ecrime

The Economic Impacts of Cyber Crime

Lausanne
2016 May the 30th

Agenda for Lausanne opportunity identification workshop

9:30-10:00 Registration and coffee

10:00-10:30 Welcome, update on the E-CRIME project, and introduction to today's proceedings

10:30- 11:30 Round Table

11:30-12:30 Presentation of results of WP7

12:30-14:00 Coffee and networking

14:00-15:00 Discussion and propositions

15:00-15:50 Consolidation of WP7

15:50-16:00 Closing statement

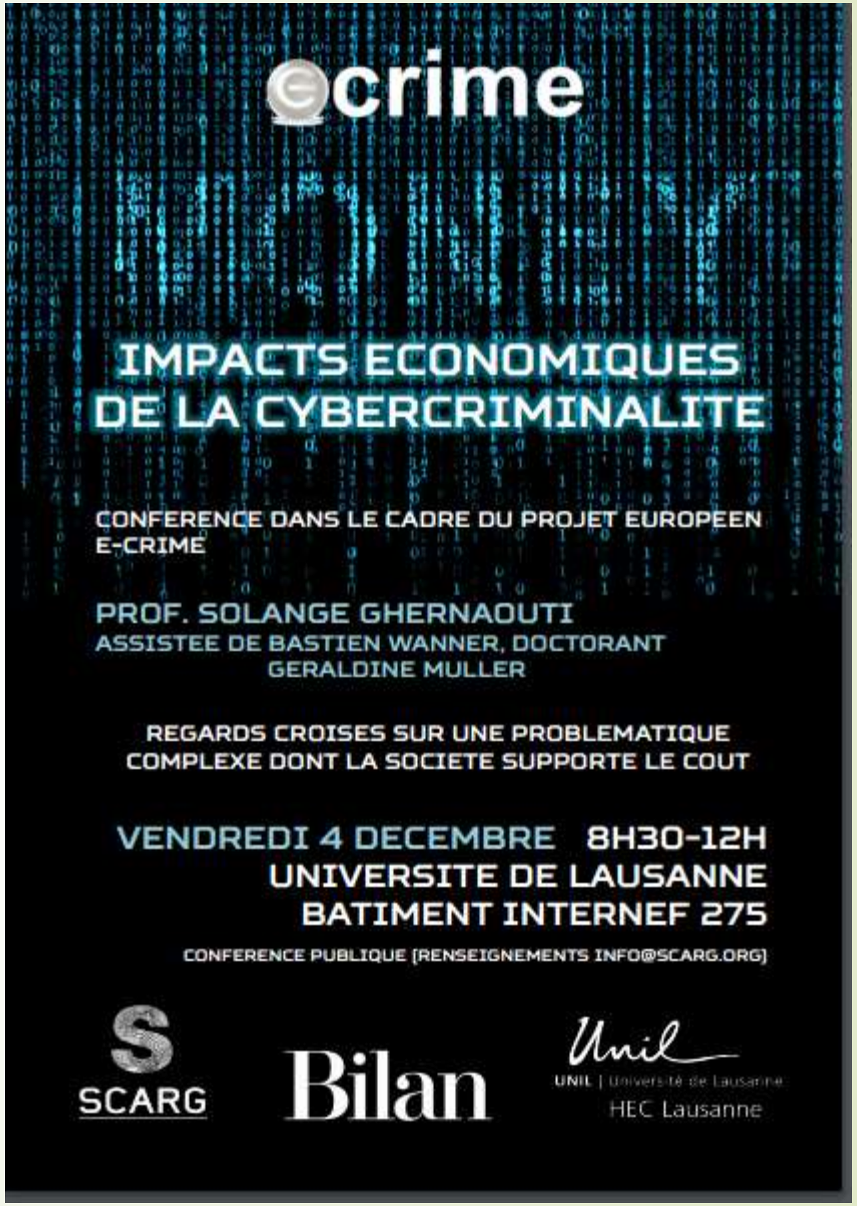
Conferences

Organized :

2015 Décember 4

UNIL - Impacts économiques de la cybercriminalité : Conférence organised by Pr Solange Ghernaouti and HEC Lausanne, opened by the Conseillère d'Etat de l'Etat de Vaud (Minister for Justice and Police Affairs of the Vaud's Canton). Participation of CNUSED and GIPRI.

