LA SECRETARÍA DE RELACIONES EXTERIORES

POR MEDIO DEL INSTITUTO MATÍAS ROMERO

CONVOCA

AL CURSO EN LÍNEA

CYBERSECURITY

QUE IMPARTIRÁ DIPLOFOUNDATION
DEL 8 DE OCTUBRE AL 14 DE DICIEMBRE DE 2018
(102 horas)

Este curso a distancia requiere comprometer diez horas de estudio a la semana. Las actividades de aprendizaje y de evaluación que deberán llevar a cabo las personas que participan se describen en el temario que aparece más abajo, en el inciso "Metodología" (*Methodology*).

Las y los participantes podrán solicitar la asistencia de quienes estén a cargo de la tutoría y el apoyo técnico de DiploFoundation.

I. REQUISITOS DE ADMISIÓN

- Buen desempeño en programas previos del IMR (no se aceptarán candidaturas de personas que tengan calificaciones reprobatorias en el último año) [*]
- Inscripción exclusiva en este curso (no se aceptarán candidaturas de personas que estén cursando otro programa del IMR de manera simultánea, excepto los cursos presenciales de inglés y francés)
- Dominio del idioma inglés
- Acceso a computadora con conexión a Internet
- Sistema operativo:Windows XP, Vista, Windows 7, MacOS X
- Hardware: 2 GB o más de RAM para Vista o Windows 7
- Software:
  - Adobe Acrobat Reader (haga clic aquí para descargarlo gratis)
  - Microsoft Office u Open Office (haga clic aquí para descargarlo gratis)
- Navegadores: Google Chrome, Internet Explorer 9 o posterior; Firefox 8 o posterior
- JavaScript, Cookies y Pop-ups (elementos emergentes) deben estar habilitados
- Registro de su solicitud de inscripción en el formulario del Campus Virtual del IMR [**]. Para ello:
  - Haga clic aquí o copie y pegue la siguiente dirección electrónica en su navegador *Google Chrome*:
  - https://registroimr.sre.gob.mx/
  - Capture los datos que se solicitan en cada una de las secciones del formulario.
    1. **Utilice la tecla <Tabulador> para desplazarse de un campo a otro del formulario.**
    2. Escriba su nombre completo, tal como aparece en su pasaporte, empleando mayúsculas y minúsculas.
    3. Utilice el campo *Observaciones*, si tiene dificultades para ingresar su nombre: descríbalas y nosotros haremos los cambios necesarios.
    4. Si es de nacionalidad mexicana, ingrese cuidadosamente su CURP. Recuerde que esa clave constituye el número de matrícula de cada participante. Si no cuenta con ella o no la recuerda, puede obtenerla en: **http://consultas.curp.gob.mx/CurpSP/** (a quienes no tengan nacionalidad mexicana y, por tanto, no cuenten con la CURP, se les asignará un número de matrícula interno).
  - Haga clic en **<Enviar>** y espere hasta que se despliegue el mensaje **¡REGISTRO EXITOSO!**
  - Haga clic en **<Aceptar>** para ver la confirmación de su registro y guarde el comprobante para futura referencia. Si durante el proceso se generara un error, capture la pantalla con ese mensaje, guárdela y póngase en contacto con la Dirección de Educación a Distancia.

Deberá enviar las cartas de inscripción (autorización y compromiso), por correo electrónico a la dirección: jhuertal@sre.gob.mx.

Le solicitamos atentamente NO enviar las cartas de inscripción al correo oficial del Instituto Matías Romero.

- Prepare su documentación

  - Carta de autorización del jefe inmediato completa (firmada y escaneada)
  - Carta compromiso completa (firmada y escaneada)

Recuerde que sólo se considerará completo el registro con el envío de dichas cartas.

Consulte el "Aviso de privacidad" aquí.

II. CRITERIOS DE SELECCIÓN

Si el número de solicitudes entregadas a tiempo y en forma fuera mayor al número de espacios disponibles, el IMR aplicará los siguientes criterios para seleccionar a quienes participarán:

1. Ser miembro de la rama Técnico-administrativa del SEM con especialidad en informática
2. Desempeño de tareas vinculadas con el tema del curso
3. Expediente (se dará prioridad a las candidaturas de personas que no hayan tenido calificaciones reprobatorias en los cursos del IMR)
4. Interés reiterado en participar en este programa en línea (se dará prioridad a las personas solicitantes cuyas candidaturas hayan sido rechazadas en imparticiones previas de este programa, si cumplen los criterios anteriores)
5. Equidad de oportunidades (se dará prioridad a las candidaturas de quienes hayan participado en menos de tres cursos del IMR)
6. Equidad en adscripciones (se pondrá un límite al número de participantes de una misma representación)

En caso de igualdad de condiciones, y como criterio adicional, se considerará el orden de llegada de las solicitudes.

