



9th International Cybersecurity Forum

24TH & 25TH
OF JANUARY 2017

LILLE
GRAND PALAIS

Cartographie académique en cybersécurité
GT Cybersécurité de l'Alliance des Sciences
et Technologies du Numérique (ALLISTENE)



Smarter security for future technologies

INTERVENANTS/ SPEAKERS

Claude Kirchner, Directeur de recherche, Inria

Jean Mairesse, Directeur adjoint, CNRS – Institut des sciences de l'information et de leurs interactions (INS2I)



24 & 25
JANVIER 2017 | LILLE
GRAND PALAIS



Membres du GT Cybersécurité

- Gildas Avoine (CDEFI, Rennes)
- Nora Cuppens (CDEFI, Rennes)
- Hervé Debar (IMT, Paris-Sud)
- Sébastien Gambs (CPU, Montréal)
- Marc-Olivier Killijian (CNRS, Toulouse)
- Claude Kirchner (Inria, Siège, animateur)
- Florent Kirchner (CEA, Paris Saclay)
- Jean Mairesse (CNRS, Paris, co-animateur)
- Laurent Olmedo (CEA, Paris)
- Didier Rémy (Inria, Paris)
- Jean-Louis Roch (CPU, Grenoble)
- Jean-Pierre Tual (Gemalto, Meudon)



24 & 25
JANVIER 2017

LILLE
GRAND PALAIS



Objectifs de la cartographie

- Taxonomie à deux niveaux : 11 grandes catégories, et environ 60 sous-catégories
- **Objectif 1** : évaluation quantitative des forces de recherche en France (via les 11 catégories)
- **Objectif 2** : évaluation qualitative des sous-domaines forts ou au contraire moins présents (via les 60 sous-catégories)



24 & 25
JANVIER 2017 | LILLE
GRAND PALAIS



Taxonomie GT : les 11 catégories

- *1- Cryptology design, techniques and protocoles*
- *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*



24 & 25
JANVIER 2017

LILLE
GRAND PALAIS



Évaluation quantitative

- **Tous employeurs académiques confondus (CEA, CNRS, Ecoles d'ingénieurs, Inria, Universités)**
- **Trois types de résultats :**
 - Nombres total de personnes impliquées
 - Equivalent Temps Plein (ETP) pour la recherche
 - Répartition des ETP entre les 11 grands domaines
- **ETP pour la recherche. Mode de calcul par l'exemple:**
 - Chercheur à 80% sur la cyber = 0,8 ETP
 - Enseignant-chercheur à 80% sur la cyber = 0,4 ETP



24 & 25
JANVIER 2017 | **LILLE**
GRAND PALAIS



Forces totales de recherche

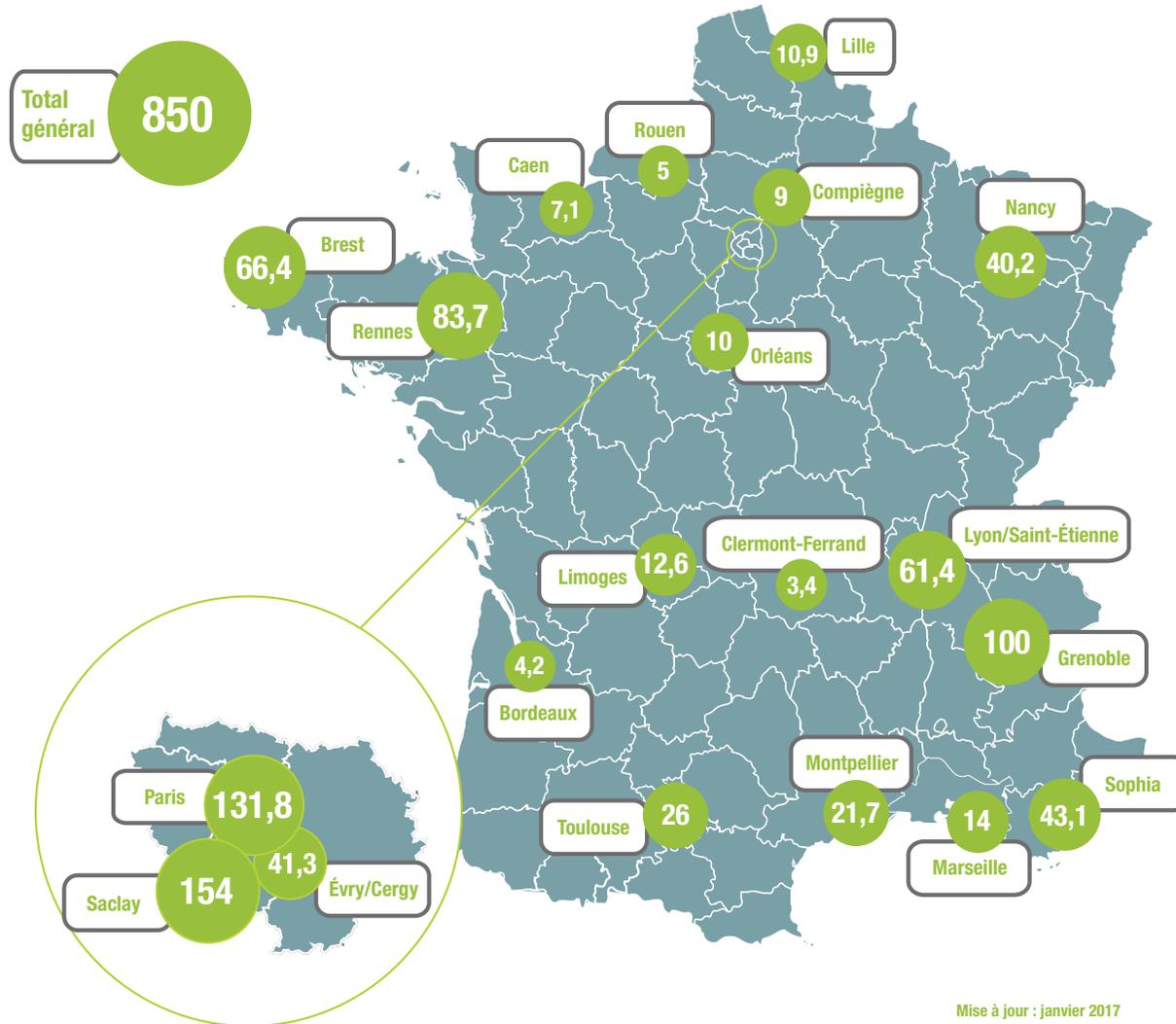
ETP pour la recherche	852
– Chercheurs	143
– Enseignants-chercheurs	130
– Ingénieurs	126
– Post-doctorants	82
– Doctorants	371
Nombre de personnes	1 101



