Cybersecurity
Summer
BootCamp

2017

Syllabus

Policy Makers (extensive)

Cybersecurity Summer BootCamp 2017

18-29 July - León (Spain)

www.incibe.es/en/summer-bootcamp

Organised by:

GOBIERNO DE ESPAÑA · MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA | OAS

With the cooperation of:

universidad de león

AYUNTAMIENTO DE LEÓN

León Cuna del Parlamentarismo

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

Santander

IDB Inter-American Development Bank

EUROPOL EC3 European Cybercrime Centre

INTERPOL

PROFESSORS

Asier Martínez

David Cantón

Jesús Feliz

Workshop 16

Cybersecurity basics

Workshop duration: 5 hours

Description

The objective is to act as an introduction to the concepts and issues that cybersecurity raises and its treatment in the work of Policy Makers. Specifically, it presents basic support training to facilitate the understanding and interpretation of the concepts and reports related to cybercrimes.

Syllabus

- ❑ Cybersecurity: What are we facing? (2 hours)
  - Vulnerability and threat
  - Cybercrime and cybercriminality: security incidents
  - Cryptography/Encryption
  - Anonymization systems: VPN, Deep Web, TOR network etc.
  - Traditional crimes enhanced by IT systems.
  - Major stakeholders in the detection, prevention, response and recovery in the face of cyberattacks.
  - Issues of researching on the Internet from a technical perspective.

- ❑ Introduction to cybersecurity: technology. (2 hours)
  - Evolution and the current technological context
  - Networks and operative systems
  - Virtualization
  - Public and private Cloud

- ❑ Introduction to digital forensic analysis (1 hour)
  - There will be an explanation of what digital forensic analysis consists of, its phases and the technical concepts that the workshop attendees may need to know on a day to day basis.

PROFESSOR

Vicente Moret

Workshop 17.1

Cybersecurity Legal Aspects (I). Applicable regulations

Workshop duration: 5 hours

Syllabus

- **International applicable regulatory framework**
  - Introduction to the different legal approach to cybercrime, cyberterrorism and cyberwar. Conceptual details
  - Procedural law and criminal law to face the challenge of cybersecurity
  - International humanitarian law and cybersecurity
  - International agreements and conventions
    - The Council of Europe Convention on cybercrime (Budapest 2011)
    - The Council of Europe Convention on the prevention of terrorism (Warsaw 2005)
    - Tallinn Manual
    - UN and cybersecurity
  - European Legislation
    - EU cybersecurity strategy (2013)
    - Directive 2013/40/EU
    - NIS Directive (2016)

- **Territoriality on the Internet:** international law aspects applied to cybercrime research: jurisdiction, competence and international cooperation.
  - Mechanisms for mutual assistance among authorities
  - Access to information hosted in infrastructure located in other States
  - Multinational databases
  - International bodies
  - Cooperation with private entities of other States

Cybersecurity Legal Aspects (I)

PROFESSORS

Jorge Villarino

Pablo García Mexía

Taller 17.2

Cybersecurity Legal Aspects (II). Rights and freedoms of individuals

Workshop duration: 5 hours

Description

This workshop will start by explaining the context in which the last generation of rights arise and highlighting the rights included under this category, as well as their characteristics.

Following this explanation, the topic regarding the right to access the internet and whether it may be classified as a fundamental right will be addressed. A reference will be made to the main regulations in which it has been classified as a. Later on, the principle of neutrality on the net and the open internet will be addressed. The historical evolution of these concepts and the current situation will be also addressed, including the stance of the European and North-American authorities.

The next part of the workshop will focus on the main conflicts between fundamental rights on the Net. By using real cases in Europe and in the United States, the main characteristics of freedom of expression on the Internet will be explained, as well as their limits and their protection systems. Likewise, the evolution of the conflict between freedom and security will be analysed and, particularly, the extent to which the freedom on the Internet may be limited for the sake of security. This part will end with a brief reference to the Computer Emergency Response Teams (CERTs).

