Agora FIC

L'union fait la force

Les citoyens et la cybersécurité au XXIe siècle

Auteurs : Molly HALL, Apolline ROLLAND

Direction éditoriale : Pauline MASSART, Guillaume TISSIER, Amélie RIVES

TABLE DES MATIÈRES

Agora FIC

À propos

L'Agora du FIC est la plateforme de réflexion stratégique du Forum International de la Cybersécurité (FIC). Son objectif est de contribuer au débat public sur les grands enjeux de la confiance et de la sécurité numérique tout au long de l'année.

Cette plateforme de haut niveau est née du besoin des élus, décideurs, politiques et dirigeants des secteur public ou privé, des universitaires d'appréhender et de débattre des risques ou menaces, des politiques publiques (résilience, lutte contre la cybercriminalité, diplomatie numérique, politique industrielle, formation, etc.) et des grands défis sociétaux induits par les ruptures technologiques.

Parce que les réponses aux enjeux de sécurité numérique nécessitent une réponse globale, partant du citoyen (niveau local) aux États (politique nationale) jusqu'au niveau international (Union Européenne) l'Agora mène ses travaux à la fois à Paris et à Bruxelles. Afin de s'adapter à la sensibilité des sujets traités, elle propose également différents cadres d'échange et de diffusion, ouverts ou plus restreints.

agora-fic.com

Avisa Partners

BELGIQUE
Boulevard du Régent 35,
1000 Brussels

FRANCE
17, avenue Hoche,
75008 Paris

Contact :
agora@forum-fic.com

NOVEMBRE 2022

Résumé

L'augmentation du nombre de cyber-attaques semble sans fin, bénéficiant la de la numérisation toujours plus importante de nos sociétés, phénomène largement accéléré par la généralisation du télétravail pendant la pandémie de COVID19. Alors que les stratégies et plans d'action gouvernement aux à travers le monde se sont avant tout concentrés sur le renforcement de la sécurité en ligne, la place du citoyen a souvent été négligée. Les citoyens restent et demeurent le maillon faible de la cybersécurité, il apparaît primordial de pouvoir enfin les placer au cœur des efforts politiques de cybersécurité.

Comment mieux protéger les citoyens dans un espace numérique en perpétuelle mutation ? Quelle perception ont-ils des dangers auxquels ils sont exposés et quel responsable pour leur sécurité ? Comment transformer ce maillon faible en maillon fort de la cybersécurité ?

Ce livre blanc de l'Agora du FIC analyse et compare les différentes stratégies nationales, politiques publiques, cadres réglementaires et initiatives industrielles ou du secteur privé déployés à l'échelle nationale ou de l'Union Européenne, pour protéger les citoyens dans leur utilisation de produits, services et processus informatiques. Il s'intéresse aussi à la place que les citoyens doivent y tenir pour devenir acteurs de leur propre cybersécurité, aux moyens et outils nécessaires à leur fournir pour prévenir les cyberattaques et y répondre.

Ce document aborde nécessairement la question de la sensibilisation : seuls des citoyens pleinement conscients des risques qu'ils encourent et la manière d'y faire face, seront en mesure d'œuvrer à leur propre sécurité. Il est donc essentiel d'améliorer la sensibilisation à la cybersécurité, pour offrir aux citoyens une chance de devenir moins vulnérables sur Internet.

L'Agora du FIC, avec Opinion Way, a interrogé plus de 1000 citoyens européens afin d'évaluer leur niveau de sensibilisation aux questions de cybersécurité et leur expérience face aux cyber-attaques.

Les résultats sont clairs :

alors que pléthore d'initiatives sont destinées à l'amélioration de la cybersécurité des entreprises, les citoyens sont eux largement laissés pour compte. De sérieux efforts sont donc nécessaires en Europe pour améliorer la sensibilisation en matière de cybersécurité afin de rendre tout citoyen acteur de sa propre sécurité en ligne.

Ce document propose 12 recommandations concrètes visant à placer les citoyens au cœur des efforts de cybersécurité, dans le cadre d'une approche globale : gouvernements, entreprises et citoyens eux-mêmes ont chacun un rôle à jouer pour améliorer notre cybersécurité collective.

ÉDUCATION & SENSIBILISATION

1

Financer des programmes d'éducation à la cybersécurité dans les écoles. Bien qu'enfant du numérique, la génération Z, est celle dont les pratiques en matière de cybersécurité sont parmi les plus faibles de toutes les générations actuellement sur le marché du travail[1]. Cette tendance risque malheureusement de se poursuivre si la formation à la cybersécurité ne commence pas à un âge plus précoce. Il apparaît nécessaire d'intégrer aux programmes scolaires des programmes d'éducation à la cybersécurité qui soient adaptés à chaque âge et inclusifs Les financements de tels programmes pourront provenir de partenariats public-privé, car le secteur privé est responsable de la sécurité des produits ou services numériques utilisés par les citoyens.

