CAMPUS CYBER

HORIZON CYBER 2030

PERSPECTIVES ET DÉFIS

PRÉFACE

Le Campus Cyber est un vaisseau amiral qui, tout en connaissant son cap, a besoin de tracer des trajectoires agiles et mobilisatrices. Cet exercice de prospective s'inscrit dans un horizon proche : il dessine une carte des itinéraires probables ou possibles de la cybersécurité. L'écosystème, fort de sa diversité de points de vue, s'est mobilisé depuis des mois pour produire ce commun, le premier du Campus Cyber.

Si les conclusions de cette synthèse ne constituent pas une stratégie d'action, elles soulignent un nombre de défis et d'actions qui peuvent constituer des axes d'attention pour les travaux à mener collectivement au sein du Campus Cyber. Si l'importance des enjeux à venir peut donner le vertige, ce premier accomplissement est la preuve de la capacité de l'écosystème à se mobiliser et produire collectivement. J'espère que cette première production du Campus Cyber suscitera votre intérêt, tout comme celles qui suivront.

Michel Van Den Berghe,
Président du Campus Cyber

LE MOT DES COORDINATEURS

Nous avons eu, avec le support des équipes d'AXA, de Wavestone et du Campus Cyber, le plaisir de coordonner les actions aboutissant à ce document, qui, nous l'espérons, contribue au rôle sociétal de prévenir le risque cyber.

Ces travaux ont été extrêmement enrichissants grâce à l'expertise et aux connaissances partagées par les personnes que nous avons rencontrées et par les entités participantes aux ateliers de travail. L'écosystème cyber est riche et sachant : nous les remercions vivement pour leurs actions.

Les travaux de prospective sont périlleux de par leur nature. Ils imposent des choix et des orientations, mais l'exercice est en même temps libérateur et passionnant ! Il est évident que nous restons humbles par rapport à nos prévisions. Le futur sera forcément différent, mais nos scénarios ou les défis identifiés sont volontairement larges pour permettre de s'adapter aux évolutions à venir.

Dans tous les cas, nous espérons que ces travaux vous éclaireront, comme il nous ont éclairé, sur les enjeux à venir !

Arnaud TANGUY, Gérôme BILLOIS

Arnaud TANGUY,
Directeur
de la Sécurité
du Groupe AXA

Gérôme BILLOIS,
Partner cybersécurité,
Wavestone

SOMMAIRE

ANTICIPER LE FUTUR : UN EXERCICE TOUJOURS PERILLEUX MAIS NÉCESSAIRE

Le premier exercice de prospective du Campus Cyber a mobilisé des profils très variés pour favoriser une vision presque palpable sur notre avenir proche de la cybersécurité, à 5 voire 10 ans. D'autres travaux complètent cette vision et en particulier ceux de la Red Team Defense du Ministère des Armées et de l'université PSL.

Notre objectif : dessiner un futur proche, en identifiant les priorités et les futurs défis de notre secteur et en extrapolant les tendances observées aujourd'hui. L'exercice, forcément périlleux, a nécessité de faire de nombreux choix.

Plusieurs dizaines de priorités et plusieurs centaines d'actions ont été collectées, démontrant le bénéfice des synergies entre les acteurs de l'écosystème cyber. Nous avons d'abord réalisé que les priorités d'aujourd'hui seront aussi celles de demain : les fondamentaux de la cybersécurité ne seront pas forcément remis en cause dans les années à venir. En revanche, leurs déclinaisons en solutions concrètes posent un véritable défi si on considère la multiplicité des chemins possibles et la complexité des changements à opérer pour résoudre les problèmes majeurs identifiés.

Nous avons fait le choix de ne sélectionner que les défis qui nous semblaient les plus complexes à résoudre et qui nécessitaient la coopération de nombreux acteurs, un principe au cœur même du projet du Campus Cyber.

Ces choix ont été arrêtés au travers d'un parcours d'ateliers collaboratifs, impliquant plus de 60 entités publiques et privées.

Ce document n'a ni vocation à rapporter avec exhaustivité et complétude le contenu des échanges ayant pris place, ni à apporter une vision définitive de ce qui nous attend dans les années à venir.

Il en présente une synthèse volontairement courte et donc frustrante, des futurs envisageables ainsi que des priorités et défis associés. L'exercice aura certainement vocation à se poursuivre et à s'améliorer avec le temps. Cependant, nous esperons qu'il inspira les futurs travaux du Campus Cyber.

Nous adressons nos remerciements aux 51 entités contributrices qui ont accepté de participer aux différents ateliers malgré le contexte sanitaire et dans un format quasi intégralement digitalisé.

L'organisation des ateliers et la production de ce document n'auraient pas été possibles sans l'engagement des membres et particulièrement d'AXA, de Wavestone et du Campus Cyber, coordinateurs du Groupe de travail dédié.

MÉTHODOLOGIE

QUELS SONT LES GRANDS DÉTERMINANTS DU FUTUR À 10 ANS ?

Interview avec des prospectivistes et exploration des facteurs majeurs qui influencent le futur (e.g., géopolitique, environnement, société, travail, vie privée, économie)

QUELLES SONT LES OPPORTUNITÉS D'ATTAQUE, ET LES SOLUTIONS POUR SE DÉFENDRE ?

Trois ateliers de travail avec plus de 60 participants issus de 4 collèges du Campus (fournisseurs, recherche, institutions et bénéficiaires), pour regrouper les points de vue, les sujets d'inquiétude et les solutions existantes ou à inventer pour se protéger.

QUELLES SONT LES PRIORITÉS ?

Un atelier croisé regroupant l'ensemble des 4 collèges du Campus pour prioriser ensemble les solutions proposées.

RAPPORT DE SYNTHÈSE

Rapport d'analyse et de synthèse afin de résumer les principales tendances à anticiper dans le futur à 10 ans, ainsi que les priorités pour se protéger dans ces futurs possibles.

CHAPITRE 01

4 FUTURS ENVISAGÉS

À QUOI RESSEMBLERA 2030 ?

Pour anticiper les menaces cyber à 10 ans, il est avant tout nécessaire de se projeter dans le futur. Lors des ateliers et sur la base des interviews de prospectivistes, les participants ont tenté l'exercice périlleux de proposer des futurs possibles à horizon 2030. De l'analyse des points de vue récoltés ressortent quatre tendances principales.

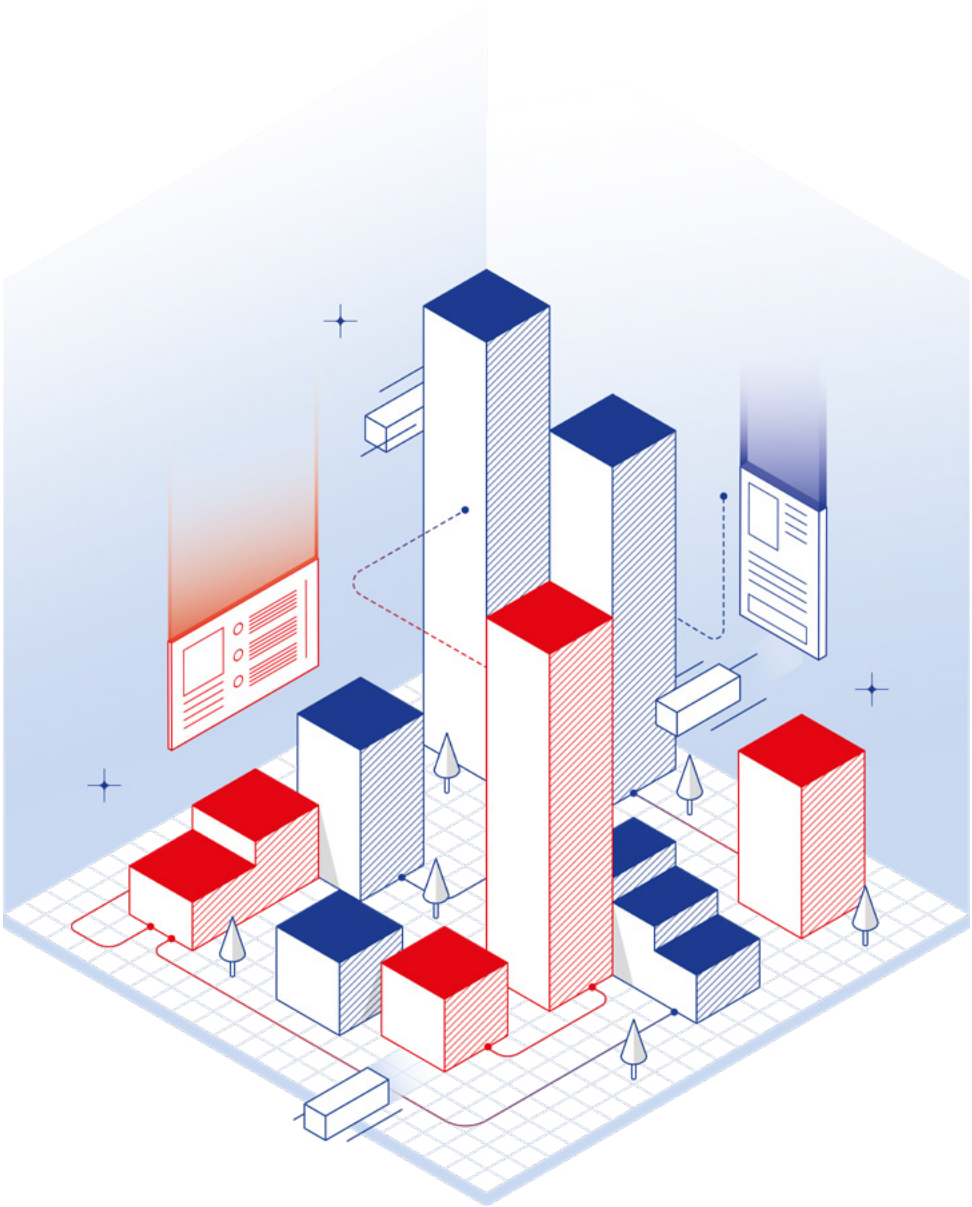
- **l'ultra-connectivité,** liée à l'accélération des échanges de données et de leur vitesse ;
- **l'ultra-cloisonnement,** lié à l'exacerbation des souverainetés, en raison de la méfiance géopolitique et des craintes face aux dépendances entre écosystèmes numériques ;
- **l'ultra-green,** lié au renforcement des idéologies environnementales et de sobriété numérique face au changement climatique ;
- **l'ultra-réglementation,** liée au durcissement réglementaire dans un objectif de restauration de la confiance numérique.