The third and last part of the workshop will deal with some of the main challenges facing privacy from the perspective of the new General Regulation on Data Protection. Technical and legal aspects of Big Data and Analytics will be studied, as well as the leakages of information and the obligations that organisations must comply with; international data transfers, including the new system for transfers to the United States and the role that the BCR may play; the organisational and technical measures which must be implemented by the organisations, including the role of privacy from the design stage and by default, the PIAs and the data protection officers.

Syllabus

- ❑ The development of "fourth generation" rights.
- ❑ The right to access the Internet: neutrality on the net and the open internet.
- ❑ Fundamental freedoms in cyberspace: expression vs. information Freedom vs. security. The CERTs.
- ❑ Privacy and data protection: territorial borders in a barrier-free connected world.
    - ○ Big Data and analytics: legal and technical aspects.
    - ○ Leakages of information.
    - ○ From the Safe Harbour to the Privacy Shield: international data transfers. The BCR.
    - ○ Organisational and technical measures to be implemented in the organisations. Privacy from design and by default. PIAs. The DPO.

PROFESSORS

Marco A. Lozano

Alejandro Diez

Workshop 18 (1/4)

Cybersecurity for Business – First part (Marco A. Lozano and Alejandro Diez)

Workshop duration: 1 hour 30 minutes

Syllabus

- Fundamentals and standards of information security: information security management system (ISMS) and information system auditing. Risk management and methodology to manage regulatory compliance
- Actual implementation of basic protection measures for the SME.
- Examples of sector regulation and self-regulation:
  - PCI-DSS, financial environment
  - Emerging technologies (Cloud Computing, IoT, RFID, etc.)

PROFESSOR

Rafael García del Poyo

Workshop 18 (2/4)

Cybersecurity for Business – Second part (Rafael García del Poyo)

Workshop duration: 3 hours 30 minutes

Description

Cybersecurity is an area that has recently become one of the biggest concerns for companies subject of analysis, investment and allocation of resources by all types of companies. A trend that is likely to be more relevant day by day, even more after the latest events at worldwide level that have put security measures and procedures of many large companies at stake. In general terms, companies should be better prepared both technically and organizationally as to be able to efficiently deal and cope with this type of events.

The purpose of this session is not only to focus exclusively on the applicable regulation at national level in relation to cybersecurity, but also to provide a legal and eminently practical vision on other aspects directly or indirectly related and demanded by companies based on business risk management from the perspective of cybersecurity. These include the delimitation of the responsibility of companies and their directors/officers or the implementation of crime prevention strategies or compliance programs.

Syllabus

- ❑ The new labour relations and corporate control in digitalized companies
  - Introduction
  - Brief overview of the fundamental rights of workers within the framework of labour relations and their limits
  - Proportionality criteria
  - New booming measures implemented in recent years
    - The use and monitoring of e-mail and computer tools made available to workers
    - Installation of video-surveillance cameras and CCTV
    - The installation of access control devices using biometric data
    - The implementation and use of geolocalization devices
  - Personal and professional use social networks and implications in their implications from a labour relation standpoint

PROFESSOR

Rafael García del Poyo

Workshop 18 (3/4)

Cybersecurity for Business – Second part (Rafael García del Poyo)

Syllabus

- ❑ Risk management methodology and compliance management
    - Introduction
    - Risks identification in accordance to the current regulatory framework
    - Special reference to the protection of personal data
    - Identification of main operational and reputational risks at stake
    - Identification of the needs of a company with regard to the preparation of internal guides or manuals and procedural issues.
- ❑ Cybersecurity in social media and business reputation
    - Introduction
    - Digital identity
    - Main risks in the management of social networks and their impact in the reputation of companies
    - Public sphere and private sphere
    - Protection of personal data and new European Data Protection Regulation
    - Big data and Internet of Things
    - Legal persons
        - ○ Right to forget
        - ○ Right to honour
    - Brief reference to the Directive on measures to ensure a high common level of security of information networks and systems in the Union
    - Management of an incident
    - Implementation of policies for responsible use of social networks by employees.

