



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 Décembre 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

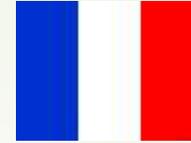
CONFERENCE PUBLIQUE [RENSEIGNEMENTS INFO@SCARG.ORG]

S
SCARG

Bilan

Unil
UNIL | Université de Lausanne
HEC Lausanne

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,159989.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.

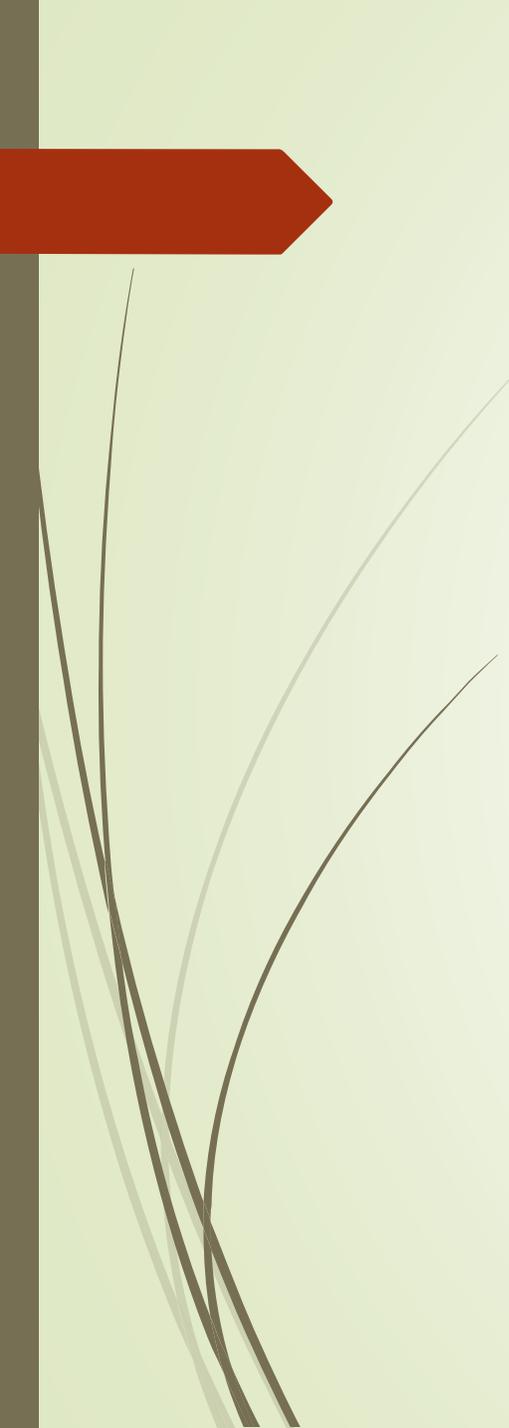
200 people <http://www.vbs.admin.ch/internet/vbs/fr/home/themen/security/svs/Medienmitteilungen.html>



