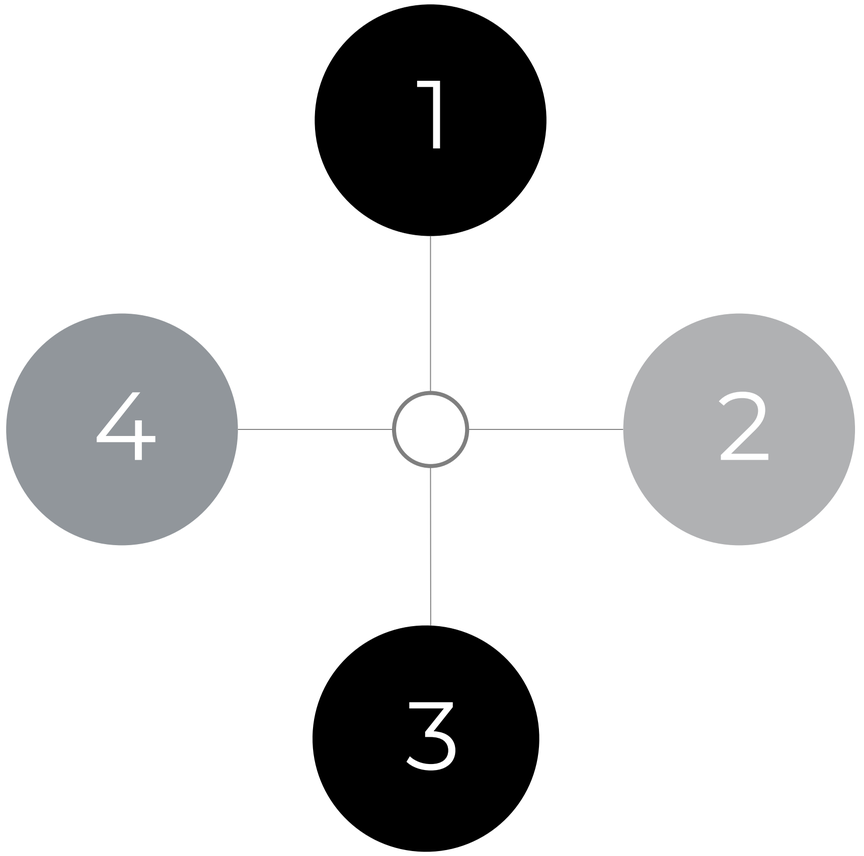
0 0 0 1 0
2600
0 0 1 1 1

Ecole de cybersécurité

ÉCOSYSTÈME PUBLIC ET PRIVÉ & MÉTIERS ET CARRIÈRES

LES QUATRES PILIERS DE CYBERSECURITÉ

QUATRE POINTS CARDINAUX QUI DOIVENT ÊTRE AU COEUR DE LA MISSION DU CYBERDÉFENSEUR



DISPONIBILITÉ

ASSURER LE BON FONCTIONNEMENT DES SYSTÈMES D'INFORMATION (SI)

