Comité de la filière industrielle de sécurité

Technologies critiques et technologies de rupture

F. Murgadella - SGDSN

Lyon, le 17 octobre 2018

@FiliereSecurite #Rencontrescofis

TECHNOLOGIES CRITIQUES

Une **technologie critique de sécurité** est une technologie **essentielle et sensible** pour la mise en œuvre de missions de sécurité **sur laquelle pèsent des risques de maitrise** (nombre de fournisseurs très restreints, rentabilité insuffisante, risque de prise de contrôle capitalistique, perte de savoir-faire, absence de technologies alternatives ou de contournement possible etc.).

La définition prise ici pour le terme technologie est extensive : il peut s'agir au cas par cas de composants, de procédés, de sous-système, voire de systèmes entiers, de compétences académiques, etc.

TECHNOLOGIES CRITIQUES

- Gouvernance : Pilotage par l'Etat (SGDSN et ministères).
- Trois phases de travail
  - Identification des technologies critiques de sécurité.
  - Recensement des entreprises en particulier des PME entrant dans la chaine de valeurs des technologies critiques identifiées.
  - Définition des plans d'actions à mettre en œuvre pour soutenir les technologies critiques retenues, au plan national ou européen.

TECHNOLOGIES CRITIQUES

- Analyse guidée par la segmentation CoFIS et les ruptures technologiques identifiées
- 2 critères pour les technologies actuelles
  - Caractère essentiel et sensible des technologies
  - Risques concrets pesant sur la maitrise nationale
- 27 technologies identifiées comme critiques.
- Exemples :
  - Cyber : sondes d'analyse et sondes souveraines de détection.
  - Systèmes complets de contrôle d’accès logique et physique.
  - Système radio privé offrant des communications de groupe sécurisées.
- Des entreprises identifiées sur ces segments

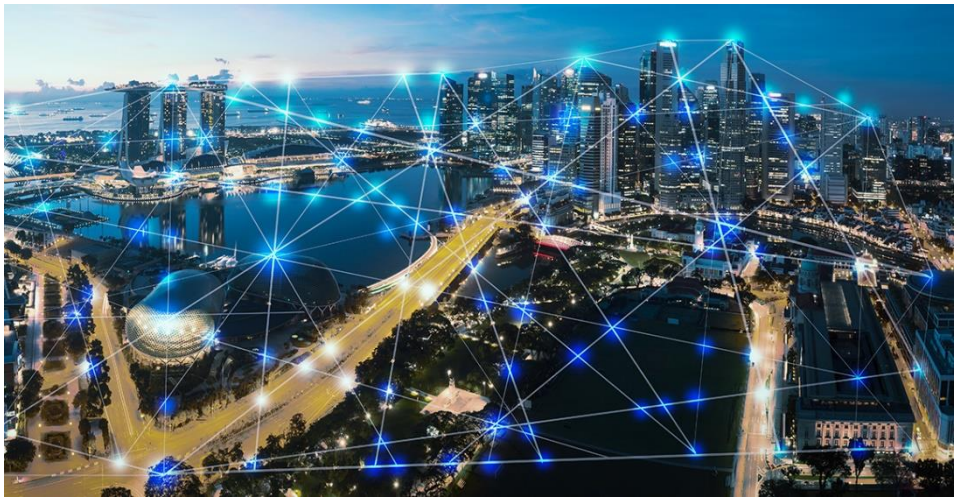
TECHNOLOGIES DE RUPTURE

Une technologie de rupture pour la sécurité sera une technologie qui devrait être indispensable pour les missions de sécurité avec un impact fort sur le marché de la sécurité à horizon 2025.

Certaines de ces technologies pourront s'avérer critiques et nécessiteront des plans d'actions afin de favoriser leur développement.

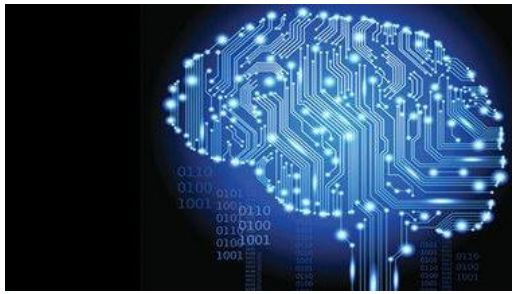
QUELS ENJEUX POUR LA SÉCURITÉ À HORIZON 2025-2030?

- Rôle central des données et correction par design
- Bouleversements induits par les technologies au niveau des usages
- Nouveaux modèles économiques et nouveaux acteurs
- Transparence et acceptation



12 Domaines de rupture à fort impact pour la sécurité

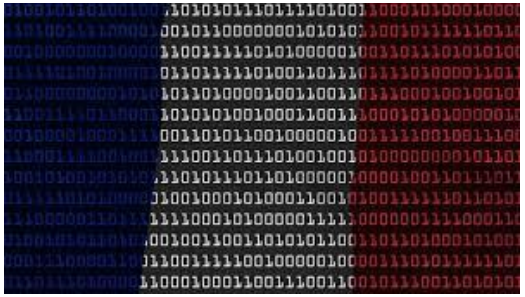
- Ruptures « métiers » pour l'ensemble des professionnels de la sécurité
- Nouveaux modèles de confiance
- Nouvelle dynamique des marchés
- Foisonnement technologique
- Vers une sécurité « cognitive »



Intelligence artificielle, HW de confiance
Plates-formes intégrées véhicules services, drones, robots
Détection de produits dangereux ou illicites, contrefaçon
Intervenant augmenté
Observation locale
Identification authentification
Interface entre les mondes réels et virtuels
Blockchain pour la sécurité
Objets connectés
Big-Data pour la sécurité
Analytics pour la sécurité
Ubérisation et post-ubérisation de la sécurité
Plates-formes ouvertes pour la sécurité

RUPTURES: LES DIFFÉRENTS AXES D'ANALYSE

- Souveraineté économique et protection des données
- Maximisation du retour sur investissement et de la création de valeur
- Optimisation des engagements financiers de l'état
- Compromis acceptation sociétale vs apport à la sécurité nationale



SCENARIOS ET ANALYSES CROISÉES

Souveraineté économique et protection des données: position nationale par rapport aux ruptures.