III. CALENDARIO

- Publicación de la convocatoria: **jueves 20 de septiembre de 2018**
- Fecha límite de recepción de solicitudes: **viernes 28 de septiembre de 2018, a las 13:00 Hrs. (hora del centro del país)**
- Publicación de la lista de aceptados: **jueves 4 de octubre de 2018**
- Fecha de inicio del curso: **lunes 8 de octubre de 2018**
- Fecha de clausura del curso: **viernes 14 de diciembre de 2018**
- **En este programa no hay periodo de bajas voluntarias**

Todas las personas que aprueben este programa de estudio recibirán una constancia de participación que se expedirá única y exclusivamente con propósitos curriculares, para el desarrollo personal y profesional del participante.

[*] El periodo de un año de espera para quien repruebe un curso se cuenta a partir de la fecha de término del mismo.
[**] Solamente se tomarán en cuenta las candidaturas de quienes completen su registro en línea en el formulario del Campus Virtual del IMR y envíen a la dirección electrónica indicada las cartas compromiso y de autorización, debidamente firmadas y escaneadas.

CYBERSECURITY

Course details

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.

What are the real cybersecurity challenges? What is the role of diplomacy, international legal instruments, and regional and national policies in addressing these threats, and how efficient are they? How does international cooperation in cybersecurity work, and what are the roles of the various stakeholders?

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.

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

- Identify the defining features of cybersecurity, and the factors which shape the international issues.
- Identify principal threats to cybersecurity; describe and analyse the key cybersecurity issues for users, and states.
- Understand and analyse the Internet security issues for e-commerce including online banking and identity.
- Explain the issues involved in cybercrime, its impact and investigation.
- Understand the threats to the core Internet infrastructure.
- Explain the concepts of cyberwarfare and cyberterrorism, and their role in international Internet policy.
- Understand and assess the challenges involved in social aspects of cybersecurity.
- Explain and analyse the international frameworks for cybersecurity policies and strategies.

Course outline

1. Introduction to security discusses the historical development of cybersecurity, and global and geo-strategic challenges. The module distinguishes between the common, narrow, understanding of cybersecurity related to cyber-threats, and broader views which include

information security and 'friendly' cyber conquest through technological standardisation dominance. It also looks at the mapping of targets, and motives behind cyberattacks, such as hactivism, crime, espionage, terrorism, and warfare.

2. Cybersecurity threats focuses on vulnerabilities of the Internet. The module reviews key vulnerabilities of cyberspace and common cyber-security threats to individuals and institutions, such as malware (including spyware, Trojans, viruses), botnets, 'Distributed Denial of Service' (DDoS), phishing, e-scams, and identity theft.

3. Cybercrime defines and classifies cybercrime, and analyses its economic and social impact. The module then focuses on combatting cybercrime: existing legal frameworks at the global and regional levels, international cooperation frameworks and various law enforcement approaches, computer investigation, and e-forensics.

4. Internet safety defines Internet safety, and reviews the challenges of the Web 2.0 era where users are contributors and the Internet is ubiquitous. It then looks at child safety, including cyber-bullying, abuse, and sexual exploitation, and discusses ways to address these challenges through policy, education, and technology.

5. Critical infrastructure and resources explains how the critical components of the Internet work, and discusses the political dimension of global security – the (unilateral) control over the Domain Name System (DNS) – and technical vulnerabilities of the DNS. It then looks at the security and protection of the critical infrastructure: the Internet infrastructure and also water supply facilities, transport, industrial facilities, and power plants. It concludes with expected challenges of future networks: Internet of Things/Next Generation Networks and 'smart networks'.

6. Cyber-conflict and cyberterrorism discusses cyberterrorism, recent threats, and possible counteracts. It then looks at cyber-conflicts, including the main risks for triggering warfare by cyber-means, and reviews attempts to codify international humanitarian law with regards to cyberspace and draft confidence-building measures and norms related to state behaviour in cyberspace.

7. Cyber-security policies and mechanisms analyses national cybersecurity mechanisms, starting with examples of national cybersecurity strategies, followed by a close look at the importance, role, and structure of national Computer Emergency Response Teams (CERTs) / Computer Security Incident Response Teams (CSIRTs). The module then looks at existing international cybersecurity initiatives and frameworks for cooperation, including those by the private sector and technical community, and discusses the importance and risks of public-private partnerships.

8. Broader context of cybersecurity correlates cybersecurity and other social and political issues related to digital policies and Internet governance. The module looks at the connection between privacy and security, with particular reflection on social media challenges, issues of openness and online freedoms, and objectionable and harmful content. It then briefly covers ethics and gender issues, and concludes with discussing economic aspects and building trust in e-commerce.

Methodology

This course is conducted online over a period of ten weeks, including one week of classroom orientation, eight weeks of dynamic class content and activities, and one week for the final assignment. Reading materials and tools for online interaction are provided through an online

classroom. Each week, participants read the provided lecture texts, adding comments, references, and questions in the form of hypertext entries. The tutor and other participants read and respond to these entries, creating interaction based on the lecture text. During the week, participants complete additional online activities (e.g. further discussion via blogs or forums or quizzes). At the end of the week, participants and tutors meet online in a chat room to discuss the week's topic.

Course lecturers

- Mr Aapo Cederberg
- Dr Stefanie Frey
- Mr Tracy Hackshaw
- Ms Virginia Paque
- Dr Stephanie Borg Psaila
- Mr Vladimir Radunović
- Dr Tatiana Tropina