CONFIDENTIALITÉ

PROTÉGER L'INFORMATION POUR EMPÊCHER SA DIVULGATION

INTÉGRITÉ

PROTÉGER L'INFORMATION POUR EMPÊCHE SA MODIFICATION

PREUVE

GARANTIR LA NON-RÉPUDIATION

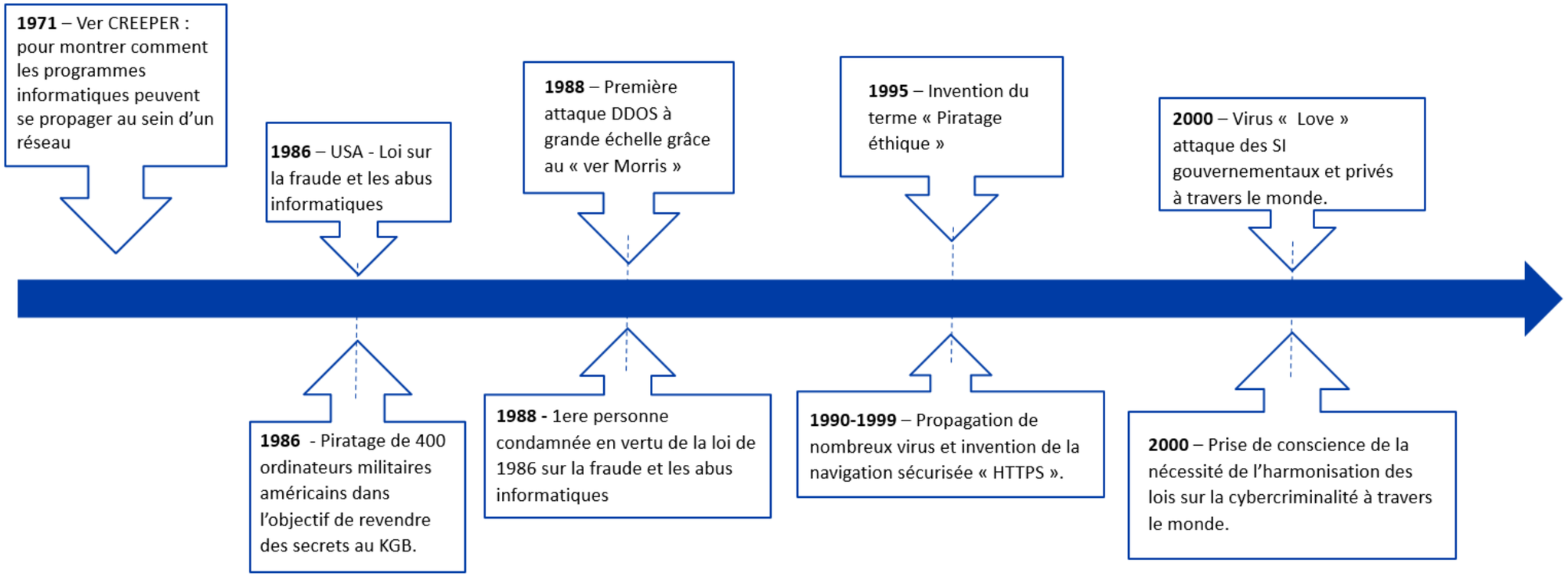
1

ÉCOLE 2600

GENÈSE DES MENACES ET AMPLEUR DU PHÉNOMÈNE

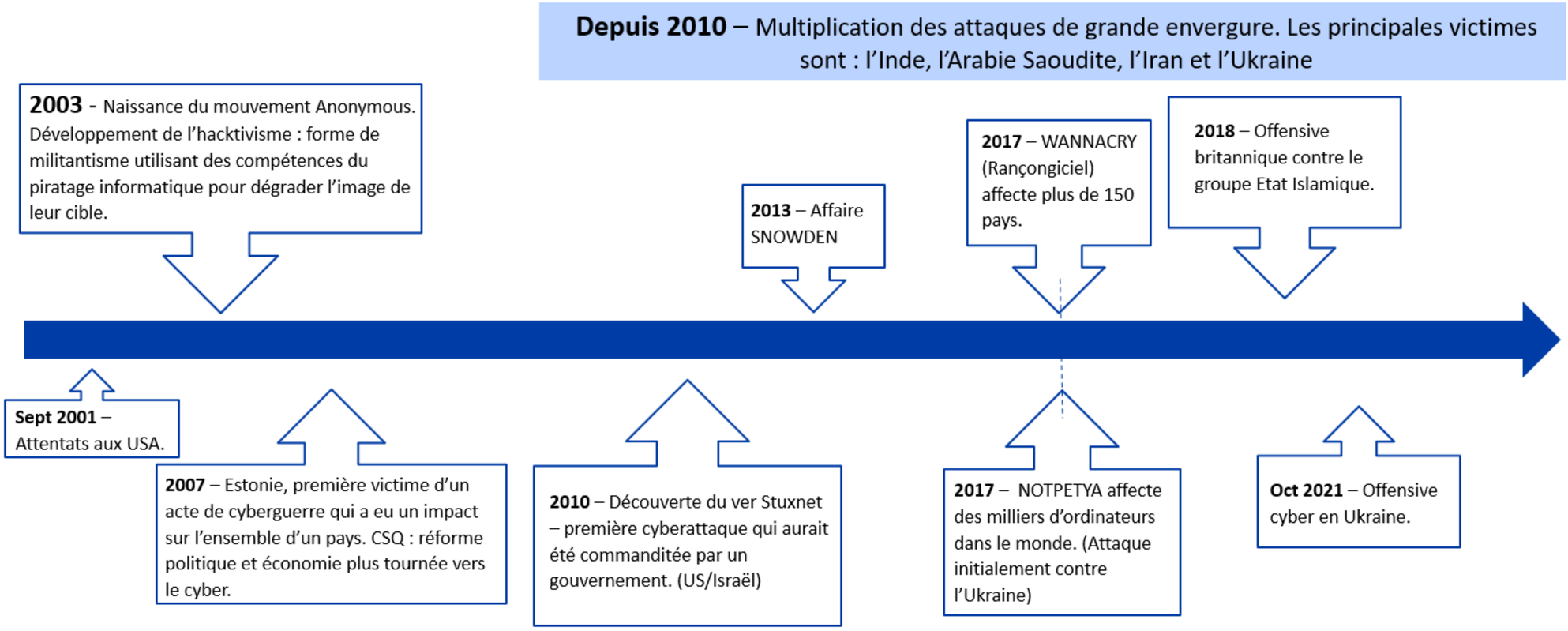
HISTORIQUE DE LA MENACE

LA CYBER, OU INFOSEC, N'EST PAS UNE CONSIDERATION RÉCENTE. DU CODE CÉSAR À LA NUMÉRISATION DES ÉCHANGES, LES PREMIÈRES ATTAQUES DATENT DE LA PRÉSIDENCE POMPIDOU



HISTORIQUE DE LA MENACE

DEPUIS LE DÉBUT 2000, DÉVELOPPEMENT DE L'HACKTIVISME ET DES ATTAQUES ÉTATISTES.



MIEUX QU'UN PLAN ÉPAGNE LOGEMENT

LA CYBERCRIMINALITÉ EST JUSQU'À 5 FOIS PLUS RENTABLE QUE LES CRIMES TRANSNATIONAUX MONDIAUX COMBINÉS

COÛTS

1 – Constitution de l'infrastructure d'attaque

/ Hébergement sécurisé
~900 $
/ VPN (anonymat)
~120 $
/ 20 accès piratés à des entreprises
60 000 $

2 – Intrusion dans les systèmes et propagation

/ Ressources humaines* et outils de propagation (type Cobalt Strike)