Chacune de ces tendances, extrapolée à l'extrême, donne lieu à un scenario. Nous espérons ainsi proposer une grille de lecture de l'avenir, ayant vocation à permettre à nos lecteurs d'apprécier les impacts de ces tendances sur la société, les individus et les organisations.

SCÉNARIO 1
UNE SOCIÉTÉ ULTRA-CONNECTÉE.

↗ **En 2025, les grands acteurs du numérique, poussés par les consommateurs et les États, ont travaillé ensemble et se sont mis d'accord sur des standards d'interopérabilité. Cet évènement a grandement accéléré le développement du numérique en rendant plus simple et plus fluide son utilisation au quotidien d'ici à 2030.**

En parallèle, les mondes numériques ont continué leur forte croissance et des économies parallèles s'y sont créées. Une large partie de la population oscille entre vie réelle et vie virtuelle dans un ou plusieurs univers numériques ou métaverses.



ÉTAT DE FAIT

- Les sphères économiques et politiques se transforment pour s'adapter à cette nouvelle configuration de la société. La chaîne d'approvisionnement (supply-chain) est davantage automatisée, notamment grâce aux robots de livraison et aux technologies de paiement automatisé.

  Dans de nombreux cas, les citoyens ne font pas confiance aux mécanismes de protection des données. Ils créent des faux jumeaux numériques ou déclarent de fausses informations personnelles. Il devient de plus en plus difficile de fiabiliser les données. Les monnaies électroniques et les achats de biens numériques se démocratisent (en particulier via les technologies NFT). Les villes, les transports, les lieux publics, les habitations sont dotés de capteurs pour proposer de nouveaux services (e.g., smart cities, smart home, smart mobility, smart health, smart education). Le numérique permet une croissance de la productivité des entreprises (e.g., automatisation, anticipation des départs d'employés grâce à l'intelligence artificielle)

  Les pratiques citoyennes (e.g., démarches administratives et votes) évoluent vers plus d'inclusivité et de simplicité grâce aux progrès technologiques et à l'interconnectivité des services.

CONSÉQUENCES

- La disparition des frontières entre vie personnelle, vie professionnelle, vie numérique et vie réelle est concrétisée.

  L'identité numérique permet de retracer les actions des personnes, de leurs objets (e.g., smart home, smart city, smart building) et l'utilisation des services associés. Le principe d'anonymat sur internet s'effrite et les utilisations commerciales des données personnelles collectées explosent. La méfiance citoyenne et le recourt à des stratégies de contournement augmente rapidement.

  Deux acteurs principaux (Chine & États-Unis) se partagent le monopole des technologies, des équipements et des matériaux servants à leur fabrication, utilisés pour des formes d'interdépendances étatiques (e.g., données stratégiques stockées dans des serveurs étrangers) pouvant mener à des tensions géopolitiques.

LES OPPORTUNITÉS POUR LES CYBERATTAQUANTS

↗ L'ultra-connectivité des personnes et des systèmes offrent aux cyberattaquants un éventail de cibles et d'accès sans précédent (e.g., vol d'informations sensibles, contrôle des objets domestiques ou professionnels, détournement de la chaine d'approvisionnement).

Ils bénéficient de la rapidité des technologies et de leur homogénéité pour étendre rapidement et largement leurs attaques.

L'essor de la plateformisation (usage de plateformes digitales ou de réseaux sociaux pour la diffusion de contenu et service) supporte le développement économique des filières criminelles qui utilisent ces plateformes pour vendre leurs compétences et s'organiser.

Pour maximiser l'impact des attaques, les organisations cybercriminelles s'internationalisent (plus de « clients » et de cibles, recherche du « plus offrant »). Elles diversifient et industrialisent leurs méthodes de recrutement pour atteindre les meilleurs talents.

LES ATTAQUES SONT PLUS MASSIVES

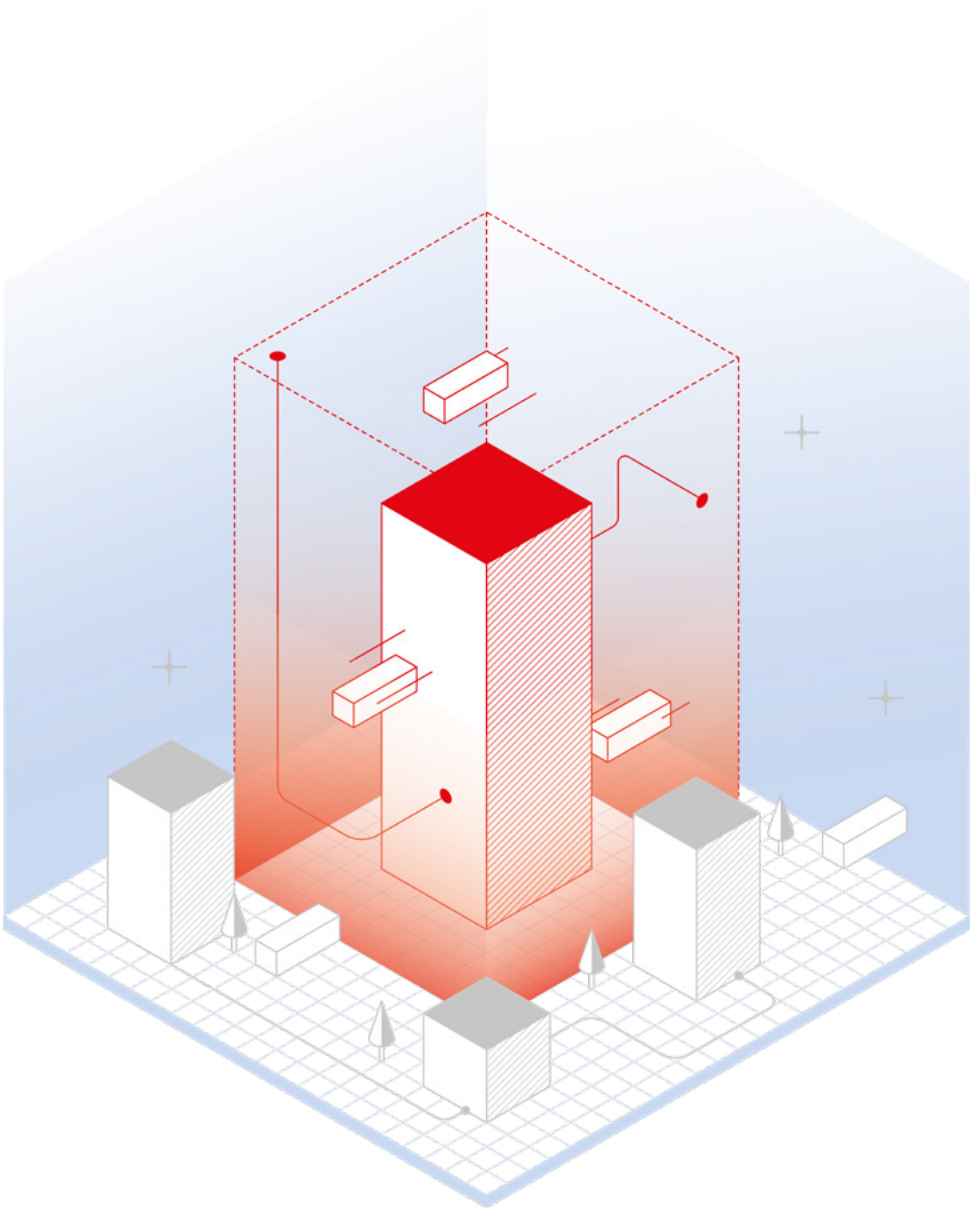
- Piégeage d'applications grand public visant un arrêt des services ou une fuite de données ;
- Piégeage à grande échelle des chaînes d'approvisionnement physiques (e.g., perturbation des usines, des magasins…) ;
- Utilisation large des systèmes numériques à des fins criminelles (e.g., réseaux de robot pour lancer des attaques) ;
- Instantanéité de propagation de logiciels malveillants (e.g., type NotPetya), instrumentalisée dans le cadre d'attaque sur les services essentiels ;
- Création de faux frais et de services numériques peu onéreux pour piéger les victimes (e.g., faux services de protection, faux accès premium à des services gratuits) ;
- Diffusion de fausses informations (fake news) dans tous les secteurs (par exemple sur la finance en impactant plus facilement les cours de bourse en raison de la forte automatisation).