2

Mettre en place au niveau européen des programmes de formation continue en matière de cybersécurité. Avec le développement rapide des nouvelles technologies, les bonnes pratiques en matière de cybersécurité ne cessent d'évoluer. Les citoyens doivent pouvoir, tout au long de leur vie, suivre l'évolution des réglementations, des outils et des solutions en matière de cybersécurité.

3

Faire passer les campagnes de sensibilisation de l'éducation à l'adoption. Alors que l'UE célèbre le 10e anniversaire de son « Mois de sensibilisation à la cybersécurité », la prochaine étape doit viser à s'assurer que les citoyens ne sont pas seulement conscients des meilleures pratiques en matière de cybersécurité, mais qu'ils adoptent et mettent effectivement en œuvre les solutions proposées. Les pouvoirs publics devraient profiter de la dynamique du « Mois de la cybersécurité » pour encourager les utilisateurs à mettre à jour leurs mots de passe, à activer les mises à jour automatiques ou à utiliser des logiciels antivirus.

1. The Generational Gap in Cybersecurity and Privacy, Weir, URL.

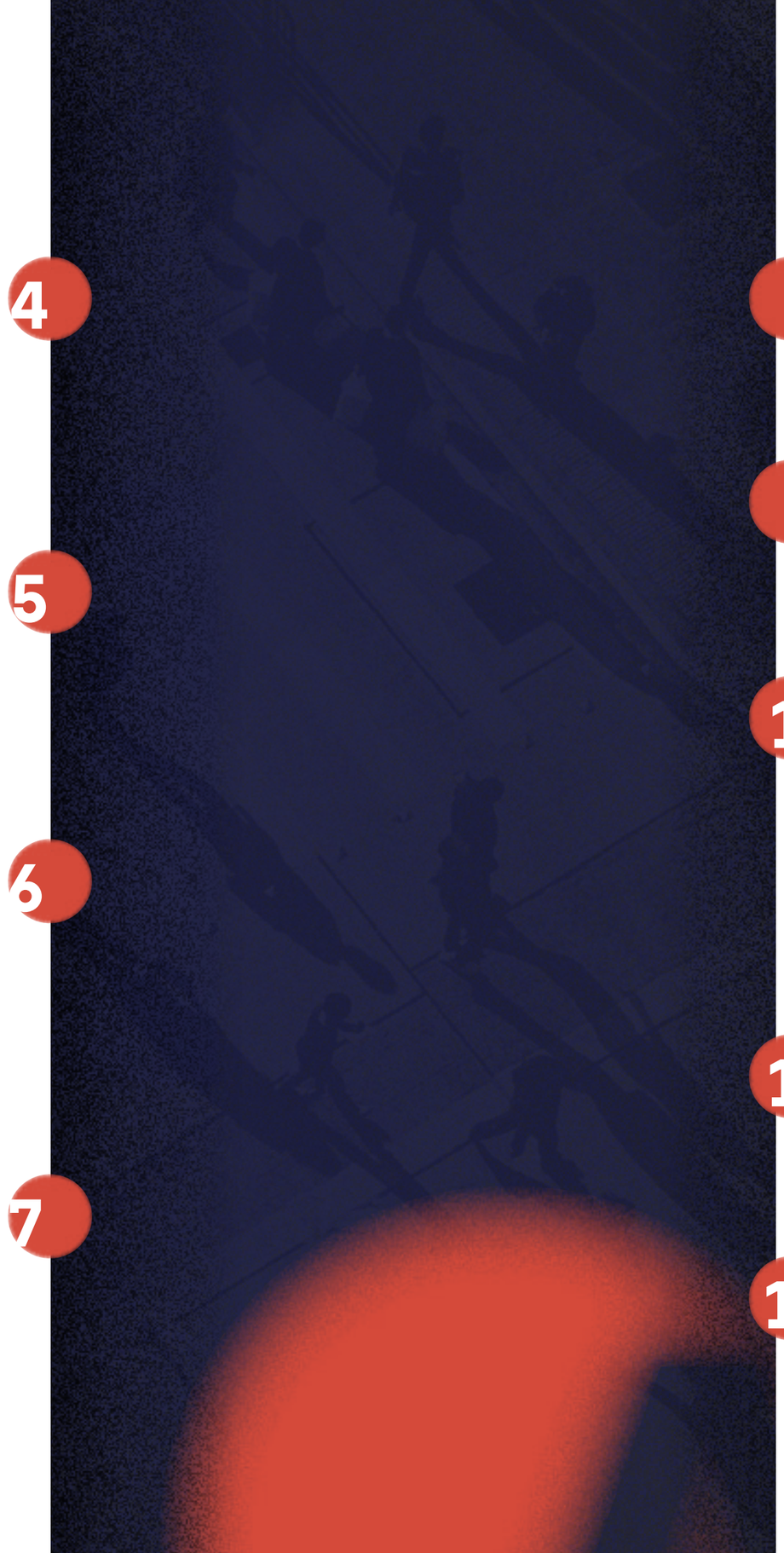
SOUTIEN AUX CITOYENS

Généraliser des « boîtes à outils » de cybersécurité à l'attention des citoyens. Certaines agences nationales de cybersécurité proposent déjà des boîtes à outils utiles, qui fournissent aux citoyens des outils leur permettant d'assurer efficacement leur sécurité en ligne, comme c'est le cas en Belgique ou au Royaume-Uni. Ces boîtes à outils devraient être facilement exploitables et très didactiques, permettant aux citoyens d'identifier les types d'attaques, de proposer des recommandations opérationnelles type « fiche réflexe », et de détailler les procédures ou démarches à réaliser auprès des bon interlocuteurs.

Élaborer et promouvoir des mesures visant à garantir des normes élevées de cybersécurité pour tous les produits. Certaines évolutions du cadre réglementaire, actuellement en cours de déploiement telles que les schémas de certification de l'UE ou la réglementation européenne sur la cyber-résilience, constituent des premiers pas importants dans cette direction. D'autres mesures devront être élaborées pour suivre l'évolution des technologies et des produits et veiller à ce qu'ils continuent à respecter des normes élevées de cybersécurité.