PROFESSOR

Rafael García del Poyo

Workshop 18 (4/4)

Cybersecurity for Business – Second part (Rafael García del Poyo)

Syllabus

- ❑ The criminal responsibility of legal persons: compliance
  - Introduction
  - Historical evolution of criminal liability of legal persons
  - New measures introduced by the Organic Law 1/2015
  - Analysis of the Circular 1/2016 on criminal liability of legal persons under the reform of the criminal code implemented by organic law 1/2015
  - Compliance Programs, what are they?
  - Differences between compliance and corporate social responsibility
  - Business compliance program
  - Compliance officer. Obligations and responsibilities
  - Content of a compliance program
  - Establishment of procedures and control measures
  - Detection, notification and management of an incident
  - Standardization and international standards - ISO / UNE standards
- ❑ The responsibility of directors and officers
  - Introduction
  - New liability regime for directors
  - Duties of directors and officers
  - Civil liability regime
  - Liability actions and other assumptions
  - Differences between de facto and de jure administrators
  - Prevention measures
  - Insurance policies for directors and officers (D & O insurances)
- ❑ Cybersecurity insurances
  - Introduction
  - What are they?
  - Current situation of cybersecurity in Spain and third countries
  - Who are the target and needs of the insured
  - Risks to be covered by the cibersecurity insurance policy
  - Blockchain and Smart Contracts

PROFESSORS

Javier I. Zaragoza

Jorge Bermúdez

Workshop 19 (1/2)

Cybercrime and Global Digital Criminality

Workshop duration: 5 hours

Description

The development of information and communication technology has deeply modified the co-habitation rules and behavioural patterns of our society. Despite the fact that the implementation of these new channels of communication has been positive for all citizens, it has also given rise to new criminal conducts, hitherto unknown in our legal system. For these purposes, the legislator has made a laudable effort to adapt our Criminal Code to the new nature of these crimes by introducing very innovative criminal concepts (stalking, sexting, childgrooming) and adapting previous concepts -such as fraud- to the new social reality.

On the other hand, the use of new technologies has opened a wide range of possibilities for investigation and clarification of criminal actions. After the last reform implemented in our Criminal Procedure Code, the outdated article 579, once and for all, has been overcome, by introducing specially innovative means for investigation such as the online undercover agent.

The purpose of this workshop is to explain the new criminal phenomenon which has been the result of the ever-increasing importance of new technologies, the new criminal concepts created to fight this issue, the new technological investigation measures used to clarify the crimes and the impact derived from the use of these technologies on fundamental rights. These topics will be explained both from a theoretical and a practical perspective through the explanation, and discussion, of real experiences lived by both speakers during the development of their professional activities.

PROFESSORS

Javier I. Zaragoza

Jorge Bermúdez

Workshop 19 (2/2)

Cybercrime and Global Digital Criminality

Workshop duration: 5 hours

Syllabus

- ❑ Introduction to Cybercrime
  - Concept of Cybercrime
  - Evolution of criminal behaviour
  - The role of the Public Prosecutor's Office in the fight against cybercrime
- ❑ Main types of offences
  - Unauthorised dissemination of personal images. Sexting.
  - The new harassment crime. Stalking
  - Harassment of minors through the net. Childgrooming
  - IT damage crime. Attacks against critical infrastructures. Cyberterrorism.
  - Glorification of terrorist actions through the net. Its conflict with the right to freedom of expression. The new offence of self-indoctrination.
  - Hate crimes and gender-based violence crimes committed through the net.
  - Protection of victims of crimes committed through the net. Removal of contents and access blocking.
- ❑ New technological investigation measures
  - New technological investigation measures and their conflict with fundamental rights. The right to virtual environment.
  - New regulation for the online undercover agent.
  - Investigation through the IP address. Regulation after the reform implemented by virtue of Act 13/2015.
  - IMEI and IMSI investigation.
  - The new regulation for the inspection of mass storage devices.
  - The collaboration of service provider entities.
  - The quick preservation of web-based materials.