3 – Gestion de l'attaque

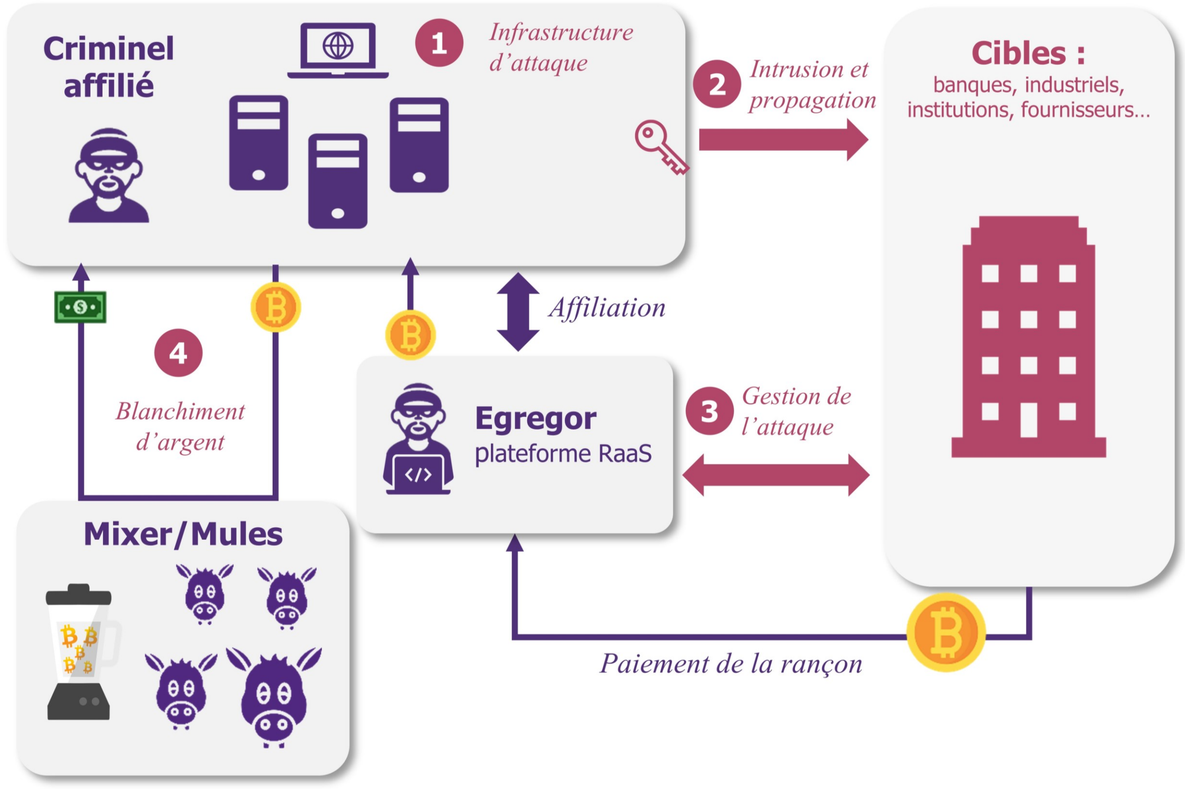
/ Ressources humaines* et commission pour le RaaS
30 % des gains

4 – Blanchiment d'argent

/ Anonymat des Bitcoins
0.5 % des gains
/ Blanchiment et conversion en monnaie réelle
50 % des gains

***Ressources humaines**
3 x 3 mois (500 $/j)
90 000 $

Coût total
151 020 $



GAINS

Cibles piratées
20

Rançons demandées entre
1.5 M$ et 2.5 M$

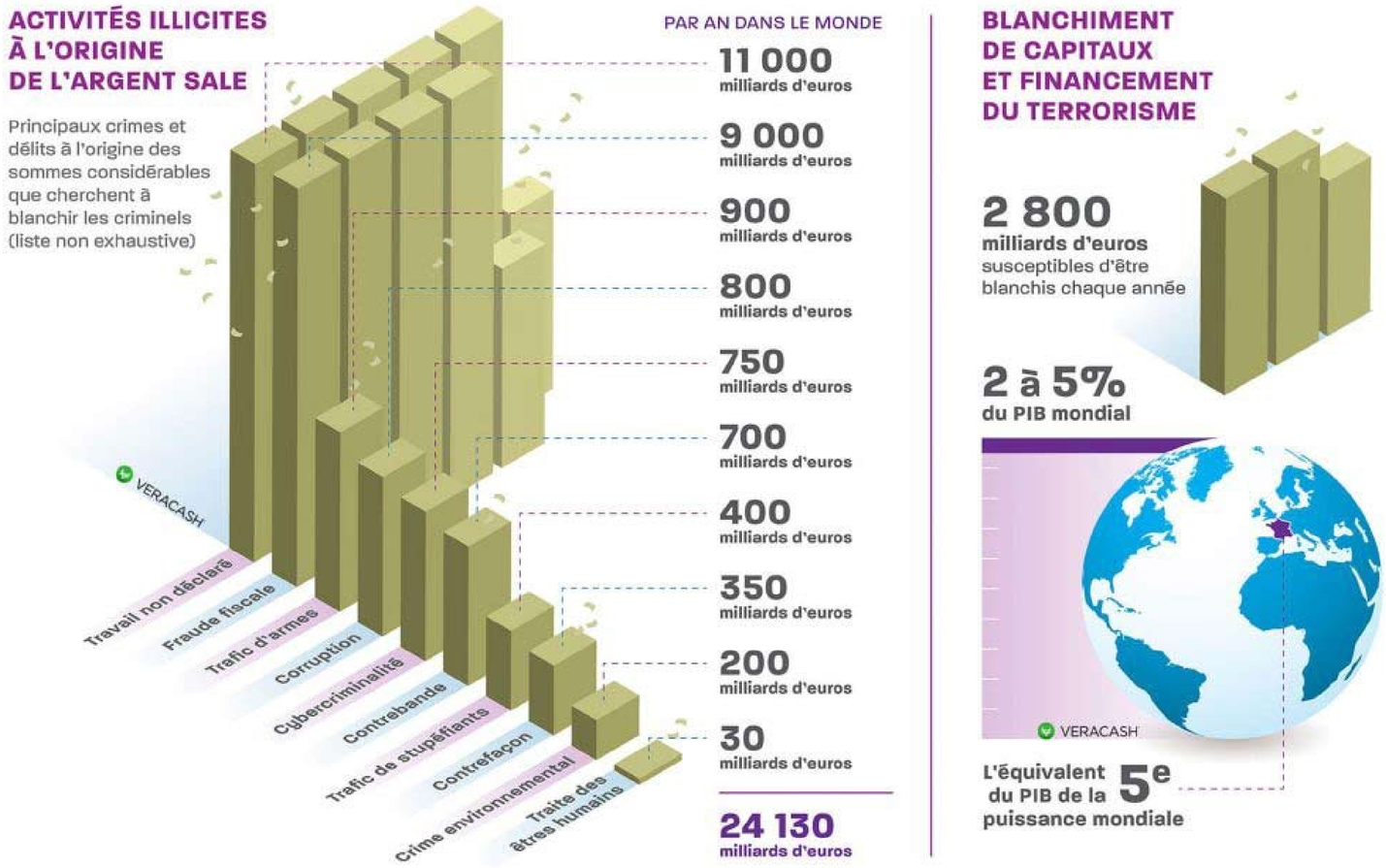
% des acteurs payant la rançon
entre **6** et **10 %**

Montant rançon négocié entre
- 15 % à **- 20 %**

Gain total brut entre
1.4 M$** et **4.3 M$
(avant paiement plateforme RaaS et blanchiment)

Gain net (après blanchiment) : entre 500 k$ et 1.5 M$ | **ROI : entre 232 % et 880 %**

C.A. DU CRIME CYBER > C.A. DE LA DROGUE



2

ÉCOLE 2600

LES ATTAQUANTS ET LEURS MOTIVATIONS

LES ATTAQUANTS

GROUPES CRIMINELS, DESTABILISATIONS ÉTATIQUES, GUERRE ÉCONOMIQUE, ACTIVISTES, GUERRE CYBER, ADOS EN MANQUE DE FRISSONS...