Exiger des fournisseurs de services numériques plus de transparence sur leurs pratiques en matière de sécurité et de respect de la vie privée. Les fournisseurs de services numériques, y compris les fournisseurs d'accès à l'internet, disposent d'une certaine marge de manœuvre quant aux informations qu'ils peuvent recueillir et stocker, et à ce qu'ils peuvent en faire, en particulier s'ils opèrent en dehors de l'UE. Les citoyens doivent pouvoir être sûrs que lorsqu'ils se connectent à l'internet et utilisent des appareils électroniques, ils sont en sécurité. Ces fournisseurs devraient donc être plus transparents quant à leurs pratiques en matière de confidentialité et de sécurité.

Créer un « Cyberscore ». Sur le modèle du Nutriscore, un « Cyberscore » pourrait indiquer le niveau de cybersécurité et de confiance dans un produit ou service via une classification sous forme de code couleurs.Ce système permettrait de fournir directement au consommateur une indication claire et lisible afin d'éclairer sa décision d'achat.



POLITIQUE & SENSIBILISATION

Élaborer un contrat social en ligne. L'élaboration d'un e-contrat social pourrait contribuer à améliorer la confiance numérique et à encourager le partage des responsabilités en ligne entre les pouvoirs publics, l'industrie et les citoyens. Les termes d'un tel contrat devraient être définis en consultation avec toutes les parties prenantes concernées, notamment les gouvernements, l'industrie, les organisations de la société civile et les citoyens.

Adopter et mettre en œuvre rapidement la loi sur la cyber-résilience et les futurs règlements européens. Les États membres utilisent des processus différents pour transposer et mettre en œuvre les règlements de l'UE, ce qui peut entraîner une mise en œuvre inégale, défavorable aux citoyens. Les États membres doivent mettre en œuvre rapidement les politiques de cybersécurité de l'UE.

Améliorer le partage d'informations sur les menaces entre les gouvernements, l'industrie et les citoyens. Les organismes gouvernementaux compétents doivent continuer à informer l'ensemble des organisations de l'état de la menace et des tendances observées, mais aussi en informer directement les citoyens. La Belgique, par exemple, propose une revue d'informations cybersécurité qui informe les citoyens des cyber menaces, comme ils le font par exemple pour les menaces météorologiques sérieuses. Un parallèle peut être fait avec les dispositifs d'alerte sur la menace terroriste à l'image du plan Vigipirate en France. Cette pratique devrait être étendue à l'ensemble de l'UE et permettrait de mieux informer les citoyens sur le niveau des cybermenaces.

