Cybersecurity academic activities in France and Europe
A few items

Claude Kirchner

It will be about:

- Towards Cyber Peace
- German strong push on cybersecurity @ Saarbrücken
- Cartography of the French academic research on cybersecurity

JE SUIS
INTERNET

« Construire la paix et la sécurité internationales de la société numérique »

Acteurs publics, acteurs privés : rôles et responsabilités

6-7 avril 2017

“ Building international peace and Security in the digital society ”

Public actors, private actors : duties and responsabilities

April 6th-7th 2017

https://jesuisinternet.today

UNESCO
UNITED NATIONS
Educational, Scientific, Cultural Organization

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Saarland wird erste Adresse für IT-Sicherheit

Janek Böffel / Onlinefassung: Thomas Braun 14.03.2017 | 16:53 Uhr

Vorlesen

Das CISPA an der Saar-Uni gilt als eine der Top-Forschungseinrichtungen im Land. Jetzt steigt es in die erste Kategorie der Institute auf und wird Helmholtz-Forschungszentrum. Das schafft massenhaft neue, hochqualifizierte Arbeitsplätze.

Gerade einmal 18 Helmholtz-Forschungszentren gibt es in Deutschland, darunter das Deutsche Zentrum für Krebsforschung und das Deutsche Zentrum für Raum- und Luftfahrttechnik. Ab kommendem Jahr kommt das CISPA-Helmholtz-Forschungszentrum IT Sicherheit, wie es wohl heißen wird, in Saarbrücken dazu.

500 ARBEITSPLÄTZE, 50 MILLIONEN EURO JAHRESETAT

CISPA-Helmholtz
research centre on cybersecurity
in Saarbrücken, Germany

500 people
50 Meuros annual budget

Cartography of the French academic research on cybersecurity

Gildas Avoine (CDEFI) Nora Cuppens (CDEFI) Hervé Debar (IMT)
Sébastien Gambs (CPU) Marc-Olivier Killijian (CNRS) Claude Kirchner (Inria)
Florent Kirchner (CEA) Jean Mairesse (CNRS) Laurent Olmedo (CEA) Didier
Rémy (Inria) Jean-Louis Roch (CPU) Jean-Pierre Tual (Gemalto)


cnrs
dépasser les frontières


Inria
INVENTEURS DU MONDE NUMÉRIQUE


cea
energie atomique • energies alternatives


ALLISTENE
l'alliance des sciences
et technologies du numérique


INSTITUT
Mines-Télécom


Conférence
des présidents
d'université


DEFI
Conférence des Directeurs
des Ecoles Françaises d'Ingénieurs

Goals of this cartography

We use *a two levels taxonomy*, 11 main categories and some 60 sub-categories for:

- **Goal 1**: *quantitative evaluation* of the academic research forces in France (via the 11 main categories)
- **Goal 2**: *qualitative evaluation* of the implication on sub-domains (via les 60 sub-categories)

Taxonomy: the 11 main categories

1- Cryptology design, techniques and protocols

2- Formal methods, and theory of security and privacy

3- Security services

4- Intrusion/anomaly detection and malware mitigation

5- Security in hardware

6- Systems security

7- Network security

8- Database and storage security and privacy

9- Software and application security

10- Human, societal and ethical aspects of security and privacy

11- Forensics

Quantitative evaluation

- **No distinction between the academic employers (CEA, CNRS, Engineering schools , Inria, Universities)**