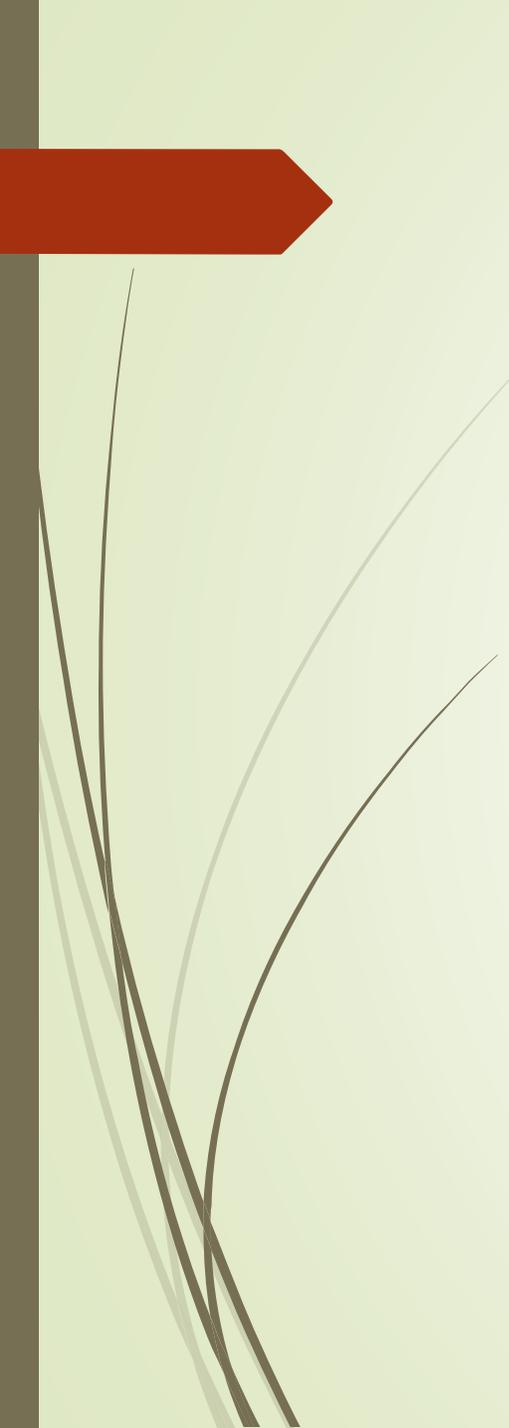


D7.1: Report on the opportunities for deterring and fighting cybercrime across non ICT sectors



- 
- Contents :
 - I. Introduction and methodology 7
 - I.1: Needs and justification 7
 - I.2: Lessons from the past 8
 - I.2.1: Cyber criminality: an additional crime. 8
 - I.2.2: Cyber criminality, a peculiar crime 9
 - I.2.3: Cybercrime, a new challenge 10
 - I.2: Methodology and approach 11
 - I.3: Expected outputs 14
 - II. Key findings and results from work packages 2, 3, 4, 5 & 6 14
 - II.1: Identification of inter-sector and common solutions 14
 - DO BE DONE BY WP LEADERS 14
 - II.2: Critical analysis of opportunities 15
 - III. Main challenges and constraints 15
 - III.1: Risk management 15
 - II.1.1: Goals and definitions 15
 - III.1.2: Understanding the underlying concepts 16
 - III.1.3: Risk management and security process 19
 - III.1.4: Information security management definitions 19
 - III.1.5: Difference between risk management and information security Management Processes 22
 - III.2: Political issues 24
 - III-2-1: Democratic Issue: 24
 - III-2-2: Understanding of the phenomena: 25
 - III-2-3: A perpetual challenge: 26
 - III-2-4: A European and international answer 27

- ▶ III -3: Economic issues 27
- ▶ III-3-1: The victim supports the cost of cyber criminality 27
- ▶ III-3-2: Society supports the cost of cyber criminality 28
- ▶ III-3-3 – Cyber risk still sparsely insured 29
- ▶ III-3-4 – Is the cost of cybercrime too low? 29
- ▶ III-3-5: Cybersecurity is a flourishing market 30
- ▶ III.4 Legal and procedural issues 30
- ▶ III.5 International cooperation issues: 32
- ▶ III.5.1: Strengthening international cooperation and law enforcement 32
- ▶ III.5.2 : Law of the sea and space law 34
- ▶ III.5.3 : Reflections on cyber laws 35
- ▶ III.5.4: Tallin's manual 36
- ▶ III.5.5: The Convention of Budapest 36
- ▶ III.5.6: The African Union convention 37
- ▶ III.5.7: International prosecution instruments 38
- ▶ III-6: Civil liberties and human rights ambitions 38
- ▶ III.6.1 – Some complex and global questions 39
- ▶ III.6.2 - Privacy definition and global approach 39
- ▶ III.6.3 – The main issues in privacy 39
- ▶ III.6.4 - Computer related crime and the needs of justice and the police 41
- ▶ III.6.5 - Privacy stakes and challenges 42
- ▶ III.6.6 - Beyond geographical borders 43
- ▶ III.6.7 - Beyond the idea of freedom 45
- ▶ III.6.8 - Beyond the digital web 46
- ▶ III.6.10: Some privacy related considerations 49
- ▶ III.6.11: Privacy definition and global approach 49
- ▶ III.6.12: The main issues in privacy 49
- ▶ "In developing countries, human rights organizations understand the need for privacy but do not have the technology. Those in developed countries have the technology but do not think they need to protect privacy". 50
- ▶ III.6.13: Computer related crime and the needs of justice and the police 51
- ▶ III.6.14: Privacy stakes and challenges 52

