Cybersecurity Capacity Building and Research Programme for South-Eastern Europe

Conducted by DiploFoundation, in cooperation with DCAF
with the support of the Federal Department of Foreign Affairs FDFA of Switzerland

Call for applications:

Online Course on Cybersecurity for South-Eastern Europe

DiploFoundation is accepting applications for the online course **Cybersecurity for South-Eastern Europe**. This course is aimed at officials and professionals from south-eastern Europe and is organised within the Cybersecurity Capacity Building and Research Programme for South-Eastern Europe, organised in cooperation with the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and with the support of the Federal Department of Foreign Affairs FDFA of Switzerland.

Background

Cyberspace has become an essential component of modern society. Critical societal infrastructure, the financial sector, governmental services, the security sector, schools, and hospitals are increasingly and irreversibly dependent on interconnectivity and the global network. So are citizens.

The merits of the open Internet are accompanied by risks. Such risks need to be approached comprehensively and systematically though the cooperation of all stakeholders. Many countries have adopted national cybersecurity strategies and related legislation, taking into account both security and freedoms. A growing number of countries have set up national mechanisms for response to cyber-incidents, involving government as well as the corporate, academic, and NGO sectors. Some have declared 'cyber' as the fifth military domain, and have set up defensive and offensive cyber-commands within their armies.

South-eastern Europe (SEE), and especially the western Balkans, is lagging behind. The online course on cybersecurity aims to increase cybersecurity capacities of public institutions and the private and civil sectors in SEE, through providing policy training aimed in particular at young officials and professionals. Through developing the capacities of individuals, the course aims to drive a shift in public policies and encourage cooperation among countries and stakeholders. The course marks the start of a new round of the regional capacity building programme in cybersecurity, following the successful 2014 Cybersecurity Winter School within the Young Faces Network (YFN), organised by DCAF and DiploFoundation.

Online course

The interactive 10-week-long course is delivered entirely online, starting from **22 February 2016**. A group of 20 participants will gather in an online classroom to learn about cybersecurity challenges and policy and diplomatic responses, and discuss national and regional concerns and cooperation frameworks. Successful participants will receive a certificate awarded by DiploFoundation and will join Diplo's global Internet governance alumni.

The online course covers an introduction to cybersecurity and definitions; threats and vulnerabilities; cybercrime challenges and frameworks to combat cybercrime; security of the core Internet infrastructure and critical infrastructure; cyberterrorism, cyber-conflicts, and international law and norms of state behaviour in cyberspace with focus on related international and regional initiatives; national policies and mechanisms such as strategies and CERTs; security sector reforms and cybersecurity; and the broader context of cybersecurity including Internet governance, human rights, privacy and data protection, and economic growth and development.

By the end of the course, participants should be able to:

- Identify the defining features of cybersecurity, and the factors which shape the international and regional issues.
- Identify principal threats to cybersecurity; describe and analyse the key cybersecurity issues for users, and states.
- Explain the issues involved in cybercrime, its impact and investigation.
- Describe how the Internet is used for terrorism and ways to address this concern.
- Explain the threats to the core Internet infrastructure and the core infrastructure of society.
- Explain the risks of cyber-conflict and map international law and global and regional norms of state behaviour in relation to cyberspace.
- Outline key national mechanisms for prevention and response to cyber-incidents and explain the working models of the CERT.
- Map the broader context of cybersecurity, including the links with human rights, privacy and data protection, and economic growth.
- Explain and analyse the international frameworks for cybersecurity cooperation.

Eligibility

This course will be of interest to anyone who seeks to engage in the fields of cybersecurity, cyber-diplomacy, and digital policies, such as:

- Officials from ministries and authorities in charge of information society, technology, security, foreign affairs, industry and economic development, media, human rights, or education, among others.
- Diplomats responsible for digital issues or security cooperation.
- Staff of regional and international organisations whose work is related to the security sector, human rights, or digital policies.
- Representatives of the private sector, especially the ICT industry, such as telecommunication companies and Internet service providers, as well as the financial or energy sector, and other critical sectors.

- Professionals working with the critical infrastructure operators and cybersecurity bodies (such as CERTs).
- Educators, graduate students, and researchers interested in multidimensional perspectives on cybersecurity.
- Professionals and activists from NGOs and civil society working on or interested in cybersecurity.

To be considered for the course, applicants must:

- Be from and working in the SEE region: Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Greece, Kosovo*, Republic of Macedonia, Moldova, Montenegro, Romania, Serbia and Turkey.
  (Applicants from other countries are invited to apply for Diplo's regular annual online course in cybersecurity – see www.diplomacy.edu/courses/cybersecurity for more details.)
- Hold an undergraduate university degree and, ideally, at least two years relevant working experience.
- Have sufficient ability in the English language to undertake postgraduate level studies (including reading academic texts, discussing complex concepts with other course participants, and preparing short written texts).
- Be available to dedicate four to six hours per week study time (at whatever time is convenient to the participant – this might be during evenings or weekends) including a weekly one-hour meeting (at a time to be announced), in the period between 22 February and 28 April.

Priority will be given to applicants younger than 35, from the western Balkans (Albania, Bosnia and Herzegovina, Croatia, Kosovo*, Republic of Macedonia, Montenegro, Serbia).

Fee

Participation in this course for selected applicants is fully funded by the Federal Department of Foreign Affairs FDFA of Switzerland.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

Application

For more information and to apply, please visit:
http://www.diplomacy.edu/courses/SEE

Please note that you must fill out the online application form and upload your CV and a short motivation letter (maximum one page). **The application deadline is 25 January 2016; the course starts on 22 February.**