Dégager des financements pour accompagner la mise en conformité des nouvelles normes. L'élaboration de systèmes de certification en matière de cybersécurité et l'introduction de nouvelles normes représentent souvent une charge financière pour les fournisseurs comme pour les utilisateurs. Des fonds dédiés devraient être mis à disposition pour permettre aux parties prenantes de suivre le rythme et de se conformer aux exigences législatives.

Promouvoir une approche locale pour la mise en œuvre des stratégies de cybersécurité. Les autorités locales, qui sont au plus proche des citoyens ont un rôle clé à jouer pour impliquer ces derniers dans les efforts de cybersécurité. Les autorités locales doivent être habilitées par les autorités européennes, nationales et régionales à communiquer avec les citoyens sur le « dernier kilomètre ».

INTRODUCTION

L'Union européenne (UE) s'est pleinement engagée dans sa « décennie numérique », ayant pour objectif la numérisation complète de ses États membres d'ici à 2030. Or, le développement d'une société numérique sûre repose sur la cybersécurité de ses organisations et de ses citoyens.

La pandémie COVID-19 a considérablement accéléré la numérisation de l'Europe et a entraîné une augmentation significative des cyber-attaques (+ 81 %). La guerre en Ukraine a ensuite propulsé la cybersécurité au premier plan des préoccupations, notamment avec les tactiques de guerre hybride de la Russie.

Comment mieux protéger les citoyens dans cet environnement en mutation ? Qui est responsable de la protection des citoyens, et comment leur donner les moyens de devenir les maillons les plus forts, et non les plus faibles, de la cybersécurité ?

L'UE a développé un solide corpus réglementaire en matière de cybersécurité et de protection de la vie privée. Du règlement général sur la protection des données (RGPD) de 2016 à la plus récente loi sur la cyber-résilience (2022), l'UE a établi des normes d'une portée globale pour garantir la sécurité des citoyens en ligne, leurs données, et leur vie privée.

Les efforts visant à créer un environnement numérique sûr dépassent le cadre réglementaire élaboré par l'UE, et englobent à la fois les initiatives des États membres, du secteur privé et de la société civile. Pourtant, malgré les réglementations, les outils et les initiatives en matière de cybersécurité, **il existe un décalage manifeste dans la manière dont les gouvernements et les particuliers perçoivent la cybersécurité.**

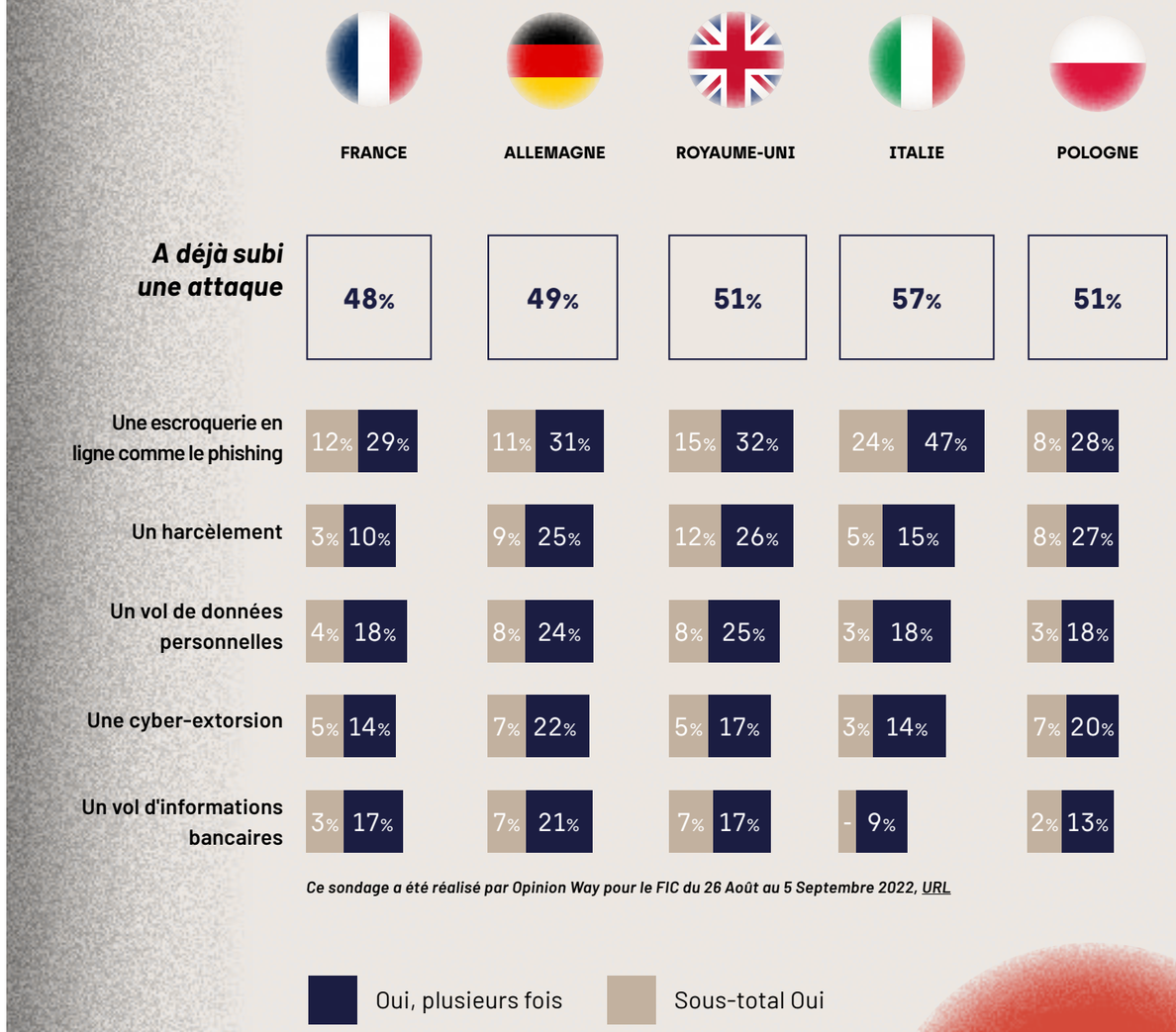
Une **enquête exclusive menée par le FIC** sur la sensibilisation des citoyens européens à la cybersécurité en France, en Allemagne, au Royaume-Uni, en Italie et en Pologne a révélé que 51 % d'entre eux avaient déjà subi une cyberattaque, mais que deux tiers n'avaient jamais vu de campagne de sensibilisation à la cybersécurité. Ces résultats révèlent une déconnexion évidente et un besoin de recentrer les cadres de cybersécurité existants sur les citoyens .