ÉTATS

Alliés, neutres, adverses, belliqueux (NSA unité TAO, GRU unité 26165/74455, 3ème département de l'armée chinoise unité 61398, SEA)

GROUPES

Mafias, APTxxx, Lapsus$

HACKTIVISTES

International Submersives, cDc, Anon, The Realm, etc

INDIVIDUS

Excellent vecteur d'entrée ("insider")

LEURS OBJECTIFS

2 244 164 CYBERATTAQUES PAR JOUR

CYBERCRIMININALITÉ : ESCROQUER, EXTORQUER, FAIRE CHANTER, PRENDRE EN OTAGE, CONTREFAIRE, VOLER, INCITER À LA HAINE, TERRORISME

DÉSTABILISATION : ATTEINDRE L'IMAGE, INSTILLER DE FAUSSES INFORMATIONS, INFLUENCER LA POLITIQUE

ESPIONNAGE : COLLECTER DE L'INFORMATION SENSIBLE

SABOTAGE : PORTER ATTEINTE AU FONCTIONNEMENT DES MATÉRIELS

3

ÉCOLE 2600

LES DÉFENSEURS

LES DÉFENSEURS & LES PROIES

1.082 INTRUSIONS CRITIQUES AU BON FONCTIONNEMENT DU PAYS EN 2021

ÉTAT FRANÇAIS

17 OPÉRATIONS TRÈS SENSIBLES EN 2021 DONT 14 SE SONT AVÉRÉES ÊTRE DE L'ESPIONNAGE ET 9 ÉTAIENT MENÉS PAR DES GROUPES DE HACKERS CHINOIS (ANSSI)

ENTREPRISES

COÛT MÉDIAN D'UNE CYBERATTAQUE POUR UNE ENTREPRISE 50 000€
PERTE DE CA DE 27% ET 60% DES VICTIMES FONT FAILLITE

PERSONNALITÉS

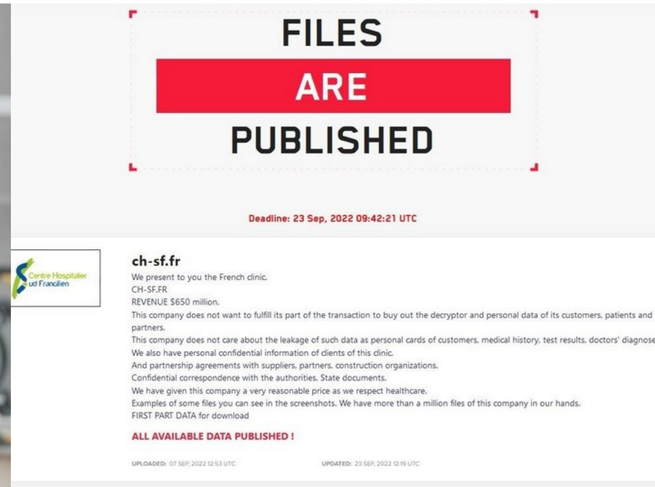
VIP & VAP
CIBLES VIP NON PRÉPARÉES ET MONITORÉES.

CITOYENS

DIFFUSION LE VENDREDI 23 SEPTEMBRE, PAR PLUS DE 11 GO DE CONTENUS SENSIBLES. DU CENTRE HOSPITALIER CORBEIL-ESSONNES

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité



MITRE ATT&CK

EST UN OUTIL D'ANALYSE, DE COMPRÉHENSION, ET DE DÉFENSE, MAIS PAS UN OUTIL D'ATTRIBUTION.

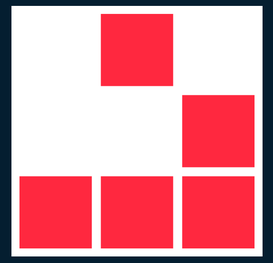
4

ÉCOLE 2600

ECOSYSTÈME PUBLIC

80% des postes en cybersécurité concernent la cyber-défense

Les missions offensives et critiques sont étatiques



LEURS OBJECTIFS

CONTINUITÉ ET INTÉGRITÉ
FOCUS SUR LES OIV ET OSE

Protégez les personnes : Safety first !