Tech scenario
Lego-like Web

- **Plates-formes ouvertes pour la sécurité**
- **Drones, robots…**
- **Interface entre mondes réels et virtuels**
- **Intervenant augmenté**
- **Objets connectés**
- **Détection**
- **Blockchain**
- **Analytique**

Big-Data - Plates-formes IoT - Blockchain - IA en Open Access - Open Data - API ouvertes - Standards

Club scenario
Paying for trust

- **Identification / authentification**

Interface utilisateur - Réel/virtuel - Données perso et Analytics - Services Premium - Verticales connectées : santé, voiture,..

Low-Cost scenario
Sharing to spend less

- **Ubérisation / post-ubérisation**
- **Observation locale**
- **Objets connectés**

Cloud-Computing - Virtualisation - Plates-formes urbaines - Robotisation - Capteurs, WLAN - EaaS - Standards

Shield scenario
Net giants' domination

- **Plates-formes intégrées véhicules / services pour la sécurité**
- **Observation locale**
- **Objets connectés**

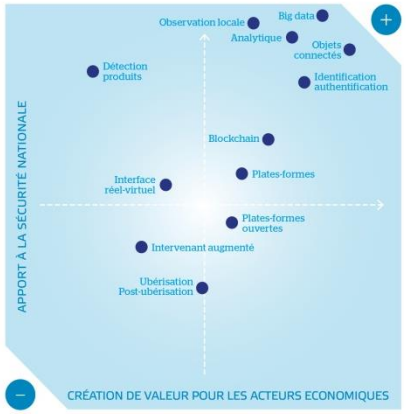
Hardware - Infrastructures sécurisées (5G, IT) - IoT industriel - Privacy - Règlementation

INTENSITY OF PERSONNAL DATA USAGE (+)
OPENNESS OF TECHNOLOGY & DATA (+) (−)
INTENSITY OF PERSONNAL DATA USAGE (−)

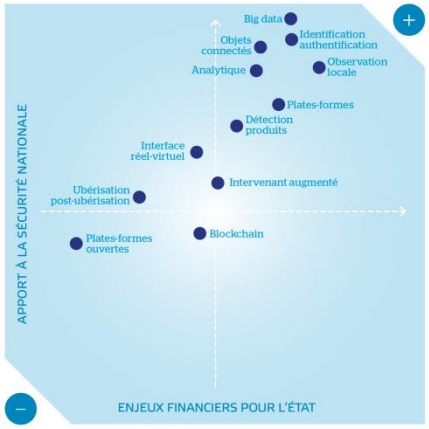
Source : DigiWorld Yearbook de l'IDATE

ACCEPTATION SOCIÉTALE

EFFICACITÉ DE LA FILIÈRE



RETOUR SUR INVESTISSEMENT



IDENTIFICATION TECHNOLOGIES CRITIQUES : RUPTURE

- 6 technologies critiques spécifiques aux domaines identifiés
- 2 technologies critiques génériques

Domaine	Technologies spécifiques	Hardware de Confiance	Intelligence Artificielle
Plates-formes	Gestion distante Véhicule, UAV, Robots	Secure Elements	Aide à la conduite en situation urgence Détection de menaces temps réel
Intervenant Augmenté		Capteurs sécurisés ULP, Electronique souple, Batteries, Actuateurs	Assistants vocaux, bots ..
Identité	Identité numérique forte	HW Tokens, Secure Elements	Identification contextuelle Enrôlement à distance
Détection , contrefaçon		Circuits de séquençage ADN /SIP à base CMOS	Algorithmes de reconnaissance avec apprentissage. ADN et vie privée
Observation Globale		Composants intelligents pour la fusion/filtrage de données hétérogènes	Reconnaissance de patterns en local Apprentissage local
Interface réel/virtuel		Accélération HW des algorithmes	Algorithmes bio-inspirés
Blockchain	Performance transactionnelle	Intégration Blockchain/HSM HW wallets	Coordination de systèmes d'IA, gestion de systèmes de réputation
Internet des objets	Sécurité des infrastructures 5G et IoT	« Secure element » et «Racines de Confiances » SW (TEE, Hyperviseurs)	Détection APT, signaux faibles, menaces en cyber-sécurité
Big-Data	Architectures de processing et stockage	Architectures de processing et stockage	Bases de données partagées
Analytics	Bases de données d'apprentissage.	Chips neuromorphiques Calcul quantique	Réseaux neuronaux multicouches Algorithmes éthiques. Adversarial ML
Ubérisation/post Uberisation		Secure element amovible	Composition de services à partir de données de grande variabilité
Plates-formes ouvertes		Design Open HW certifiés	Outillage sécuritaire orienté IA