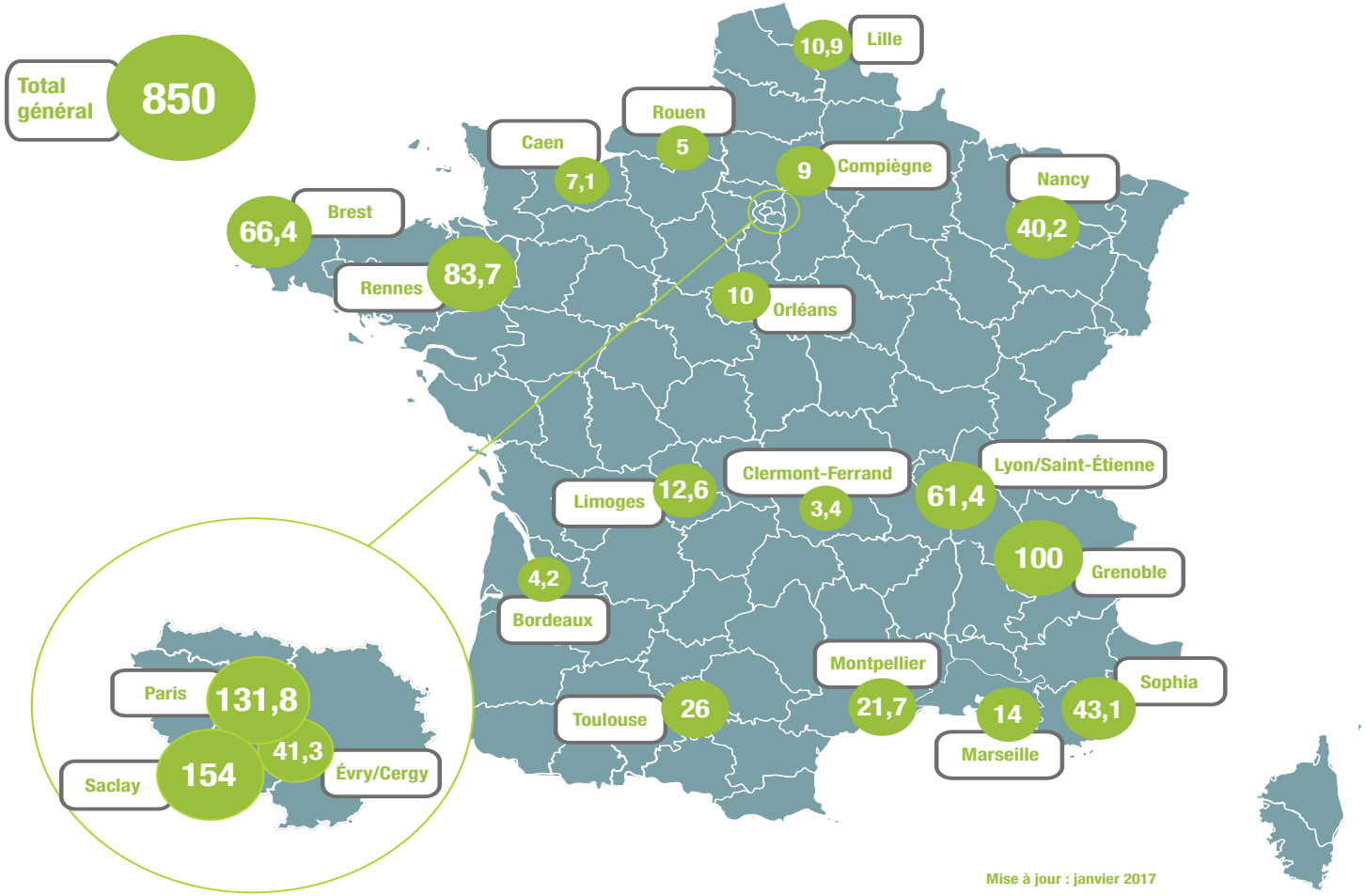
- **Three types of results:**
  - Total number of active persons
  - Full time equivalence (ETP) for research
  - Repartition of ETP amongst the 11 main domains

- **Example of research ETP computation:**
  - Full time researcher involved at 80% of his research time on cybersecurity = 0,8 ETP
  - Professor or associate prof. at 80% of his research time on cybersecurity = 0,4 ETP

Research Human Power

ETP for research only	**825**
Total number of persons	**914**
Researchers	136
Faculty	215
Engineers	126
Post-doc	80
Phds	357

Répartition géographique des ETP en cybersécurité



Mise à jour : janvier 2017

Main domains ETPs

Activity in cybersecurity	100%
1 Cryptology design, techniques and protocols	20%
2 Formal methods and theory of security and privacy	14%
3 Security services	8%
4 Intrusion/anomaly detection and malware mitigation	9%
5 Security in hardware	18%
6 Systems security	10%
7 Network security	8%
8 Database and storage security and privacy	3%
9 Software and application security	6%
10 Human, societal and ethical aspects of security and privacy	2%
11 Forensics	3%