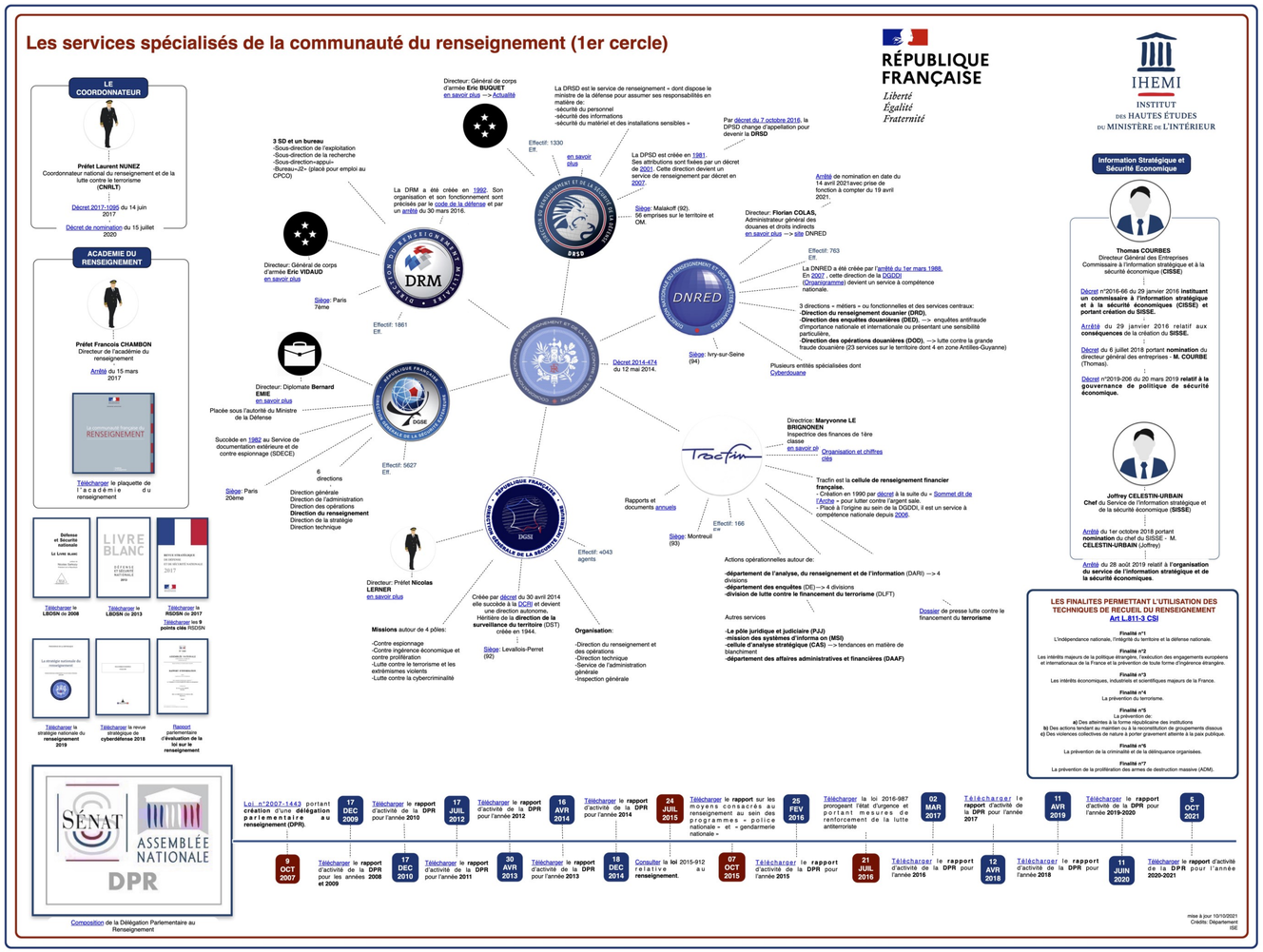
Assurer la continuité de l'activité du SI : souvenez-vous des piliers

Protéger l'information sensible : secrets nationaux, secrets industriels, données personnelles