120 people



ecrime

IMPACTS ECONOMIQUES DE LA CYBERCRIMINALITE

CONFERENCE DANS LE CADRE DU PROJET EUROPEEN E-CRIME

PROF. SOLANGE GHERNAOUTI
ASSISTEE DE BASTIEN WANNER, DOCTORANT
GERALDINE MULLER

REGARDS CROISES SUR UNE PROBLEMATIQUE COMPLEXE DONT LA SOCIETE SUPPORTE LE COUT

VENDREDI 4 DECEMBRE 8H30-12H
UNIVERSITE DE LAUSANNE
BATIMENT INTERNEF 275

CONFERENCE PUBLIQUE [RENSEIGNEMENTS INFO@SCARG.ORG]

Participation to :

2016 January 25/26

Christian Aghroum : Agora « Cyber et éthique »

Forum International de la Cybersécurité – Lille. Thema of the year : « Data Security and Privacy » https://www.forum-fic.com/site/FR/Intervenants,I59989.htm

70 people

New Dehli 2016 February 2

Solange Ghernaouti « Cyber Weapon and Cyber Power: A new warfare Paradigm »

Presentation and discussion at the Observer Research Foundation

45 people

New Delhi 2016 February 3

Solange Ghernaouti « Is digital privacy and personal data protection compatible with big data and cloud computing? »

Presentation and discussion at the Indian Institute of Technology (Centre of Excellence in Cyber Systems and Information Assurance) (http:///)

25 people

2016 February 8-10

Organisation internationale de la francophonie 08 – 10 février 2016 Grand- Bassam / Abidjan – Côte d’Ivoire - Conférence francophone sur le renforcement de la cybersécurité et de la cyberdéfense

Solange Ghernaouti « Les enjeux de la cybersécurité et de la cyberdéfense »

Christian Aghroum « Surveillance de masse, vie privée et liberté d'expression : quelles réponses francophones ? »

80 people

2016 February 20

Solange Ghernaouti « Homo Numericus : quel avenir pour les secrets d’état ? »

Archives nationales, Paris

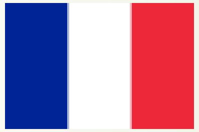
50 people

2016 March 22

Solange Ghernaouti « Anticipation et résilience par la formation et la recherche, retour d'expérience des projets européens E-Crime et PrismaCloud, Conférence « Cybermenaces à l'horizon 2020 : enjeux, anticipation et résilience »

Université de Savoie Mont-Blanc, Chambéry Campus scientifique

60 people

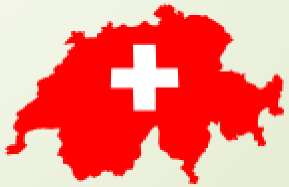


2016 April 6

Solange Ghernaouti : «Cyberrisques et approches cybersécuritaires – initiatives européenne et internationale. Enjeux et perspectives pour la Suisse ».

Sicherheitsverbund Schweiz - Réseau national de sécurité - 4e Cyber-landsgemeinde, Stade de Suisse Wankdorf.

200 people http://www.vbs.admin.ch/internet/vbs/fr/home/themen/security/svs/Medienmitteilungen.html



D7.1: Report on the opportunities for deterring and fighting cybercrime across non ICT sectors

- Contents :

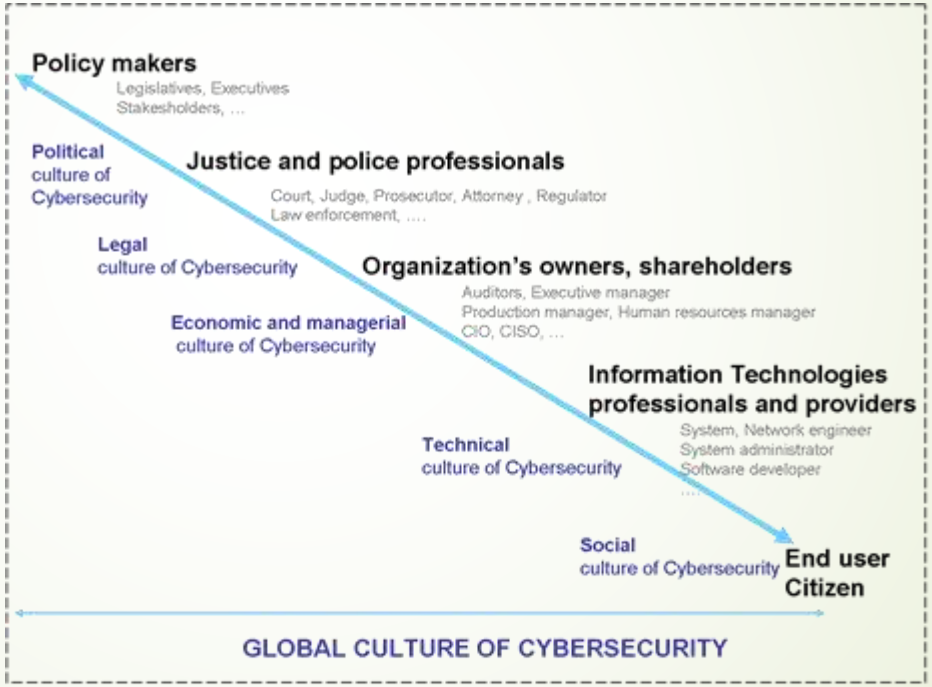
- http://www.francophonie.org/IMG/pdf/25._quelle_cooperation_internationale_pour_prevenir_les_cyber-conflits.pdf