SCÉNARIO 2
UNE SOCIÉTÉ ULTRA-CLOISONNÉE

↗ **En 2025, la révélation de pratiques scandaleuses, dont les piratages, les vols et les recroisements de données réalisés par des gouvernements avec le support de sociétés privées sonnent le glas de la confiance numérique : c'est la datastrophe. Les populations se révoltent et manifestent pour une remise sous contrôle de l'utilisation du numérique.**

En regard, les États réagissent par la création de frontières numériques, leur fermeture immédiate et la nationalisation des chaines d'approvisionnement stratégiques. La période est marquée par le cloisonnement d'Internet et une forte isolation technologique.

La priorité est donnée aux solutions souveraines (processeurs, cloud, crypto assets…) pour assurer la défense nationale.



ÉTAT DE FAIT

La réaffirmation des souverainetés fait resurgir des conflits directs et accentue les pratiques d'espionnage entre États. La cyber et le numérique deviennent des postes majeurs d'investissement budgétaire.

La scène géopolitique est marquée par de nouveaux clivages et alliances entre pays souverains : le bilatéralisme domine sur les initiatives internationales, les institutions perdent en contrôle et en envergure (e.g., ONU, OTAN, UE, OMC, etc.). En l'occurrence, l'Union Européenne se fragmente.

CONSÉQUENCES

L'identité numérique est largement imposée, puisqu'elle permet aux États le suivi et la traçabilité des personnes, des objets et des services qu'elles utilisent. Surveillés, les individus ne peuvent plus échanger de l'information librement et de manière anonyme.

La fermeture des frontières numériques permet davantage de filtrage et engendre la multiplication des plateformes et sites nationaux (e.g. l'utilisation de réseaux sociaux non nationaux est interdite).
Les entreprises internationales vivent un grand bouleversement dans la gestion de leurs opérations et sont contraintes de dé-globaliser en cloisonnant leurs systèmes d'information (e.g., flux réseaux, localisation des données), leurs ressources et leurs expertises dans chaque zone souveraine. L'expansion vers de nouvelles zones est extrêmement difficile et restreinte.

Les cabinets experts en tests d'intrusion, R&D cyber et recherche de vulnérabilité sont nationalisés et leurs activités catégorisées au même niveau de confidentialité que celles du contre-espionnage.

Certaines zones incluent dans leur corpus réglementaire lié à la souveraineté numérique des nouvelles sanctions pénales en cas d'utilisation d'outil permettant le chiffrement, l'anonymisation, etc. Ces règles renforcent le pouvoir de surveillance numérique des États.

Les différentes zones géographiques se livrent une guerre sur la formation, l'acquisition et la rétention des talents et des technologies numériques.

LES OPPORTUNITÉS POUR LES CYBERATTAQUANTS

↗ La multiplication des plateformes souveraines donne lieu à une recrudescence des groupes d'attaquants spécialisés sur certaines cibles.

Les journaux informent régulièrement sur les cyberguerres et les cyberaffrontements en cours. Les infrastructures critiques sont évidements les plus visées.

Le maintien d'un marché international de vulnérabilités favorise l'essor économique d'organisations cybercriminelles. Ces dernières détiennent l'expertise et les ressources nécessaires pour les exploiter de manière extrêmement rapide et efficace.

Le cloisonnement régional des écosystèmes simplifie la détection des cibles pour les attaquants, mais réduit le risque de dégâts collatéraux chez des tiers alliés.

La proximité entre États et cybercriminels permet aux groupes d'être dotés de meilleures capacités offensives, tout en bénéficiant d'impunité et de protection dans leur propre espace souverain.

LES ATTAQUES SONT PLUS PERNICIEUSES, DESTRUCTIVES ET DÉSTABILISANTES

- Attaques mixant les volets informationnel, cognitif et cyber ;
- Attaques sur les services critiques nationaux dans un objectif de déstabilisation. Les « attentats » numériques voient le jour ;
- Multiplication des attaques sur les chaînes d'approvisionnement (e.g., piégeage des logiciels, piégeage des composants), en particulier lorsqu'acquis en dehors de la zone souveraine ;
- Renforcement des attaques par rançongiciel menées par des États dans un objectif de gain financier et de déstabilisation ;
- Renforcement d'attaques complexes avec rebond (e.g., attaque d'espionnage suivie d'une attaque par rançongiciel visant à effacer les traces de l'attaque précédente et à désorganiser) ;

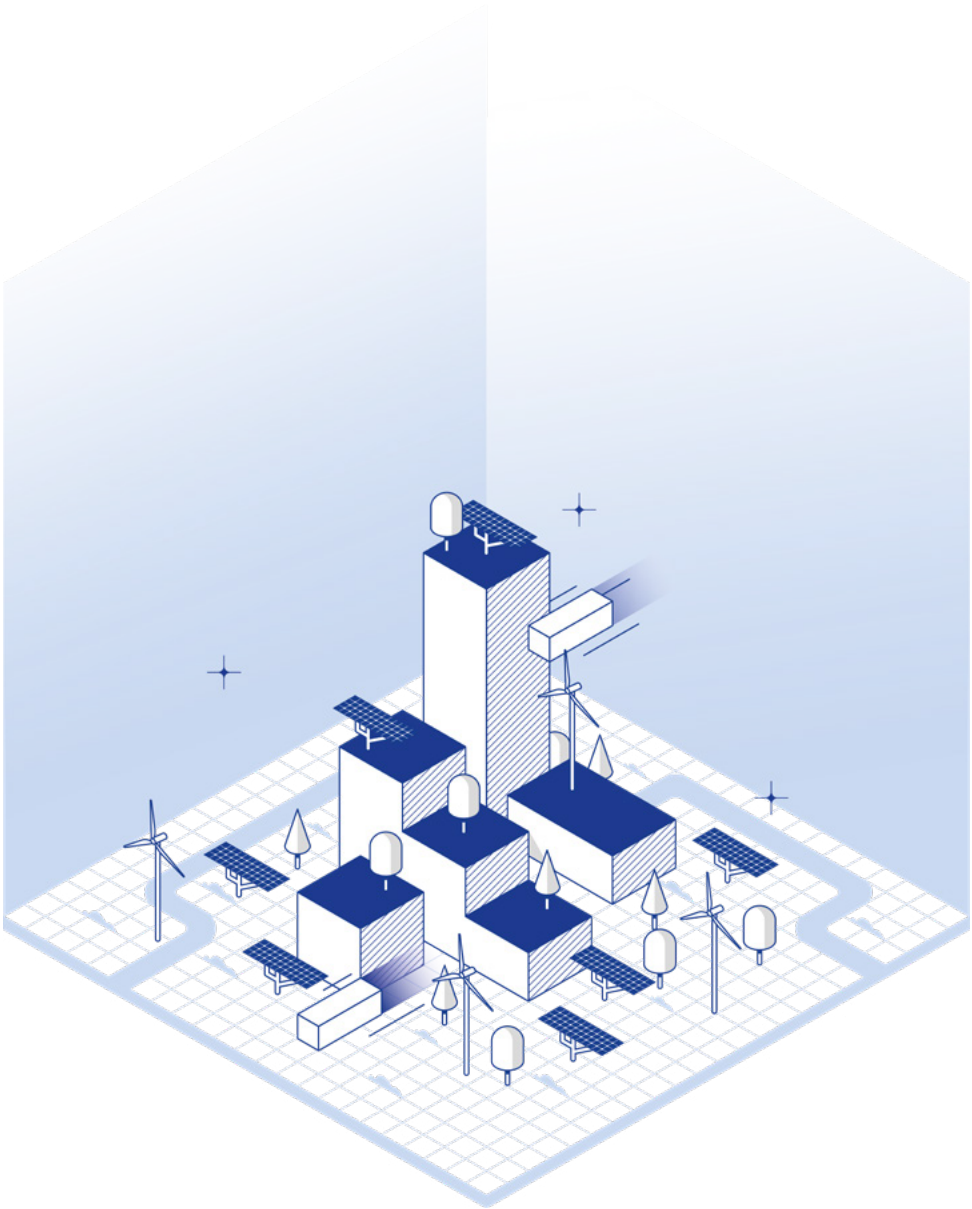
- Renforcement de l’espionnage numérique : multiplication d’acteurs sous-traitants qui vendent des services d’espionnage haut de gamme aux États à des fins géopolitiques. ;
- Renforcement du hack back, des capacités militaires de défense et des attaques sous « faux drapeau » ;
- Destruction physique de certains câbles sous-marins ou de satellites et attaques sur les chaînes d’approvisionnement critiques (terres rares…).