Stopper la crise au plus vite en sachant réagir grâce notamment à la préparation

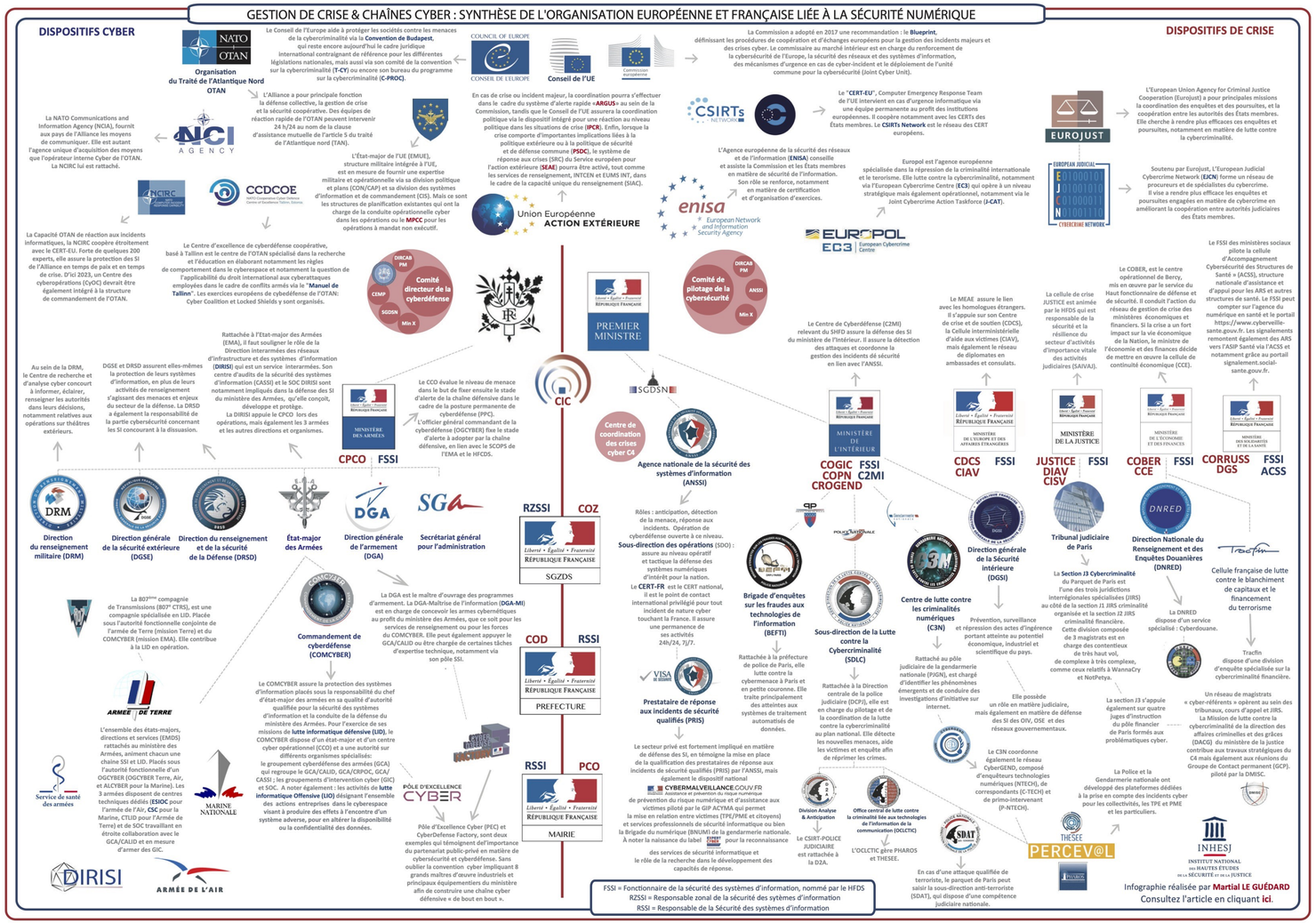
LES DÉFENSEURS

LES SERVICES SPÉCIALISÉS DE LA COMMUNAUTÉ DU RENSEIGNEMENT



LES DÉFENSEURS

GESTION DE CRISE & CHAÎNES CYBER : SYNTHÈSE DE L'ORGANISATION EUROPÉENNE ET FRANÇAISE LIÉE À LA SÉCURITÉ NUMÉRIQUE



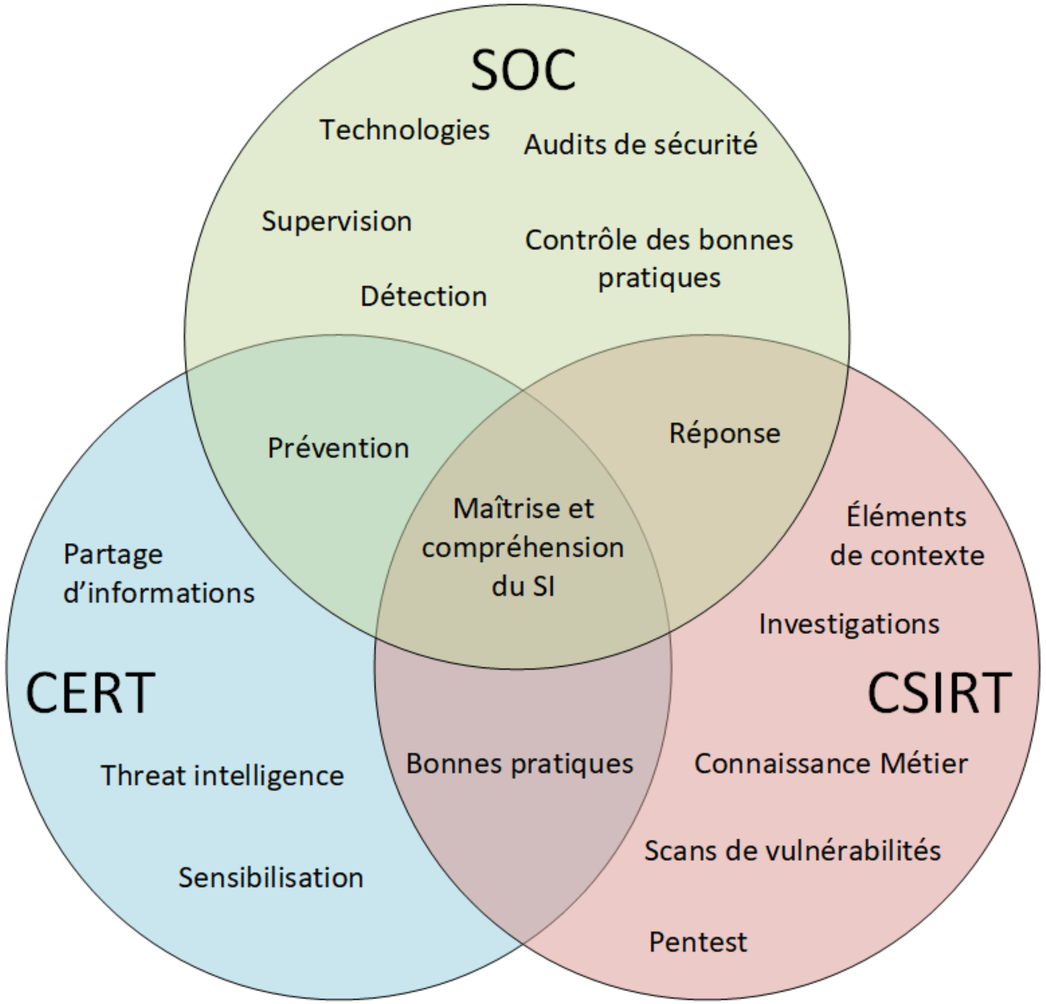
5

ÉCOLE 2600

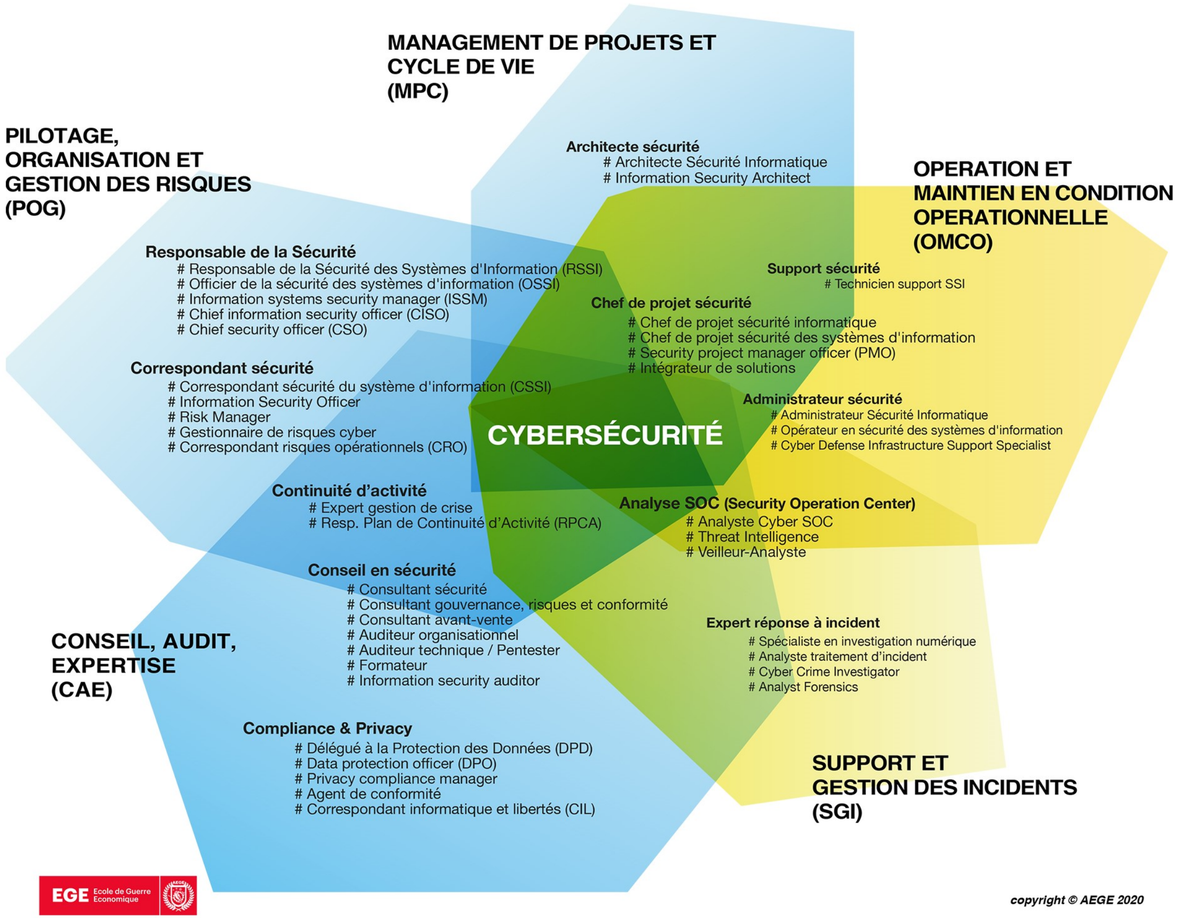
LES MÉTIERS DE LA CYBERSÉCURITÉ

FOCUS SUR LES SOC, CERT & CSIRT

COMPLÉMENTARITÉ DES TROIS COMPOSANTES OPÉRATIONNELLES



SEGMENTATION VUE PAR L'EGE



EGE École de Guerre Économique

MATRICE ANSSI NIVEAU MASTER

Niveau Master ou spécialisé	**COMPETENCES FORMATION**	Technicien support (technique et administratif)	Auditeur, contrôleur, évaluateur	Post-auditeur	Intégrateur	Architecte de sécurité	Développeur de sécurité	Formateur, Instructeur (niveau 3 dans matière enseignée)	Expert (préciser domaine, (Niveau 3 dans le domaine)	Expert en test d'intrusions	Consultant en sécurité	Spécialiste en gestion de crise	Opérateur	Analyste	Expert connexe	Juriste spécialisé en cyberdéfense	Responsable de la sécurité des systèmes d'information (RSSI)
Fondamentaux			3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Electronique et architectures matérielles			1	2	2	2	2	*	*	2	1	1	1	1	1	1	1
