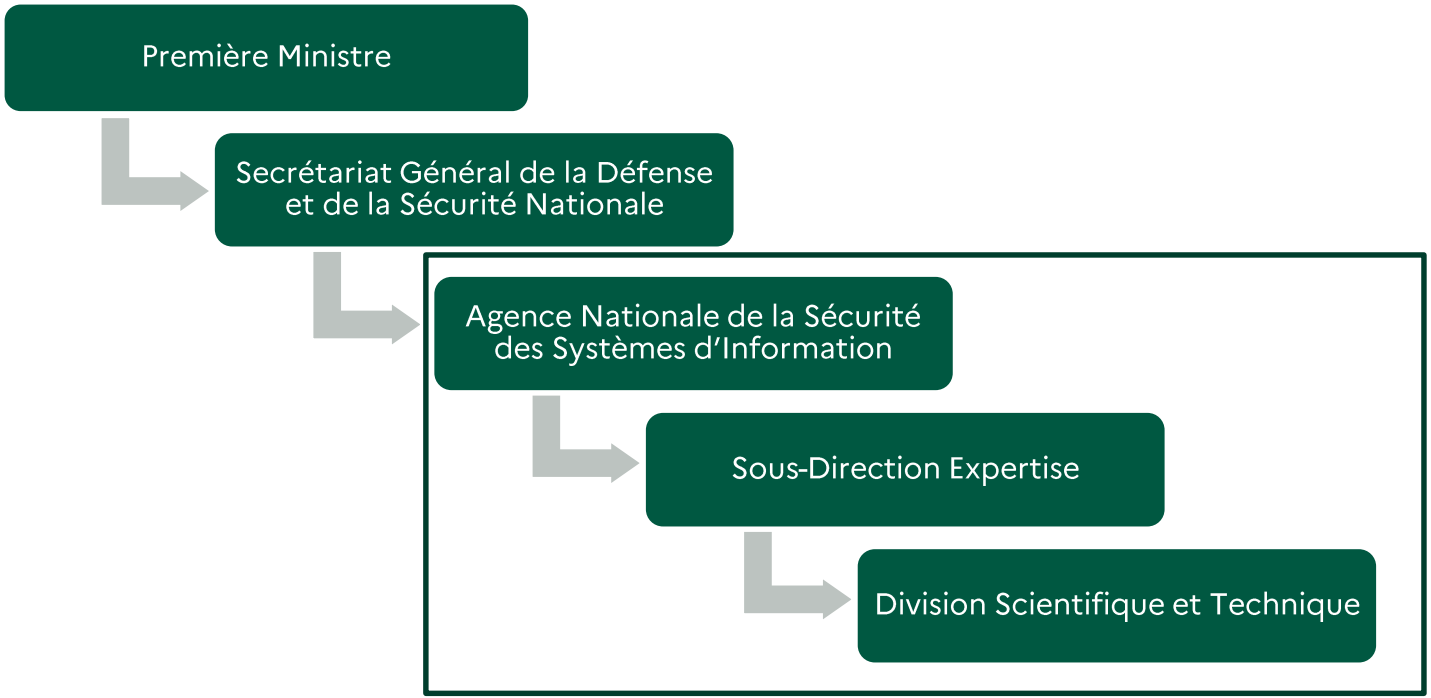
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Orientations R&D de la division scientifique et technique de l'ANSSI

Aline Gouget Morin
Cheffe adjointe de la division scientifique et technique

25/05/2023


Première Ministre
Secrétariat Général de la Défense et de la Sécurité Nationale
Agence Nationale de la Sécurité des Systèmes d'Information
Sous-Direction Expertise
Division Scientifique et Technique

La division Scientifique et Technique : 7 laboratoires…

Autorité nationale pour le Chiffre

- Laboratoire de Cryptographie (LCR)
- 2010 — Laboratoire de la sécurité des composants (LSC)
- Laboratoire architectures matérielles et logicielles (LAM)
- 2011 — Laboratoire réseau et protocoles (LRP)
- 2015 — Laboratoire exploration des données et détection (LED)
- 2017 — Laboratoire de la sécurité du logiciel (LSL)

Autorité nationale pour le Tempest

- Laboratoire de la sécurité des réseaux sans fil (LSF)

… basés à Paris et à Rennes

Nos missions au sein de l'agence

1. Maitriser l'état de l'art de la sécurité des technologies et des systèmes d'information dans nos domaines de compétences.

2. Conduire les missions **d'autorité nationale** pour le ***Chiffre*** et pour le ***Tempest*.**

3. Définir les **référentiels techniques** de l'agence**.**

4. Anticiper les évolutions des technologies afin d'orienter nos **travaux de R&D** pour être en capacité de fournir une **expertise technique** aux autres bureaux de la sous-direction Expertise ou des autres sous-directions de l'agence (Opérations et Stratégie) ainsi qu'au Centre de Certification National.

5. **Former** sur différents domaines de la sécurité des technologies et des systèmes d'information via le centre de formation de l'agence CFSSI.

Orientations R&D de la division ST

Certains travaux R&D des laboratoires de la division ST ne sont pas capturés par les enjeux techniques décrits dans la suite de cette présentation et sont néanmoins essentiels à nos missions afin notamment :

- d'émettre des avis sur les différents algorithmes et protocoles cryptographiques utilisés par les systèmes gouvernementaux;
- être à l'état de l'art dans le domaine du Tempest;

Les enjeux techniques définis par la SDE de l'agence identifient des enjeux prioritaires et des enjeux exploratoires.