SCÉNARIO 3
UNE SOCIÉTÉ ULTRA-GREEN

↗ **En 2025, le monde subit de plus en plus de catastrophes naturelles et sanitaires, ce qui entraîne des vagues migratoires sans précédent.**

Le grand public fait pression sur les institutions gouvernementales et les grands groupes pour prioriser leurs réponses aux enjeux environnementaux.

Le numérique est au cœur des discussions : ses avancées sont décriées en raison des conséquences qu'elles peuvent avoir sur l'environnement.



ÉTAT DE FAIT

L'accès aux services numériques est conditionné par les ressources énergétiques disponibles, exacerbant les tensions sociales et diplomatiques entre les différents pays.

Les pays les moins engagés dans la transition écologique sont attaqués par des groupes cybergreen. Il en va de même pour les organisations considérées comme polluantes et gaspilleuses d'énergie. Des campagnes de piratages visent même les utilisateurs de monnaies électroniques ou de jeux en ligne.

L'exacerbation des idéologies extrêmes donnent lieu à des affrontements numériques et physiques entre les personnes en faveur et celles opposées aux politiques environnementales misent en place.

Une nouvelle catégorie sociale des « non-connectés » émerge : ces derniers refusent les pratiques numériques pour éviter d'accroitre leur impact carbone, mais aussi pour protéger leur vie privée.

CONSÉQUENCES

Les citoyens militent pour des économies d'énergie, y compris dans le numérique. Des services sont contraints à la fermeture ou à des transformations en profondeur de leur mode de fonctionnement. Les organisations subissent des coûts importants pour acter leur transformation.

Les avancées technologiques priorisent la diminution de leur impact sur le changement climatique, qui devient un différenciateur entre solutions concurrentes.

Des quotas de pollution individuels, y compris pour l'utilisation des technologies (e.g., nombre de courriels, quantité de données stockées) sont mis en place, avec un suivi personnel des consommations par les autorités.

LES OPPORTUNITÉS POUR LES CYBERATTAQUANTS

↗ Les cyberattaquants tirent profit de l'environnement conflictuel entre groupes d'acteurs idéologiques en monétisant leur services pour la réalisation d'actes d'hacktivisme parfois violents et très déstabilisateurs.

Ces hacktivistes visent les systèmes qui seraient trop énergivores (monnaie numérique & cryptoactif, data centers…) et les détruisent en faisant la promotion des messages pour l'avènement de la sobriété numérique. Les idéologies extrêmes, partagées largement, encouragent le développement transnational des groupes d'attaquants.

En parallèle, les attaques cybercriminelles se multiplient grâce à l'exploitation de mécanismes mis en place pour un numérique plus sobre (e.g., vols, manipulations, arnaques et/ou revente de quota…).

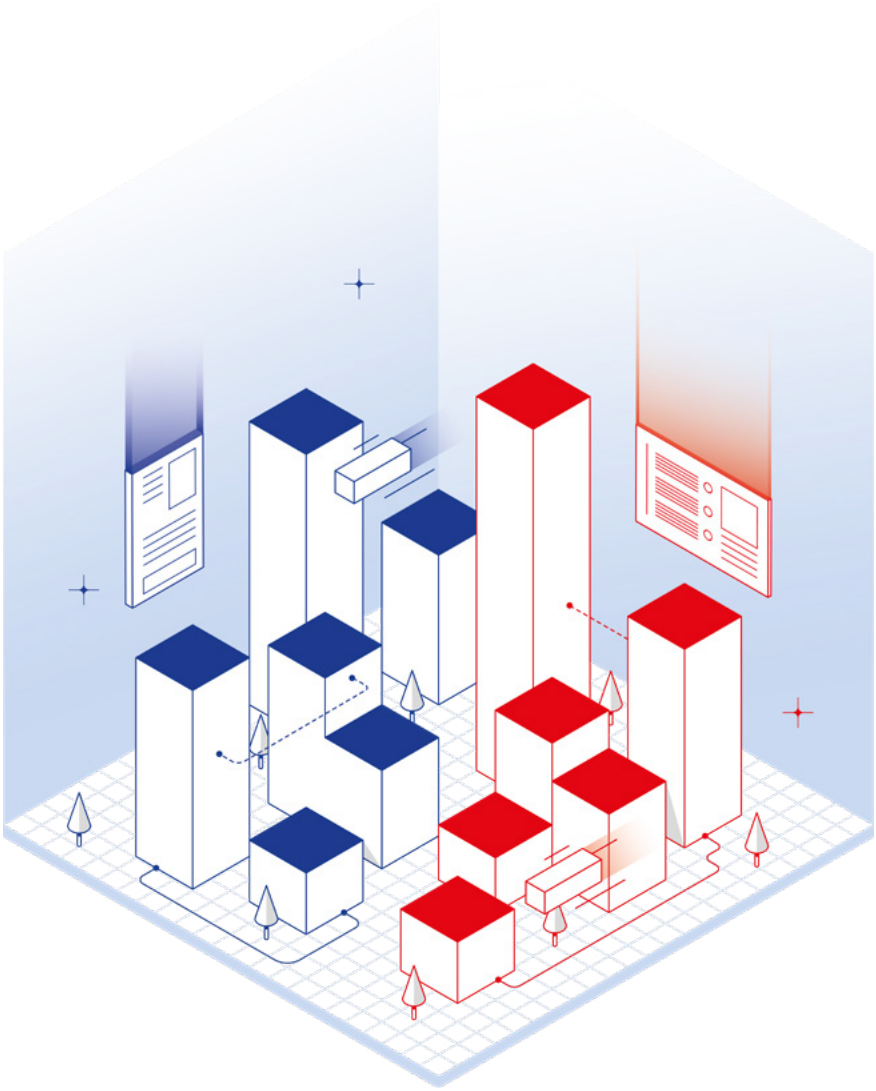
LES ATTAQUES SONT PLUS VISIBLES, CHOQUANTES ET DESTRUCTRICES :

- Attaques contre la réputation des personnes morales et physiques ;
- Renforcement de l'hacktivisme – ou activisme numérique ;
- Destruction des systèmes numériques trop énergivores ;
- Attaques contre les chaines d'approvisionnement non « locales » ;
- Instrumentalisation des idéologies environnementales au profit des cyberattaques (e.g., rançongiciel, extorsion, etc.).

SCÉNARIO 4
UNE SOCIÉTÉ ULTRA-RÉGLEMENTÉE

↗ **En 2025, les attaques et scandales d'utilisation de données à caractère personnel continuent de se multiplier et rompent la confiance dans le numérique.**

Le grand public réclame plus de transparence, de contrôle et d'autonomie sur la gestion de ses données. Les gouvernements réagissent afin de préserver le développement économique lié à la transformation digitale.



ÉTAT DE FAIT

Les réglementations se multiplient et les différentes autorités renforcent leurs capacités de contrôle.

Deux philosophies s'affrontent : celle en faveur d'une monétisation des données contrôlées par l'utilisateur et celle percevant ces dernières comme un « bien commun » à protéger. Chaque grande zone de puissance met en place ses propres réglementations donnant plus ou moins de contrôle et d'obligations aux utilisateurs et offreurs de services numériques.

Dans les zones où le citoyen détient ses données personnelles la possibilité de contrôler et de valoriser leurs « traces numériques » (ex : adresse IP ou avatar numérique dans le métaverse), certains éprouvent des difficultés à gérer de façon adaptée leurs données sensibles et à en garder le contrôle.

Dans les autres zones, le modèle « bien commun » protège les individus contre la collecte insidieuse de données personnelles par des acteurs privés. Bien qu'il soit considéré comme un frein au développement de l'économie numérique, ce modèle est majoritairement défendu par la population.