24 & 25 | **LILLE**
JANVIER 2017 | GRAND PALAIS



Répartition géographique des ETP en cybersécurité



Mise à jour : janvier 2017



24 & 25
JANVIER 2017 | **LILLE**
GRAND PALAIS



ETP par grands domaines

Activity in cybersecurity

- 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

100%

20%

16%

8%

8%

17%

10%

8%

3%

6%

2%

3%



24 & 25
JANVIER 2017

LILLE
GRAND PALAIS



Évaluation qualitative

Tous employeurs académiques confondus (CEA, CNRS, Ecoles d'ingénieurs, Inria, Universités)

Chaque équipe répond par un booléen 0/1 sur son implication dans les 60 sous-disciplines

Explication des résultats par l'exemple : « Post-quantum cryptography - 22 » signifie que 22 équipes contribuent au thème



Cryptology design, techniques and protocols

1	Cryptology design, techniques and protocols	
1	1 Key management	18
1	2 Public key (asymmetric) techniques	25
1	2 1 Digital signatures	17
1	2 2 Public key encryption	26
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	29
1	5 Information-theoretic techniques	15
1	6 Mathematical foundations of cryptography	23
1	7 Cryptography for identity management	13
1	8 Secure multiparty computation	17
1	9 Post quantum cryptography	22
1	10 Quantum cryptology	5
1	11 Steganography	7



24 & 25
JANVIER 2017 | LILLE
GRAND PALAIS



Formal methods and theory of security and privacy

2 Formal methods and theory of security and privacy

2 1 Trust frameworks

18

2 2 Security and privacy requirements

24

2 3 Formal security models including security policies

27

2 4 Logic and verification

35



24 & 25
JANVIER 2017

LILLE
GRAND PALAIS



Security in hardware

5 Security in hardware

- 5 1 Tamper-proof and tamper-resistant designs
- 5 2 Embedded systems security
 - 5 5.2. Firmware security
- 5 3 Hardware security implementation
 - 5 5.3. Hardware-based security protocols
- 5 4 Hardware attacks and countermeasures
 - 5 4 1 Malicious design modifications
 - 5 4 2 Side-channel analysis and countermeasures
- 5 6 Hardware reverse engineering

15

23

9

21

15

21

12

25

12



24 & 25
JANVIER 2017

LILLE
GRAND PALAIS



Exploitation du travail effectué

- Communication sur ces informations
- Appropriation par les équipes
- Préparation d'un document de synthèse centralisant les cartographies
 - recherche,
 - plateformes,
 - enseignement



24 & 25
JANVIER 2017 | LILLE
GRAND PALAIS



Questions ouvertes

- **A-t-on des cartographies comparables :**
 - des autres pays d' Europe ?
 - globalement de l' UE ?
- **Comment situer la France et l' Europe dans le monde ?**
- **Comment étendre la démarche pour inclure les autres forces de recherche nationales, à savoir celles des agences gouvernementales et de l'industrie ?**



24 & 25 | **LILLE**
JANVIER 2017 | GRAND PALAIS



Conclusion

- **Première cartographie publique des forces académiques françaises en cybersécurité**
- **Une recherche en cybersécurité conséquente avec plusieurs domaines phares**
- **Un quasi-doublement des effectifs depuis le précédent recensement datant de 2008**
- **Des éléments objectifs pour construire les stratégies française et européenne**



24 & 25
JANVIER 2017

LILLE
GRAND PALAIS