Cette présentation est la sélection de certains de ces enjeux en les déclinant au périmètre de la division ST sans aucune recherche d'exhaustivité.

Enjeu technique prioritaire
la transition vers la cryptographie post-quantique

Contexte

- possibilité de l'émergence future d' un ordinateur quantique suffisamment puissant pour compromettre la sécurité d'une grande partie de la cryptographie utilisée aujourd'hui;
- Les motivations pour initier cette transition au plus vite sont notamment :
  - la **possibilité d'attaques rétroactives** sur la confidentialité des communications qui seraient enregistrées aujourd'hui dans le but d'être décryptées plus tard;
  - temps nécessaire à la réalisation par chacun d'un **état des lieux de ses usages de la crypto** afin **d'analyser les risques** et **prioriser les étapes de la transition;**
  - contribuer à l'amélioration de la résilience;
  - besoin de gagner en maturité de **la sécurité des implémentations**.
- une recommandation majeure de l'agence pour cette transition est l'**hybridation** qui consiste à combiner des algorithmes classiques éprouvés avec des algorithmes post-quantiques largement analysés par la communauté de recherche.

Orientations R&D pour ST

- participation à l' effort international de la communauté de recherche en cryptographie post-quantique piloté par l'organisme de normalisation américain NIST;
- travaux de R&D sur les volets cryptanalyse, conception, et protection des implémentations;
- **avis scientifique de l'ANSSI** publié en 2022 sur le site de l'agence et un complément de cet avis sera publié à l'été 2023.

Enjeu technique prioritaire
l'informatique nuagique et les interconnexions de systèmes

Contexte

- la migration d'une partie des systèmes d'information a été initiée vers le « cloud » sans nécessairement avoir préalablement évalué l'impact sur la sécurisation des données qui ont été transférées;
- le référentiel SecNumCloud ne permet pas de s'adresser à tous;
- l'émergence du « data-centric security» permettant de « traiter » notamment de manière sécurisée les informations selon différents niveaux de sensibilité.

Orientations R&D pour ST

- mécanismes sous-jacents à certaines offres cloud, e.g. conteneurisation, confidential computing, introspection de machines virtuelles;
- analyse des avantages et inconvénients des technologies « Data-centric security »;
- recommandations de sécurité pour les interconnexions de transfert de données.

Enjeu technique prioritaire
la numérisation des services

Contexte

- accélération de la généralisation des services en ligne en raison de la pandémie Covid 19;
- besoin de disposer d'une identité numérique de confiance;
- initiative européenne de la mise en place d'un portefeuille électronique européen.

Orientations R&D pour ST

- maintenir un niveau élevé de sécurité pour les services les plus sensibles y compris lorsqu'ils sont déployés sur des téléphones mobiles;
- analyser les propriétés de sécurité de produits existants pour réaliser des votes de manière électronique, e.g. vote des français à l'étranger ou élections non politiques comme les élections professionnelles ou les primaires de partis politiques;

Enjeu technique prioritaire
améliorer les pratiques de développement

Contexte

- dans la plupart des solutions numériques, des vulnérabilités sont un jour ou l'autre trouvées et il n'existe pas a priori de solution qui en soit exempte;
- une fois la vulnérabilité connue, il est essentiel de la corriger au plus vite afin de limiter autant que possible son exploitation;
- il est essentiel que chaque entité concernée dispose des informations pertinentes pour pouvoir évaluer rapidement l'impact d'une vulnérabilité et de mettre en place une procédure adaptée au traitement des corrections.

Orientations R&D ST

- contribuer à la progression de la généralisation de l'outillage d'analyse de code aussi bien par les laboratoires d'évaluation de la sécurité que par les développeurs de produits de sécurité;
- élaboration de guides sur certains langages de programmation et dissémination de bonnes pratiques;
- contribuer à l'adoption de l'approche *secure by design* au niveau matériel afin notamment d'améliorer des architectures de processeurs (protection du flow d'exécution, protection de la gestion mémoire...)

Enjeu technique prioritaire
la détection

Contexte

- avec la généralisation de l'utilisation du chiffrement des flux, la détection réseau perd en efficacité ;
- les dispositifs de détection doivent être complétés par des équipements supplémentaires de détection utilisant des données système ;
- les techniques d'intelligence artificielle appliquées au domaine cyber et à la détection en particulier sont à investiguer.

Activités R&D ST

- améliorer les capacités de détection en général, e.g. l'extraction d'information depuis les protocoles réseau, la prise en compte des spécificités de certains protocoles, créer de nouveaux outils pour analyser certaines données système, etc. ;
- améliorer les méthodes de détection d'anomalies/comportementale;
- améliorer les méthodes de détection reposant sur l'utilisation de métadonnées;
- évaluer les algorithmes de Machine Learning pertinents pour la détection.

Enjeux techniques exploratoires

Intelligence artificielle

- analyse de l'utilisation de l'IA dans le domaine de la détection,
- évaluation des méthodes d'IA utilisée dans des produits de sécurité,
- attaques par canaux auxiliaires.

La mesure de la santé de l'internet français

- l'ANSSI effectuait en partenariat avec l'AFNIC sous la marque « observatoire de la résilience de l'internet français » des mesures sur l'ensemble du périmètre de l'internet, avec pour objectif d'émettre des recommandations pour en renforcer la résilience et la sécurité;
- ces activités, inactives depuis 4 ans, vont être relancées en juillet 2023.

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Merci pour votre attention ☺