Qualitative evaluation

No distinction between the academic employers (CEA, CNRS, Engineering schools , Inria, Universities)

Every team answer with a boolean 0/1 describing its implication in the 60 sub-domains

Example: « Post-quantum cryptography - 22 » means that 22 teams work on this sub-domain

Cryptology design, techniques and protocols

1	**Cryptology design, techniques and protocols**				
1	1	Key management			18
1	2	Public key (asymmetric) techniques			24
1	2	1	Digital signatures		16
1	2	2	Public key encryption		25
1	3	Symmetric cryptography and hash functions			13
1	3	1	Block and stream ciphers		11
1	3	2	Hash functions and message authentication codes		10
1	4	Cryptanalysis and other attacks			28
1	5	Information-theoretic techniques			15
1	6	Mathematical foundations of cryptography			22
1	7	Cryptography for identity management			13
1	8	Secure multiparty computation			17
1	9	Post quantum cryptography			21
1	10	Quantum cryptology			5
1	11	Steganography			7

Open questions

- **Does it exists similar cartographies for:**
  - Some European countries?
  - Globally for EU?

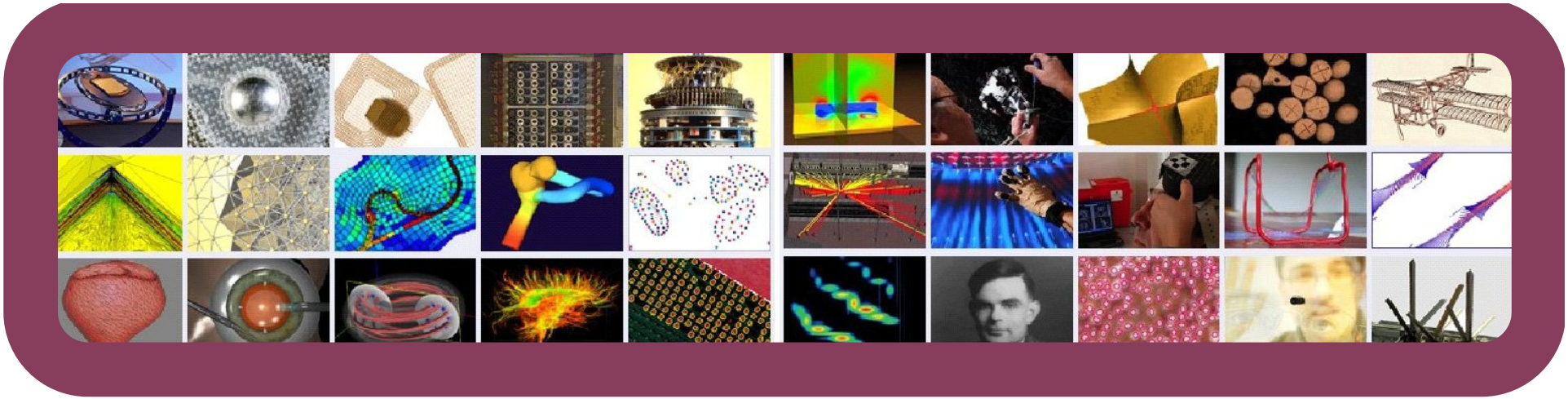
- **How does France compare into EU and internationally?**

- **How can we extend this work to research on cybersecurity in industry as well as in agencies like ANSSI, DGA, …**

Conclusion

- The taxonomy may evolve to include interdisciplinary topics like
  - Machine learning
  - Big data
- The taxonomie is open access and open to joint development, in all domains like ``Human, societal and ethical aspects of security and privacy'':

10. Human, societal and ethical aspects of security and privacy
    - 10.1. Economics of security and privacy
    - 10.2. Social and organizational aspects of security and privacy
    - 10.3. Legal protections
    - 10.4. Usability in security and privacy
    - 10.5. Ethics of research and usages
    - 10.6. Crisis analysis and resilence
    - 10.7. Risk analysis and trust evaluation



Thank you!

claude.kirchner@inria.fr