CONSÉQUENCES

La prolifération des organes de régulations et des agences étatiques sur le numérique dans tous les pays entraîne une absence de clarté sur les règles à respecter, les zones d'influence et responsabilités de chacun. Les régulations restent sujettes à interprétation, notamment en Europe où de nouvelles directives sont créées mais implémentées de façon hétérogène.

Le modèle économique de grands acteurs numériques est mis à mal dans plusieurs zones géographiques. Certains services ferment, d'autres basculent vers des modèles payants. De nouvelles logiques de valorisation des données émergent. Elles sont sujettes à de nombreux débats éthiques et technologiques.

Seuls de grands groupes internationaux parviennent encore à se mettre en conformité face aux nombreuses régulations, même si la plupart ne parviennent pas à adapter leur processus de conformité sur toutes les géographies et subissent des amendes ou des fermetures de service.

Les solutions technologiques de contrôle et de traçabilité des données se déploient massivement. Mais face au manque de confiance vis-à-vis du respect de la vie privée (e.g., centralisation des données, connaissance de la localisation des données), certains acteurs plébiscitent la traçabilité « manuelle et humaine» des utilisateurs.

En parallèle, le darkweb, la blockchain et les métaverses décentralisés proposent une échappatoire à cette société ultra-réglementée, mais sans d'autres garanties que la confiance dans ceux qui les font fonctionner.

LES OPPORTUNITÉS POUR LES CYBERATTAQUANTS

Les cyberattaquants profitent de la multiplicité des régulations pour entreprendre du cyberchantage. Ils menacent de dénoncer leurs victimes aux régulateurs pour non-conformité, ou proposent de faux services de régularisation.

Ces pratiques d'extorsion sont redoutablement efficaces : le nombre de victimes et le gain des cyberattaques s'envolent, favorisant le développement économique des filières criminelles.

Les investissements humains et financiers portant sur la sécurité sont délaissés au profit de ceux œuvrant uniquement à la mise en conformité réglementaire aux nouvelles exigences, dans une logique parfois idéologique et sans prise en compte des risques réels. La sécurité globale en est d'autant fragilisée : les attaquants profitent de ce contexte pour multiplier les zones d'impact en toute impunité et les entreprises ont du mal à s'extirper de ce cercle vicieux.

LES ATTAQUES SONT PLUS FACILES, CIBLÉES ET DISCRÈTES :

- ↗ Explosion du taux de réussite des cyberextorsions ;
- ↗ Augmentation du nombre d'attaques des cybercriminels non professionnels et sans connaissance technique ;
- ↗ Montée des attaques basées sur l'imitation des autorités régulatrices et sur les fausses amendes. ;
- ↗ Chute des déclarations d'incidents cybers par les victimes à des fins de discrétion vis-à-vis des régulateurs ;
- ↗ Accroissement des pratiques d'échange d'information sur les victimes dans les réseaux cybercriminels ;
- ↗ Développement d'un « monde parallèle » qui tente d'échapper aux régulations.

CONCLUSION

Il est évident que l'avenir de notre société à 10 ans ne sera pas exactement semblable à l'un des scenarios identifiés, mais il sera probablement une combinaison plus ou moins forte des quatre.

Prises individuellement, les tendances identifiées permettent de mettre en lumière les grands enjeux du numérique et de mieux apprécier les futures menaces. Chaque lecteur est invité à appliquer cette grille de lecture sur son environnement afin d'identifier et d'anticiper les conséquences que ces futurs pourraient avoir sur les organisations politiques, publiques, privées, les instituts de recherche, ou simplement sur les aspirations des individus et des citoyens dans la société. Dans la suite de ce document, le groupe de travail a identifié de manière transverse les priorités et les défis majeurs pour sécuriser le monde de 2030. Ces scénarios ont permis d'identifier des grands défis auxquels les organisations doivent se préparer.

CHAPITRE 02

5 PRIORITÉS POUR L'AVENIR DE LA CYBER

PRIORITÉS, DÉFIS ET INVARIANTS

Les scénarios et propositions construits pendant les ateliers ont permis d'identifier cinq priorités.

Ces défis complexes - aussi bien organisationnels que technologiques - nécessitent la mobilisation de nombreux acteurs. Ils pourront être intégrés au cœur des travaux menés par le Campus Cyber.

Si la synthèse qui suit n'a pas vocation à être exhaustive, ni dans son analyse de l'état des lieux, ni dans ses propositions, elle souligne les éléments fondamentaux qui ont émergé lors des ateliers.

- **Insérer par défaut la sécurité dans tous les systèmes numériques ;**
- **Redonner le contrôle à chacun sur sa vie numérique et ses données ;**
- **Permettre la résilience à grande échelle grâce à l'automatisation et l'IA ;**
- **Combattre l'impunité des cybercriminels ;**
- **Développer l'attractivité de la filière.**

DES INVARIANTS À INTÉGRER DANS L'ENSEMBLE DES TRAVAUX

↗ **Dans le cadre de nos réflexions, trois invariants ont été identifiés.** Il est indispensable de les prendre en compte pour répondre aux différents défis afin d'assurer le succès et la crédibilité des solutions à mettre en place, mais aussi la définition d'une filière responsable.

LA COOPÉRATION

- La coopération, entre tous les acteurs privés (académique, recherche, forces de l'ordre, justice…) est nécessaire pour répondre à l'ensemble des enjeux.

L'ÉCHELLE EUROPÉENNE

- L'échelle européenne : le niveau européen doit être inscrit dans toutes les orientations et décisions, pour favoriser l'émergence d'une cybersécurité paneuropéenne.

SOBRIÉTÉ NUMÉRIQUE

- En 2022, la réalité climatique impose à tous les secteurs d'intégrer dans leurs évolutions les paramètres du développement durable. Le numérique et la cyber sont particulièrement consommateurs en énergie, à la fois lors de la conception des systèmes, de leur utilisation au quotidien et de leur décommissionnement. Les principes de sobriété doivent s'inscrire dans leur modèle de développement.

RÉINVENTER LES FONDAMENTAUX DE LA CYBERSÉCURITÉ

VERS UNE CYBERSÉCURITÉ PLUS DURABLE

↗ Nos travaux ont permis d'identifier en particulier trois sous-ensembles pour lesquels les acteurs pourraient minimiser l'utilisation des ressources et de l'énergie.

LA CRYPTOGRAPHIE

- Son usage est pervasif et extrêmement fréquent. De ce fait, même des gains mineurs de consommation d'énergie dans nos activités quotidiennes peuvent avoir un effet déterminant à grande échelle. Des travaux de recherche émergent, certains allant même jusqu'à positionner la sobriété comme un futur facteur de choix dans la normalisation algorithmique.

LA SAUVEGARDE

- Sont concernés en particulier les phénomènes de duplication des données et d'infobésité. Les mécanismes et techniques de sobriété en la matière existent, mais doivent passer à l'échelle en s'intégrant dans les pratiques organisationnelles au quotidien. Nous pouvons citer par exemple la capacité à dédupliquer les données entre différents acteurs ou à détruire les informations non-structurées (e.g., campagne d'effacement des données non nécessaires, règles de suppression automatisée, etc..).

LA BLOCKCHAIN ET LES CRYPTOACTIFS

- La blockchain et les cryptoactifs prennent une place de plus en plus importante, mais l'énergie requise au fonctionnement des cryptoactifs peut être optimisée. Les travaux de recherche en cours en matière de sobriété doivent être appuyés.

MISE EN COHÉRENCE AVEC LA STRATÉGIE NATIONALE D'ACCÉLERATION CYBER

↗ Les solutions suivantes s'inscrivent dans la stratégie d'accélération cyber.

ENJEU DE CONFIANCE :

C

Les utilisateurs doivent pouvoir bénéficier des possibilités offertes par le numérique sans craindre pour la sécurité de leurs données, pour la disponibilité des services dont ils dépendent ou encore pour leur intégrité physique.

ENJEU ÉCONOMIQUE :

E

La compétitivité des entreprises repose de plus en plus sur leur maitrise des outils numériques. Ainsi, la capacité à se protéger face aux attaques informatiques représente un enjeu vital tant pour garantir leur croissance, que pour conserver la confiance de leurs clients. Par ailleurs, la filière de cyber-sécurité est un secteur au potentiel économique important et pourvoyeur d'emplois.

ENJEU DE SOUVERAINETÉ FRANÇAISE :

S

La France doit préserver son autonomie d'action et disposer de compétences scientifiques, techniques et opérationnelles, mais également de capacités industrielles propres pour faire face aux défis du futur.

Dans la suite du document, chaque solution présentée est marquée du ou des macarons de l'enjeu auquel elle répond.