PROFESSOR

Manuel Huerta de la Morena

Workshop 20.1 (1/2)

Technological Investigation and Digital Evidence (I) – First part (Manuel Huerta)

Workshop duration: 2 hours 30 minutes

Syllabus

- ❑ Fundamentals of technological research. The requirements of the electronic evidence, The correct identification of the scenarios, the precepts of the test Conservation, inalterability and repeatability and the correct understanding of the antecedents and the scenarios.
    - Procedural aspects in the LECRim: the remote control of devices and the undercover agent in the network. The contextualization of evidence as a process of identification or dismissal of false evidence. Remote control and multiuser access in corporate environments and systems with remote maintenance.
    - Retention of data. The processes of acquisition of evidence, the typology of scenarios, technologies and acquisition techniques. Analysis and conservation, process automation technology, simulation of scenarios and systems operation.
- ❑ The management of electronic evidences The triage of evidences and the magnitudes of information.
    - Actions aimed at the identification of terminal and user, and their value in trial. The contextualization of the activity under analysis, the link between terminal and user, author or victim?
    - Electronic sources and means of proof. How to provide legal security to electronic documents. The identification of scenarios as sources of information, the approach to legal guarantees, defenselessness and effective judicial protection, the contrast of sources as evidence guarantee in processes of effective communication with electronic documentation. Contextualization of communications.
    - Legal regime of electronic evidence in the process: verification of the facts, obtaining and providing electronic evidence. The existence of decontextualized proof, systems of verification of authorship and action, The falsification of evidences, systems of discarding of intervention in evidences by third parties, Evidence indications and the request of requirements.
    - Metadata, downloads and certification of content and traffic data: digital public faith. The role of suppliers in the process of issuing evidence, The notarial role in electronic evidence and real dangers in notarial activity.
    - Associated risks in the electronic test and collision with fundamental rights. The Chain of Custody. The chain of custody before, during and after the acquisition process, The importance of the procurement process, HASH and DNA as part of the chain of custody.
    - Digital forensic analysis and its practice through forensic experts ("computerforensics"): the forensic report and its value in judgment. The researcher's morality and impartiality, research capability vs. technical capability, the importance of laboratory infrastructures, the importance of the forensic technology report format, its outline and key points.

PROFESSOR

César Lorenzana

Workshop 20.1 (2/2)

Technological Investigation and Digital Evidence (I) – Second part (César Lorenzana)

Workshop duration: 2 hours 30 minutes

Description

During the workshop, the students will have to solve a practical case in which they will have to analyze the initial evidences, establish the investigation paths, and gather the leads in order to find out who the offender is. The case is an investigation of a distributed denial-of-service (DDoS) attack. It will start with the collection of evidence of the attack, and through the investigation process the student will be able to progress through different lines until the investigation is successfully completed and the offender identified.

Syllabus

- □ Presentation, missions, and capacities of Central Cybercrime Unit of Guardia Civil (10 min)

- □ Description of investigation process (20 min)
  - Collection of evidence from affected systems (crime scene)
  - Initial actions to obtain information OSINT (without judicial control)
  - Technological Investigation Process (determination of the place of connection)
  - Traditional Investigation Process (determination of the suspect)
  - Compilation of evidence

- □ Case study (2 hours)
  - Presentation of the case study
  - Dissemination of information and initial data
  - Development of investigation (application of the methodology) with practical examples.
  - Solution of the investigation (in case the students do not reach the solution, the process followed to determine the responsible will be described)

Technological Investigation and Digital Evidence (I)

PROFESSOR

Manuel López Guerra

Workshop 20.2 (1/2)

Technological Investigation and Digital Evidence (II) – First part (Manuel López Guerra)

Workshop duration: 2 hours 30 minutes

Description

Case study of an investigation carried out by the National Police

Syllabus

- ❑ Specialized research units: Technological Research Unit – National Police
- ❑ Presentation of a case study:
    - Remote device control. Problems.
    - Procedure for obtaining and processing electronic evidence in an entry and registration procedure at the domicile of the author of the facts.
    - Implications of fundamental rights: secrecy of communications, secret communications with a lawyer, etc.
    - Forensic analysis of evidence from the police point of view.