Systèmes d'exploitation			2	2	2	2	2	*	*	3	2	2	2	1	1	1	1
Réseaux et protocoles			2	2	2	2	2	*	*	3	2	2	2	1	1	1	1
Cryptologie			1	2	2	2	2	*	*	2	1	1	1	1	1	1	1
Stéganographie et tatouage			1	1	1	1	1	*	*	1	1	1	1	1	1	1	1
Bases de données			1	2	2	2	2	*	*	1	2	1	1	1	1	1	1
Aspects systèmes et systèmes de systèmes			1	2	2	2	2	*	*	2	1	2	2	1	2	1	2
Normes, certifications, guides (organisationnel)			2	2	2	2	2	*	*	1	2	2	1	1	2	2	3
Certifications et évaluations de produits			2	1	2	2	2	*	*	1	1	1	1	1	1	1	2
Politique de cybersécurité et SMSI			3	2	2	2	2	*	*	1	2	3	1	1	2	2	3
Droit et réglementation			2	2	2	2	1	*	*	2	2	2	2	1	2	4	2
Développement logiciel et ingénierie logicielle			2	2	3	2	3	*	*	3	1	1	1	1	1	1	1
Gestion de projet			2	3	3	3	2	*	*	1	2	2	2	1	3	1	2
Cyberdéfense			3	3	2	3	2	*	*	2	2	3	2	2	3	1	3
Analyse post-mortem (Forensic)			1	2	1	1	2	*	*	3	1	1	2	1	1	1	1
Systèmes spécifiques, informatique industrielle			1	1	1	1	1	*	*	1	1	1	1	1	1	1	1
Aspects sociaux et sociétaux			3	3	2	2	1	*	*	3	3	3	2	2	2	2	2
Tests d'intrusion			1	2	2	2	2	*	*	3	1	1	2	1	1	1	1
Sécurité physique			1	2	2	2	1	*	*	1	1	1	1	1	1	2	2
Problématique SSI en contexte spécifique			1	3	1	2	1	*	*	1	2	1	1	1	1	1	1
Rétro ingénierie			0	2	1	1	2	*	*	2	1	1	1	1	1	0	1
Aspects économiques de la sécurité			2	2	2	3	0	*	*	0	2	3	1	3	3	1	3