PRIORITÉ

INSÉRER PAR DÉFAUT LA SÉCURITÉ DANS TOUS LES SYSTÈMES NUMÉRIQUES

LA SÉCURITÉ DES PRODUITS ET DES SERVICES, UNE OPPORTUNITÉ MAJEURE

↗ Le sujet de l'insertion par défaut de la sécurité dans les systèmes numériques n'est pas nouveau, mais présente aujourd'hui un niveau d'avancement trop faible. Les concepts de la sécurisation par défaut sont encore mal compris, répandus et intégrés. L'enjeu est d'assurer une sécurité intégrée dans les produits et services numériques aussi bien pour le grand public que pour les organisations publiques ou privées.

Pour que les industriels intègrent la sécurité dès la conception, il est important qu'elle devienne un facteur de choix lors des achats de solutions numériques. Ainsi, le niveau de sécurité devrait être affiché et mesurable de manière transparente et simple. Plusieurs initiatives sont en cours, dont le projet de notation de sécurité des sites internet, voté en novembre 2021 par l'Assemblée Nationale. Cependant, les critères restent difficiles à maintenir et à évaluer dans le temps, et se limitent aux sites web.

Il est nécessaire d'élargir ce type de mesures, ceci impliquant la création de mécanismes d'évaluation faciles et rapides, applicables plus largement et fréquemment. À terme, il faudrait pouvoir évaluer toute la chaine de construction d'un produit ou d'un logiciel dans son ensemble (composants tiers, hébergements…). Aujourd'hui, l'évaluation de la sécurité des produits est complexe, longue, majoritairement manuelle, et donc coûteuse. Les chaines d'approvisionnement sont difficiles à saisir, avec parfois jusqu'à plusieurs milliers de modules pour un système numérique, tous de provenance diverse.

Si plusieurs mécanismes de scoring, de qualification et d'évaluation existent, ils présentent soit des difficultés de passage à l'échelle (facilité, rapidité), soit des problèmes de qualité et de profondeur.

DÉFI MAJEUR À RELEVER

C E S

Construire des méthodes et des outils d'évaluation faciles, fiables et automatisables du niveau de sécurité des solutions, des produits, des composants et des organisations (tiers, fournisseurs, clients…) pour permettre le passage à l'échelle des évaluations de cybersécurité.

PREMIÈRES ACTIONS DU CAMPUS CYBER.

Soutenir la création d'un standard d'évaluation d'un [cyberscore] et son déploiement.

+ **Mener un benchmark des solutions d'évaluation existantes, des produits, des organisations, de leur forces et faiblesses ;**

+ **Identifier et porter des projets de recherche à soutenir sur le thème de la sécurité des produits et des organisations.**

PRIORITÉ

REDONNER LE CONTRÔLE À CHACUN SUR SA VIE NUMÉRIQUE ET SES DONNÉES

UN BESOIN FORT DE CONTRÔLE ET DE MAITRISE DES DONNÉES

↗ La multiplication des attaques et des scandales entraîne aujourd'hui les premiers mouvements de défiance envers le numérique. Comment faire confiance lorsqu'on confie ses données ? Comment bien s'assurer que notre volonté sera respectée ? Comment utiliser des services numériques clés (étatiques, santé…) nécessitant de vérifier notre identité tout en conservant une part de vie privée lors d'usages moins cruciaux ? Ces questions prennent de plus en plus de place dans l'opinion.

Chacun se heurte au quotidien aux difficultés de gestion de multiples identités en ligne et des moyens d'authentification associés. S'ajoutent à ce constat, les difficultés des fournisseurs de services pour implémenter des fonctions de sécurité associées simples et fiables (en matière par exemple d'authentification ou de protection des données par le chiffrement).

Dans les sociétés ultra-connectées, cloisonnées et régulées où les citoyens étendent leur identité dans le numérique jusqu'à un stade extrême avec les métaverses, apporter des solutions à ces problèmes (identité, authentification, sécurité des données, respect de la vie privée…) sera crucial.

Aujourd'hui, même si les réglementations se multiplient et vont dans la bonne direction, leur apport doit être démultiplié pour éviter les évènements impactant négativement et définitivement la confiance citoyenne (e.g. datastrophe du scénario n°2) tout en restant réaliste et actionnable par les acteurs du numérique.

DÉFI MAJEUR À RELEVER :

C

→ **Maitrise de l'identité, à l'aide d'un programme d'identité numérique fiable, interopérable et partagé largement.**
Il est indispensable pour être capable de prouver son identité et utiliser les services numériques les plus avancés de manière simple, (dé)centralisée et dans certains cas anonymement. Les innovations technologiques liées à la blockchain et les technologies associées (Web3) peuvent présenter des opportunités.

→ **Maitrise des données, à l'aide de dispositifs et de mesures pour redonner le contrôle à chacun de ses données.**
Aujourd'hui, ces plateformes, les privacy center, existent, mais pas dans une version centralisée (e.g. à l'aide d'API). Cette dernière permettrait de redonner de la visibilité et le contrôle des données et des identités numériques aux citoyens : accès centralisé à la localisation des données partagées, activation de ses droits à récupérer ou effacer les données… Cela implique une bonne gestion des données par les fournisseurs.

→ **Protéger plus efficacement, en simplifiant et en élargissant le champ d'action du chiffrement.**
Certaines avancées sur le sujet sont un succès (e.g. chiffrement par défaut sur les ordinateurs et téléphones), mais les innovations doivent être poursuivies pour rendre ces mécanismes plus simples et les adapter aux nouveaux usages technologiques. Après avoir travaillé sur le chiffrement des données en transit et lors du stockage, il est temps d'accélérer sur le chiffrement pendant l'utilisation. Des travaux de recherche sont déjà engagés, par exemple sur le chiffrement homomorphique, qui permet de traiter des données en les laissant chiffrées, les rendant inaccessibles pour les fournisseurs et offreurs de services.

PREMIÈRES ACTIONS DU CAMPUS CYBER.

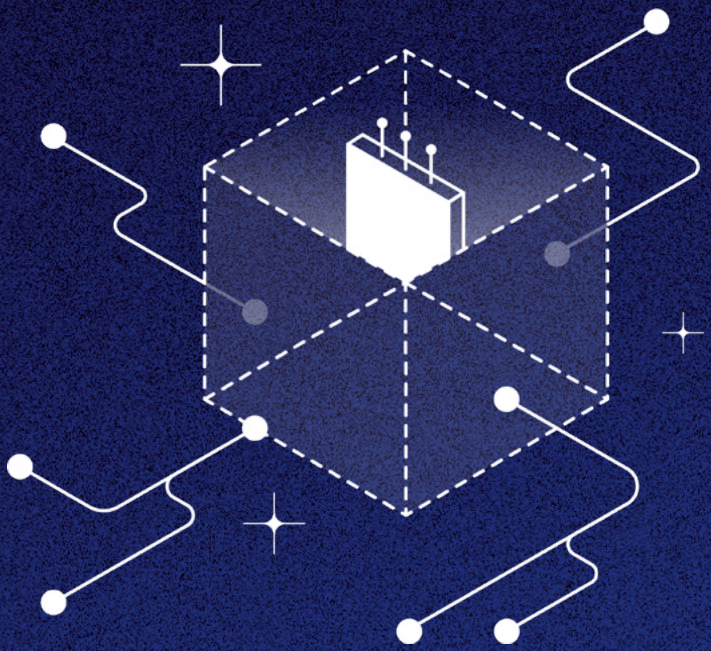
Contribuer à la construction de la confiance numérique de bout en bout.

+ **Étudier l'émergence d'un modèle centralisé de gestion de la vie privée numérique (e.g. privacy center) ;**

+ **Lancer un challenge sur le chiffrement homomorphique ;**

+ **Explorer les avantages et les inconvénients de la blockchain pour l'identité numérique.**

PRIORITÉ



PERMETTRE LA RÉSILIENCE À GRANDE ÉCHELLE GRÂCE À L'AUTOMATISATION ET L'IA

UN BESOIN FORT DE CONTRÔLE ET DE MAITRISE DES DONNÉES

↗ Les attaques se multiplient, se complexifient et leurs effets sont de plus en plus rapides. Ces impacts seront plus dévastateurs encore dans une société qui se transforme numériquement et interconnecte de plus en plus de systèmes.

Dans ce contexte, le décalage entre la rapidité d'action des cybercriminels et les temps de détection est encore trop important. Le renforcement de la solidarité entre les acteurs et la multiplication des ressources humaines ne suffiront pas à réduire l'écart dans la durée.

De nouvelles techniques éprouvées permettent déjà d'automatiser un certain nombre de processus. Nous pouvons citer notamment la détection de certaines attaques, la mise en œuvre de réactions simples ou encore le déploiement de logiciels lors des phases de reconstruction. Ces exemples montrent la voie d'une résilience renforcée basée d'abord sur l'automatisation puis à terme sur l'intelligence artificielle.