PROFESSOR

Manuel de Campos

Workshop 20.2 (2/2)

Technological Investigation and Digital Evidence (II) – Second part (Manuel de Campos)

Workshop duration: 2 hours 30 minutes

Description

In recent years, New Technologies have burst into the field of crime, causing a drastic change of paradigm in terms of Criminal Investigation, since not only has the commission structure for most of the traditional crimes changed, going from the physical space to the digital space, but also new specific crimes committed in cyberspace through digital media have been discovered and created. This situation requires a significant change regarding the methods of investigation, a change that must include all fields related to crime; and this is where electronic evidence or digital evidence, as it is currently known, takes on special importance, as well as every aspect related to its gathering, processing, chain of custody and in-court assessment, due to its specific nature.

The workshop is aimed at defining the concepts of evidence, digital or electronic evidence and digital or electronic proof, as well as the different aspects of such evidence (element, perpetrator, means and purpose of evidence) and then to develop and analyse in detail the digital evidence, how and who must obtain it, the proper way to treat it, the special characteristics of its chain of custody and, finally, in-court assessment thereof.

Syllabus

1. **Actions towards the identification of terminal and user, and its legal value.**
   The ways through which a terminal and user may be identified will be addressed, since one of the main objectives of criminal investigation is to determine "who" committed the crime.
2. **Electronic means of proof and sources. How to provide legal certainty to electronic documents.**
   The specific characteristics of the digital evidence sources will be addressed; this is closely related to the way to obtain it (identification processes, collection or acquisition and conservation or preservation), as well as the aspects of this type of proof; the definition of the roles of the specialists in electronic evidence management will also be analysed.
3. **Legal system of the electronic evidence in the process: verification of facts, gathering and submission of electronic evidence.**
   The global standard for best practices for the management of digital evidence will be discussed (identification, collection, consolidation and preservation), as well as its basic principles: application of methods and processes subject to audit, reproduction and defence.
4. **Metadata, downloads and certification of contents and traffic data: digital official certification.**
   The concept of metadatum will be addressed, as well as its registries, classification (metadata designed for a general purpose and metadata designed for a specific purpose), information schemes, and its usefulness in an investigation.
5. **Related risks in the electronic evidence and conflict with fundamental rights. Chain of custody.**
   The process to obtain digital information may affect the right to privacy; it is therefore essential to find the right balance between security and privacy, between the subject matter of digital investigation and the fundamental freedoms and the right way to legislate these issues. The value of the chain of custody as a guarantee of the right to a legal defence will be also analysed.
6. **Digital forensic analysis and its practice by forensic experts: the forensic report and its legal value.**
   The characteristics of the proper treatment of digital evidence will be analysed, as well as the required skills, the work of the expert, the characteristics of the report and its evidential value.

PROFESSORS

Manuel Ransán

Alejandra Frías

Workshop 21

Cybersecurity and minors – First part (Manuel Ransán)

Workshop duration: 2 hours

Description

The fundamentals will be addressed on issues related to the use of the Internet and ICT by minors. Its main characteristics and situation data will be discussed, and strategies and recommendations will be presented for prevention and response in case of an incident, both in the family environment and in the school environment. Also the role of the Internet Security Centers of the European network INSAFE will be analyzed

Syllabus

- ❑ Issues related to the use of the Internet by minors
  - Inappropriate contents
  - Dangerous behavior
  - Harmful contacts
- ❑ Good practices for prevention and response
  - Familiar environment
  - School environment
- ❑ Internet Security Centers (IS4K) and the INSAFE network

Cybersecurity and minors – Second part (Alejandra Frías)

Workshop duration: 3 hours

Syllabus

- ❑ Media and digital literacy
- ❑ Protection of minors on the net
- ❑ Cybercrimes affecting minors: the Lanzarote Convention and Directive 2011/93/EU