contact from OSCE participating states

Who to contact:
OSCE Cyber/ICT Security team: cybersec@osce.org

Organizers:
Organization for Security and Cooperation in Europe (OSCE)

More information:
For more information, contact the OSCE Cyber/ICT Security team

International Cybersecurity Law

In-Person Training

Cyber Law International training on international law in cyberspace

This initiative, co-funded by Australia, Singapore and the Netherlands, supports the delivery of training courses to government legal and policy advisers from ASEAN and the Pacific countries to strengthen understanding of how existing international law and norms apply to states' operations in cyberspace.

Who can apply:
Government representatives from selected ASEAN and Pacific countries

Who to contact:
CyberAffairs@dfat.gov.au

Organizers:
Cyber Law International; with funding from Australian, Singaporean and the Dutch government

More information:
CyberAffairs@dfat.gov.au

In-Person Training

Executive Courses on the International Law of Cyber Operations

The Executive Courses are designed for policy advisors responsible for cyber matters and legal experts dealing with cyber/ICT issues and aim to enable them to better navigate through the complex legal issues involving cyberspace. In particular, the courses examine key legal principles and regimes of international law that govern cyber operations conducted by, or directed against, states. Other topics cover global and regional cyber efforts, inter alia the UN Working Groups and the OSCE, general international law principles, such as sovereignty and jurisdiction, as well as more specialised topics, like the law governing the use of force, human rights law, and diplomatic and consular law.

Who can apply:
Government representatives from selected OSCE participating States

Who to contact:
OSCE Cyber/ICT Security team: cybersec@osce.org

Organizers:
Organization for Security and Cooperation in Europe (OSCE)

More information:
https://cybilportal.org/projects/international-law-of-cyber-operations-executive-course/

In-Person Training

Marshall Center course on application of international law to cyberspace

This initiative is intended to enhance participants' understanding of international law as it applies to states' cyber activities, and to promote a better understanding of how existing international law provides states with binding standards of behavior that can help reduce the risk of conflict, including by creating expectations of how states may and may not respond to cyber incidents.

Who can apply:
Civilian government representatives with a focus in international law

Who to contact:
U.S. Embassy Cyber Policy Officers in participant countries or registrar@marshallcenter.org

Organizers:
The George C. Marshall Center; with funding from Dutch and United States governments

More information:
https://cybilportal.org/projects/international-law-of-cyber-operations-executive-course/