Des initiatives sont en cours chez de nombreux fournisseurs, en particulier sur le sujet de la détection de la réaction aux attaques, mais également sur le sujet de la reconstruction de système d'information. Cependant, la solution idéale n'a pas encore été trouvée. Le sujet est complexe et nécessite un travail de recherche important.

DÉFI MAJEUR À RELEVER

E S

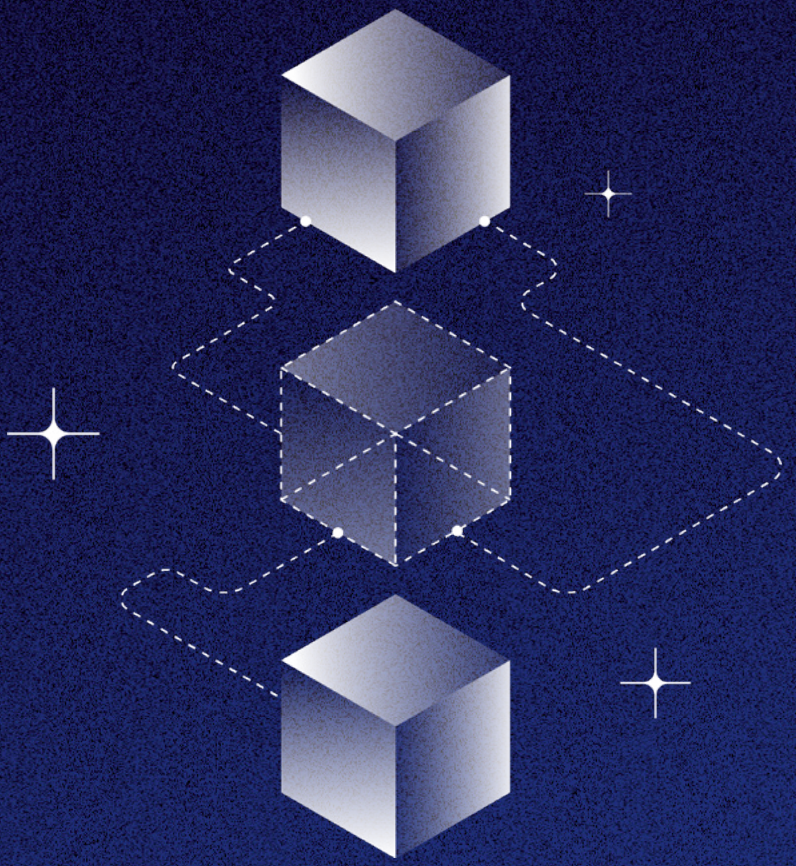
Utiliser efficacement l'intelligence artificielle pour améliorer la détection, accélérer la réaction face aux attaquants et automatiser la reconstruction à grande échelle.

PREMIÈRES ACTIONS DU CAMPUS CYBER.

Faciliter le rapprochement de l'IA et de la cybersécurité.

+ **Développer une plateforme pour expérimenter des usages IA dans la cyber ;**
+ **S'associer et développer les challenges IA de la cyber ;**
+ **Mettre à disposition des jeux de données pour permettre les expérimentations.**

PRIORITÉ



COMBATTRE L'IMPUNITÉ DES CYBERCRIMINELS

DES PROCESSUS D'IMPUTATION LABORIEUX

↗ Malgré la montée en puissance des arrestations de groupes de rançongiciels en 2021, un fort sentiment d'impunité des cybercriminels demeure.

De premiers textes législatifs en la matière ont été votés en France et en Europe, les investigations progressent, mais le problème de l'identification et de l'imputation des attaques à leur auteur reste saillant et complexe.

Aujourd'hui, l'imputation est réalisée par des recherches manuelles extrêmement consommatrices en temps, et a fortiori en argent. Les données sont difficiles à collecter et à partager, car elles sont dispersées, dans des formats variés, et leur collecte se heurte aux complexités de la coopération, en local comme en international, entre les acteurs privés et publics.

DÉFI MAJEUR À RELEVER

E S

Faciliter l'imputation des attaques en utilisant des systèmes d'intelligence artificielle capables de recouper des masses importantes d'information (outils d'attaques, modes opératoires, infrastructures utilisées, traçage sur les réseaux d'anonymisation, transactions financières en monnaie électronique ou non, information en source ouverte…).

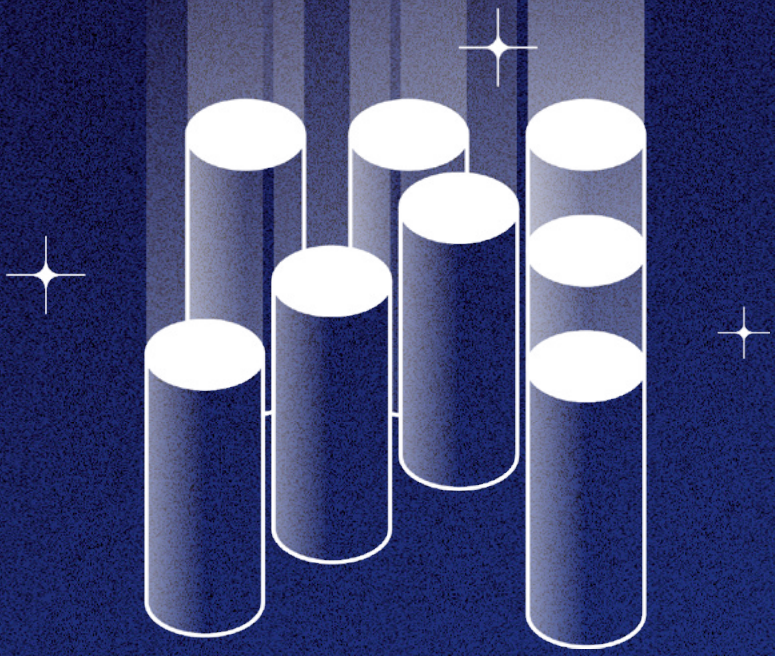
PREMIÈRES ACTIONS DU CAMPUS CYBER.

Faciliter l'émergence et la modélisation d'IA visant à améliorer l'imputation des attaques.

+ **Créer des environnements de simulation d'attaque et des projets de R&D sur l'entraînement d'IA pour imputer des attaques ;**

+ **Créer des projets R&D pour remonter ou suivre les parcours d'argent et automatiser la saisie de cryptoactifs.**

PRIORITÉ



DÉVELOPPER L'ATTRACTIVITÉ DE LA FILIÈRE

LA RESSOURCE HUMAINE AU COEUR DE LA CYBER DE DEMAIN

↗ Au-delà de la sensibilisation de toute la population aux bonnes pratiques, qui doit être poursuivie, la filière éprouve une pénurie de compétences généralisée. Cette dernière est internationale et constitue un problème majeur pour toutes les organisations et leurs fournisseurs.

L'enjeu se situe au niveau de l'attractivité des métiers et de la diversification des profils sur tous les critères, dont celui de la formation académique. La cyber n'est pas que technique et touche à beaucoup de sujets différents : résilience opérationnelle, fraude, risques, gouvernance… Des chemins de carrière de plus en plus divers et intéressants existent.

Malgré la multiplicité d'initiatives pour le grand public, les organisations, ou le secteur éducatif, nous observons toujours un manque d'attractivité des sujets technologiques et en particulier cybers. Ce frein majeur au développement de la filière doit être surmonté.