SPECTRE DES MÉTIERS

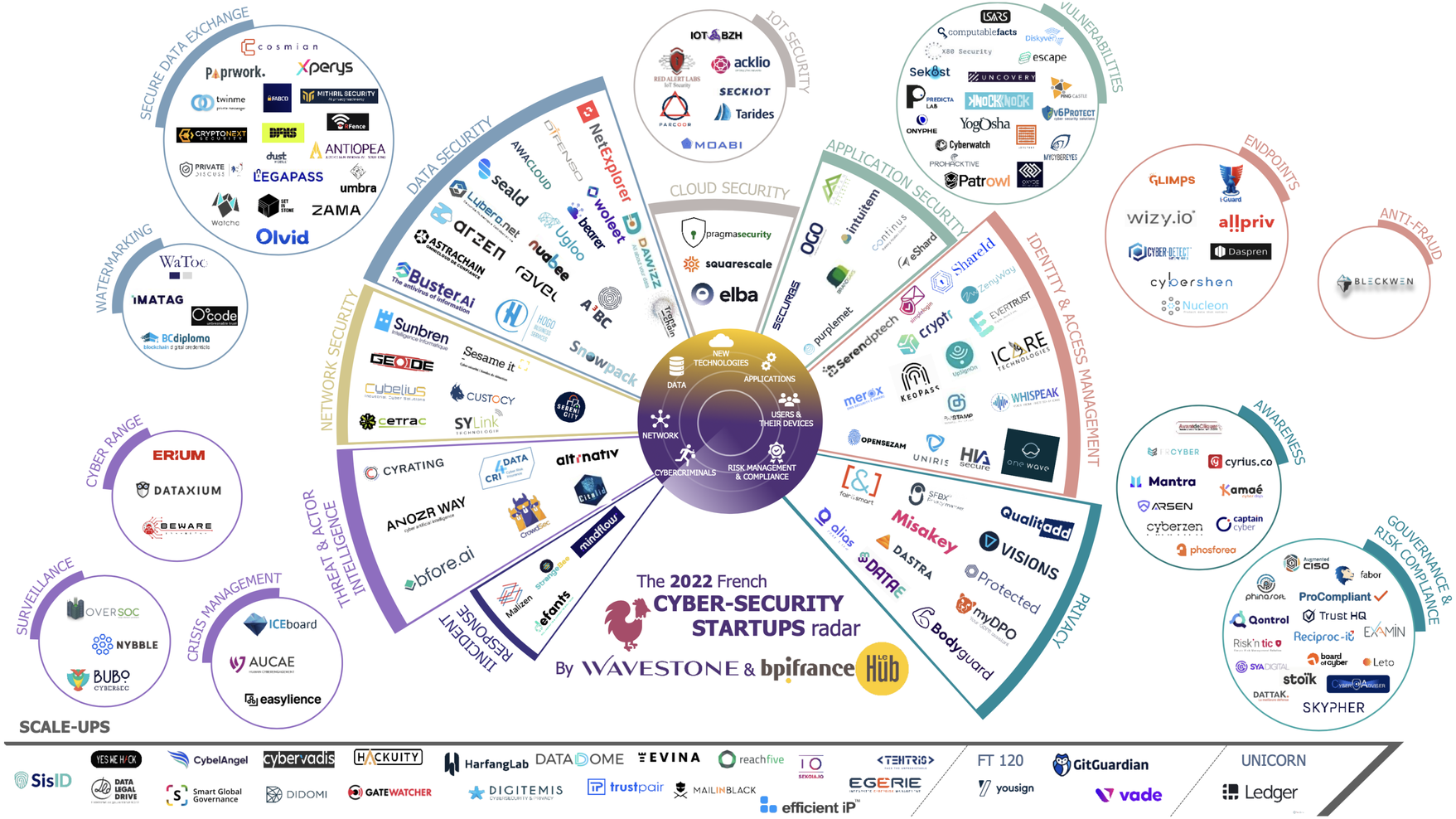
Les métiers de la cybersécurité sont en constante évolution. Certains métiers sont en gestation (ex: cybersécurité de l'IA, de la blockchain) ou sont spécifiques à une industrie

Gestion de la sécurité et pilotage des projets de sécurité	Conception et maintien d'un SI sécurisé	Gestion des incidents et des crises de sécurité	Conseil, services et recherche	Métiers connexes
Directeur Cybersécurité	Chef sécurité de projet	Responsable du SOC	Consultant en cybersécurité	Responsable du plan de continuité d'activité
RSSI	Architecte sécurité	Opérateur analyste SOC	Formateur en cybersécurité .	Délégué à la protection des données
Coordinateur sécurité	Spécialiste sécurité d'un domaine technique	Responsable du CSIRT	Évaluateur de la sécurité des technologies de l'information	Manager de risques
Directeur de programme de sécurité.	Spécialiste en développement sécurisé	Analyste réponse aux incidents de sécurité.	Développeur de solutions de sécurité	Directeur sûreté
Responsable de projet de sécurité .	Cryptologue	Gestionnaire de crise de cybersécurité	Intégrateur de solutions de sécurité	Responsable des assurances
	Administrateur de solutions de sécurité	Analyste de la menace cybersécurité	Chercheur en sécurité des systèmes d'information	Responsable du contrôle interne
	Auditeur de sécurité organisationnelle			Juriste spécialisé en cybersécurité
	Auditeur de sécurité technique			Chargé de communication spécialisé en cybersécurité
				Security service delivery manager

https://www.ssi.gouv.fr/uploads/2021/10/anssi-panorama_metiers_cybersecurite-2020.pdf

RADAR WAVESTONE 2022

LA RICHESSE DES DOMAINES TRAITÉS PAR LES STARTUP FRANÇAISES DANS LE DOMAINE CYBER SONT AUSSI DES RÉVÉLATEURS DES BESOINS MÉTIERS



6

ÉCOLE 2600

CONCLUSION

TOUT EST CYBER.

SCIENCES DE L’INGÉNIEUR, SCIENCES SOCIALES, COMPORTEMENTALES, SÉCURITÉ PHYSIQUE…

NOUS FORMONS DES EXPERTS POUR UN MONDE QUE NOUS NE CONNAISSONS PAS.

ÉCOLE 2600

MERCI !

Axel Dreyfus
axel@ecole2600.com
+33 6 67 00 42 42

00010
2600
00111

Ecole de cybersécurité