Conclusions to share :

- **VIII - Conclusion and perspective: global culture of cybersecurity**
- **VIII.1 Perspective**
- **VIII.2 Political dimension**
- **VIII.3 Organizational dimension**
- **VIII.4 Technological dimension**
- **VIII.5 Social dimension**

ecrime

The Economic Impacts of Cyber Crime


Policy makers
Legislatives, Executives
Stakeholders, …
Political
culture of
Cybersecurity
Justice and police professionals
Court, Judge, Prosecutor, Attorney , Regulator
Law enforcement, ….
Legal
culture of Cybersecurity
Organization's owners, shareholders
Auditors, Executive manager
Production manager, Human resources manager
CIO, CISO, …
Economic and managerial
culture of Cybersecurity
Information Technologies
professionals and providers
System, Network engineer
System administrator
Software developer
….
Technical
culture of Cybersecurity
Social
culture of Cybersecurity
End user
Citizen
GLOBAL CULTURE OF CYBERSECURITY

VIII.2 Political dimension

Because Cybersecurity and cybercrime issues are governmental issues, and national security issues, government people should understand:

- Links between social and economic development with crime and security issues in a connected society with interrelated infrastructures;
- ICT related threats and risks for states, organizations and citizens including privacy and economic crime issues;
- Needs for protection at national, regional and international levels;
- The role of all relevant stakeholders and relationships between private and public sectors;
- To define general measures to be taken to obtain a satisfying level of ICT security and protection assets (including privacy issues);
- How to create, maintain and develop trust in ICT environment;
- How to develop strategic improvement in ICT security.

Conditions : understanding of:

- Legal requirements at national and international levels;
- Computer investigation and forensic methodologies and tools;
- How to interpret and implement existing international regulation as Cybercrime convention of Council of Europe (doctrine) that could be considered as an international reference model to develop legal frameworks and international cooperation.

Common understanding

- Define a legal framework, appropriate cyber laws enforceable at national level and compatible at the international level;
- Develop measures to fight against cybercrime and to be able to collaborate at an international level.

VIII.3 Organizational dimension

If we consider the business and organization's points of view, executive managers of any size organisation (including small and medium enterprises) should understand basic principles in ICT security management, in particular on the following topics:

- Assessments of vulnerabilities and threats;
- Security mission, management practices and conditions of success;
- How to identify valuable assets and related risks;
- How to define security policy;
- How to organize security mission, to control, to evaluate, to audit, to estimate cost;
- How to manage security in complex and dynamic environments.

In order to be able to:

- Produce effective security process and master ICT related risks and security costs;
- Collaborate with legal, law enforcement and technical professionals;
- Create appropriate organizational structures and procedures.

VIII.4 Technological dimension

Concerning the technology dimension of cybersecurity ICT professionals should:

- Understand ICT technical vulnerabilities and misuse;
- Understand ICT related risks, cyber threats and cyberattacks;
- Understand societal and organizational issues and values.

In order to be able to:

- Decrease the number of vulnerabilities of digital environments;
- Define, design, produce, and implement efficient security tools and measures of protection and reaction to support availability, integrity and confidentiality of ICT infrastructures and develop confidence into e-services.

Security Technologies should be:

- Cost effective;
- User friendly;
- Transparent;
- Auditable;
- Third party controllable.

VIII.5 Social dimension

Any citizen should:

- Understand threats for the end-user (virus, spam, identity usurpation, fraud, swindle, privacy offence, etc.…) and their impacts
- Understand how to adopt a security behavior for a safe use of ICT resources
- Understand how to build a global cybersecurity culture based on well recognized international standards and recommendations, involving several kinds of stakeholders

In order to raise awareness among all interested parties.

As mentioned by Mr. Dempsey, Education and Science Minister of Ireland, during the 2004 OCDE meeting of Education Ministers: "Education is a key factor to strengthen competitiveness, employment and social cohesion."

Education is a critical factor of success to become an actor of the information society. Education is the cornerstone of a knowledge-based society. Thanks to education the digital divide and the cybersecurity divide could be reduced.

Therefore, to enhance confidence and security in the use of ICT and cybersecurity education should not be considered as an option.