- 
- IV. Recommendations for justice and police systems 53
 - IV.1: Human: Enhancing the level of initial and continuous training 53
 - IV-2: Many levels necessary 54
 - IV-3: A multidisciplinary approach 54
 - IV-4: enforce competencies 55
 - IV-5: Promote training 55
 - IV-6: Encourage European excellence 55
 - IV-4: Maintaining a high level of public-private partnership 56
 - IV-7: Take the partnerships out of the European borders 56
 - IV.8: Technical: Justice and Police 3.0 57
 - IV-8.1: Towards more reactivity 57
 - IV-8-2: a court in line with the world 3.0 57
 - IV.9: Organizational 58
 - IV-9-1: European cooperation 58
 - IV-9-2: European and national points of complaints 59
 - IV-9-3: Encourage joint investigation teams 59
 - IV-9-4: Associating extra-European countries to in vivo training of cyber judges and investigators. 59
 - IV-9-5: Practicing immersion of officers and liaison magistrates 60
 - IV-9-6: Statistics 60
 - IV.10: Constraints of cybercrime investigations 60
 - IV.11: Economical challenge 65
 - IV.12: Economical challenge 67
 - IV.12-1: the cost of criminal trial: 68
 - IV.12.2 – the high cost of investigations in the fight against cyber criminality: 68
 - IV.12-3: The whole cyber, an asset: 68

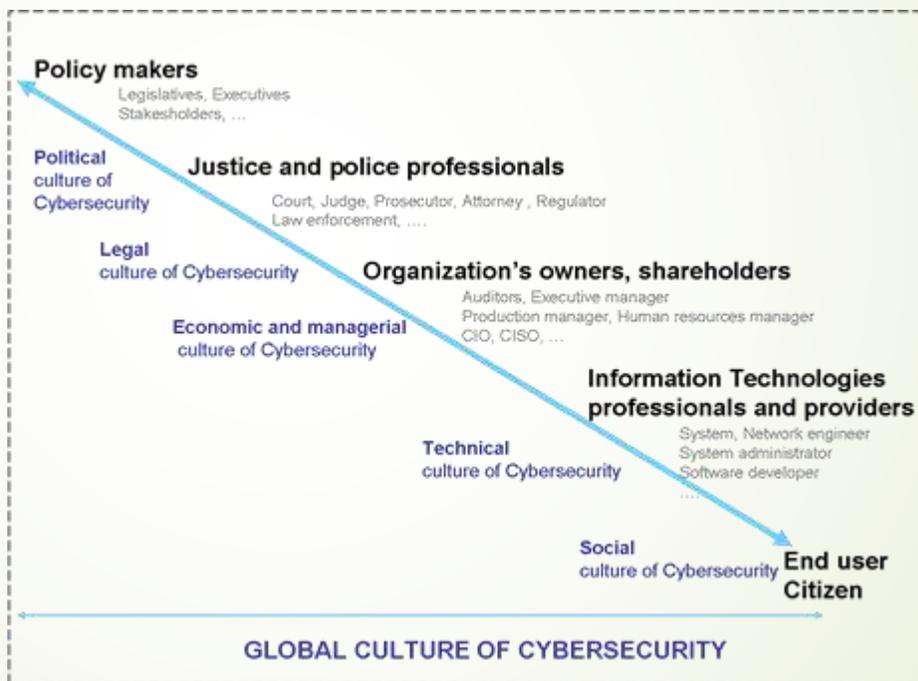
- V. Recommendations for public and private organization 70
- 1. Partnership with all different stakeholders (NGO, federations, associations ...) 70
- 2. Expectation from the ICT sector 70
- 3. Responsibilities and roles of ICT providers in the non-ICT sector 70
- 4. Managerial, technical and human requirements for institutions (alert procedures, audits, reporting, recruitments, awareness, continuous training, risk management, crisis management, business continuity plans, etc. ...) 70
- 5. Addressing and defining the issues of liability where does it stop and start. For example, in certain cybercrimes does the victim potentially shoulder some of the responsibility if they did not implement basic security measures to protect themselves? And where does the liability WITHIN the organizations stand. 70

- VI. Opportunities for end users and citizens 71
- VI.1. Education, awareness 71
- VI.2. Responsibilities via a better comprehension of technical and human risks 72
- VI.3. Security mindset and privacy behavior 73
- VI.4 - Planning the needs for next twenty years 74
- VI.5 - Alerts, whistle blowers 74
- VII. Classification and prioritization of actions 75
- VII.1 Recapitulative dashboard of the main opportunities 75
- VII.1.1 : Anticipation 75
- VII.1.4: Other enlightenments 78
- VII.2 High level and practical recommendations for stakeholders 78
- VII.3 Capacity building 79
- VIII - Conclusion and perspective: global culture of cybersecurity 81
- VIII.1 Perspective 81
- VIII.2 Political dimension 82
- VIII.3 Organizational dimension 83
- VIII.4 Technological dimension 83
- VIII.5 Social dimension 84
- IX. Références 84
- 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**



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.