DÉFI MAJEUR À RELEVER

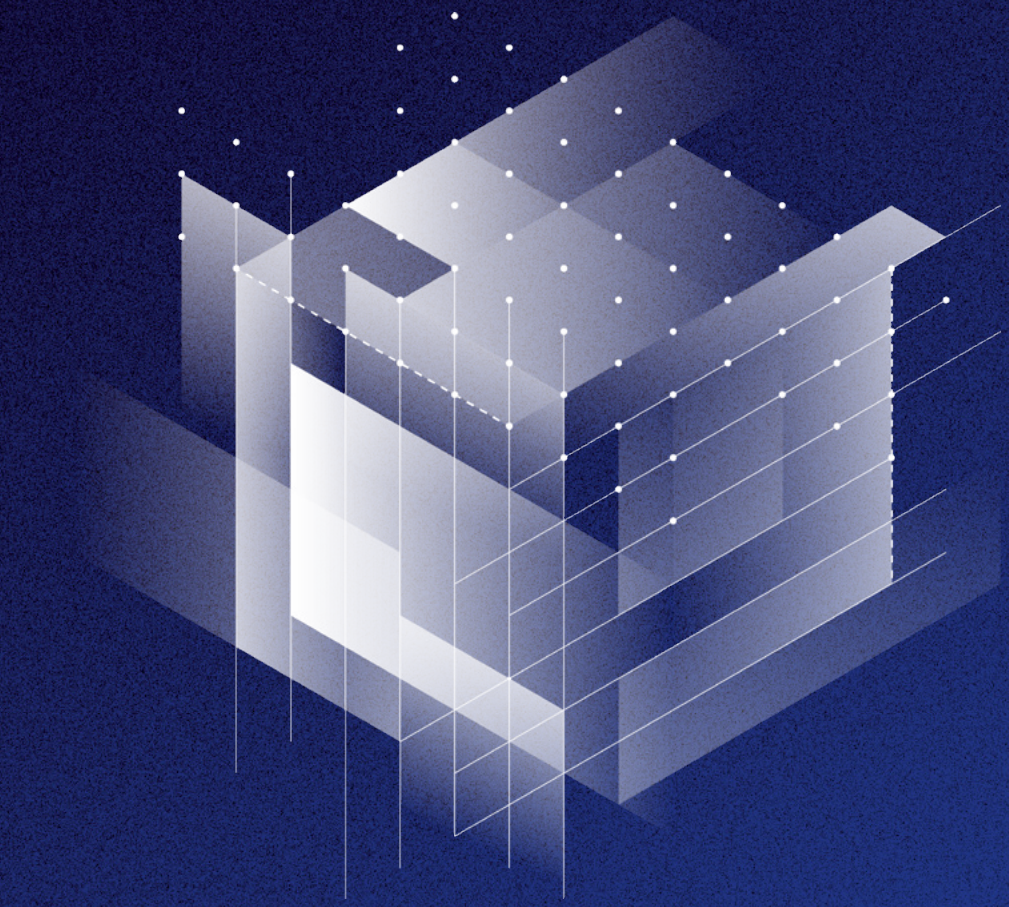
Assurer la disponibilité des compétences cyber sur le marché et augmenter l'attractivité de la filière.

PREMIÈRES ACTIONS DU CAMPUS CYBER.

Fédérer, valoriser et aider à la mise cohérence des dispositifs de valorisation de la cybersécurité.

+ **Développer un portail de la formation et de l'emploi cyber ;**
+ **Renforcer la coopération avec l'éducation nationale ;**
+ **Mutualiser des ressources et des actions de communication.**

AU DELA DE 2030
LE RÔLE DU QUANTIQUE



LE QUANTIQUE : MENACE ET OPPORTUNITÉ À LONG TERME

Le quantique, par le changement de paradigme qu'il implique et les résultats potentiellement impressionnants qu'il présente pour le numérique, peut être une menace pour la cyber (e.g. de part sa capacité à casser plus simplement les méthodes de chiffrement utilisées actuellement). Mais, il représente aussi une opportunité pour repenser la cybersécurité. Dans ce contexte, le Campus Cyber devra suivre de près ces évolutions.

→ **Aujourd'hui, nous observons les premières utilisations des propriétés quantiques pour améliorer la cybersécurité, en particulier sur la transmission des clés de chiffrement.**
Le processus est déjà fonctionnel et utile dans certains cas. Consciente de ces nouvelles capacités, la France a lancé en 2021 son plan quantique visant à renforcer la coopération entre les industriels, universités, organismes de recherche et startups en matière de recherche sur les technologies quantiques, qui inclut des éléments sur la cybersécurité. L'Europe est également engagée dans des démarches similaires.

→ **Demain, il est incontestable que les initiatives devront s'étendre, potentiellement à la création d'un « internet quantique » ou d'un « numérique quantique ».**
L'apport et l'efficacité des approches sur le quantique restent à évaluer, mais elles pourraient permettre de mettre en œuvre des mécanismes nouveaux, avec une plus-value importante pour la cyber : transmission de clé de chiffrement entre nœuds non « de confiance », délégation de calculs quantiques, calcul distribués quantiques... Même si beaucoup reste à prouver les usages sont nombreux et leurs intérêts forts.

CONCLUSION ET REMERCIEMENTS

UN PREMIER EXERCICE QUI DOIT S'ANCRER DANS LE TEMPS

Afin d'être suivies, les solutions proposées dans ce livrable pourront faire l'objet d'indicateurs. Le Campus Cyber pourra réitérer l'exercice de prospective évoluer les scénarios et les solutions envisagées.

Par ailleurs, il sera impératif de mettre en place des mécanismes d'observation de la menace et des avancées technologiques, solutions proposées le cas échéant.

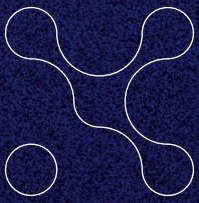
NOUS REMERCIONS CHALEUREUSEMENT L'ENSEMBLE DES CONTRIBUTEURS

ABOULHADID Ahmed, **NUMERYX**
APOSTOLOS Malatras, **ENISA**
BACHELET Julien, **HERMÈS**
BARKAOUI Badr, **BPCE**
BESNARD Quentin, **ACE CAPITAL PARTNERS**
BLARD Sebastien, **SUEZ**
BLONDEAU Florent, **NAMESHIELD**
BOBIN Maxence, **SQUAD**
CAPRONI Nicolas, **SEKOIA**
CART-LAMY Laurent, **BPCE**
CAUDRON DE CAUQUEREAUMONT, Chantal
AGENCE L'INNOVATION DE DÉFENSE
CHAILLEY Laurent, **BANQUE DE FRANCE**
CHARRAT Bruno, **CEA**
COLAS Jean-Baptiste,
AGENCE L'INNOVATION DE DÉFENSE
COUTURIER Nataël, **RED ALERT LABS**
DE FRANCO Franck, **MINISTÈRE DE L'INTÉRIEUR**
DE LIEDEKERKE Arthur, **MINARM – COM.CYBER**
DEBAR Herve, **IMT**
DELPHA Luc, **ALMOND CONSULTING**
DESAMBLANC Thierry, **ENEDIS**
DRAME Aida, **GRTGAZ**
DUAULT Hubert, **INRIA**
DUPONT Sébastien, **CYBER4U**
FEIX Olivier, **GALILEO GLOBAL EDUCATION FRANCE**
FONTARENSKY Yvan, **THALES**
GAULIER Jean-Philippe, **OSSIR – CYBERZEN**
GIANNECCHINI Mathieu, **SIMPLON**
GRANGÉ Benoit, **HUB ONE**
GREMY Jean-Marc, **CLUSIF**
GUENAUX Dominique, **ALSTOM**
HASSAN Lucas, **DGE**
HERMAN Mathilde,
AGENCE L'INNOVATION DE DÉFENSE
HEURE Jeanne, **CAPGEMINI**
HUMBERT Francis, **MINISTÈRE DE L'INTÉRIEUR**
IGLESIAS Pablo, **LFDJ**
KASSIANIDES Yoann, **ACN**
KIRCHNER Florent, **CEA**
KOLLA Vladimir, **OSSIR - GREENLOCK**
LE PIOLOT Bertrand, **LFDJ**
LECOQ Fabien, **SOPRA STERIA**
LEONETTI Xavier, **MINISTÈRE DE LA JUSTICE**
LEVASTRE David, **CYBERMALVEILLANCE**
LOUIS Nicolas, **SAFRAN**
LOURENCO Paulo, **COVÉA**
MARBAIX Jean-Pierre, **AXA**
MARREL Thibaut, **ANSSI**
MARZLOFF Bruno, **CHRONOS**
MEDA Phillipe, **ANSSI**
ME Ludovic, **INRIA**
MESEGUER Ivan, **IMT**
NETZER-JOLY Philippe, **ARKEMA**
NGUYEN Vincent, **HS2**
PAVLOV ALEXANDRE, **CYCOVER**
PERETTI Walter, **ESILV**
PITON Thierry, **AXA**
PLASSAT Gabriel, **ANSSI**
RIBEIRO Alina, **ORANGE CYBERDEFENSE**
RIBES Vincent, **EGERIE**
STEUNOU Julien, **ALMOND CONSULTING**
TABORET-AGNOLA Manuel, **MINARM – COM.CYBER**
TOUBIANA Vincent, **CNIL**
TOURNEUR Alice, **ANSSI**
TRIOLOT Benoit, **GATEWATCHER**
VALENTIN Yann, **BPCE**
VAN CAENEGEM Frank, **CNP ASSURANCES**
VINCENT Willy, **RISK & CO**

EQUIPE PROJET :
AJACQUES Jean Baptiste, **AXA**
ARGHERIA Thomas, **WAVESTONE**
BILLOIS Gérôme, **WAVESTONE**
BONNET Yann, **CAMPUS CYBER**
BRIOLAT Lucile, **CAMPUS CYBER**
COUSIN Mathieu, **AXA**
GAINIER Fabien, **CAMPUS CYBER**
QUICHAUD Marguerite, **WAVESTONE**
REGNIER Eleonore, **AXA**
Y BREH HWING Melanie, **CAMPUS CYBER**

RETROUVEZ LE DÉTAIL DE ENSEMBLE DES SOLUTIONS PROPOSÉES EN ATELIER !

https://campuscyber.fr/communs/



campuscyber.fr