La cybersécurité est une condition *sine qua non* de la souveraineté numérique européenne, et les citoyens en détiennent la clé. Forts de cette conviction, certains États membres de l'UE ont développé de vastes programmes de sensibilisation et d'outils permettant aux individus d'améliorer leur propre cybersécurité. Mais cette démarche est loin d'être majoritaire et les seuls programmes de sensibilisation gouvernementaux ne peuvent suffire. Le secteur privé doit lui aussi s'impliquer et jouer un rôle plus important dans la cybersécurité et la protection de la vie privée des utilisateurs et des citoyens. Seule une approche stratégique globale centrée sur le citoyen peut lui permettre de mieux maîtriser sa cybersécurité.

Pour développer une telle vision, il est d'abord nécessaire de partir de l'existant : comment l'UE, ses États membres, le secteur privé et les organisations de la société civile œuvrent déjà à la protection des citoyens. Ce document examine les cadres réglementaires en vigueur, les initiatives et programmes déjà déployés, et met en perspective la manière dont les citoyens perçoivent leur cybersécurité, c'est-à-dire la capacité à être protégé dans leurs usages numériques. Il propose une série de recommandations visant à placer les citoyens au cœur des stratégies de cybersécurité nationales et européennes.

2. Enquête OpinionWay pour le FIC réalisée en septembre 2022.

AVEZ-VOUS DÉJÀ ÉTÉ VICTIME DE CHACUNE DES ATTAQUES SUIVANTES ?



Ce sondage a été réalisé par Opinion Way pour le FIC du 26 Août au 5 Septembre 2022, URL

51%
des sondés ont déjà été victimes d'une cyber-attaque

OÙ S'ARRÊTE LA RESPONSABILITÉ ? PROTÉGER LES CITOYENS SUR INTERNET

Les cadres réglementaires en matière de cybersécurité se sont concentrés sur l'amélioration du niveau de protection des organisations gouvernementales ou des infrastructures stratégiques. Dans l'Union européenne, ces cadres comprennent à la fois des politiques supranationales et nationales, ce qui ne les rend que plus compliqués à comprendre pour les entreprises et les citoyens.

L'APPROCHE DE L'UNION EUROPÉENNE

La protection et la résilience en matière de cybersécurité figurent en tête de l'agenda politique numérique de l'UE. De fait, l'UE s'efforce de renforcer depuis 2013[3] son cadre réglementaire, lequel repose sur plusieurs réglementations clés qui englobent :

- **Cybersécurité :** réglementations encadrant la protection des réseaux et des systèmes
- **Protection des données :** réglementation relative à la protection des données à caractère personnel.

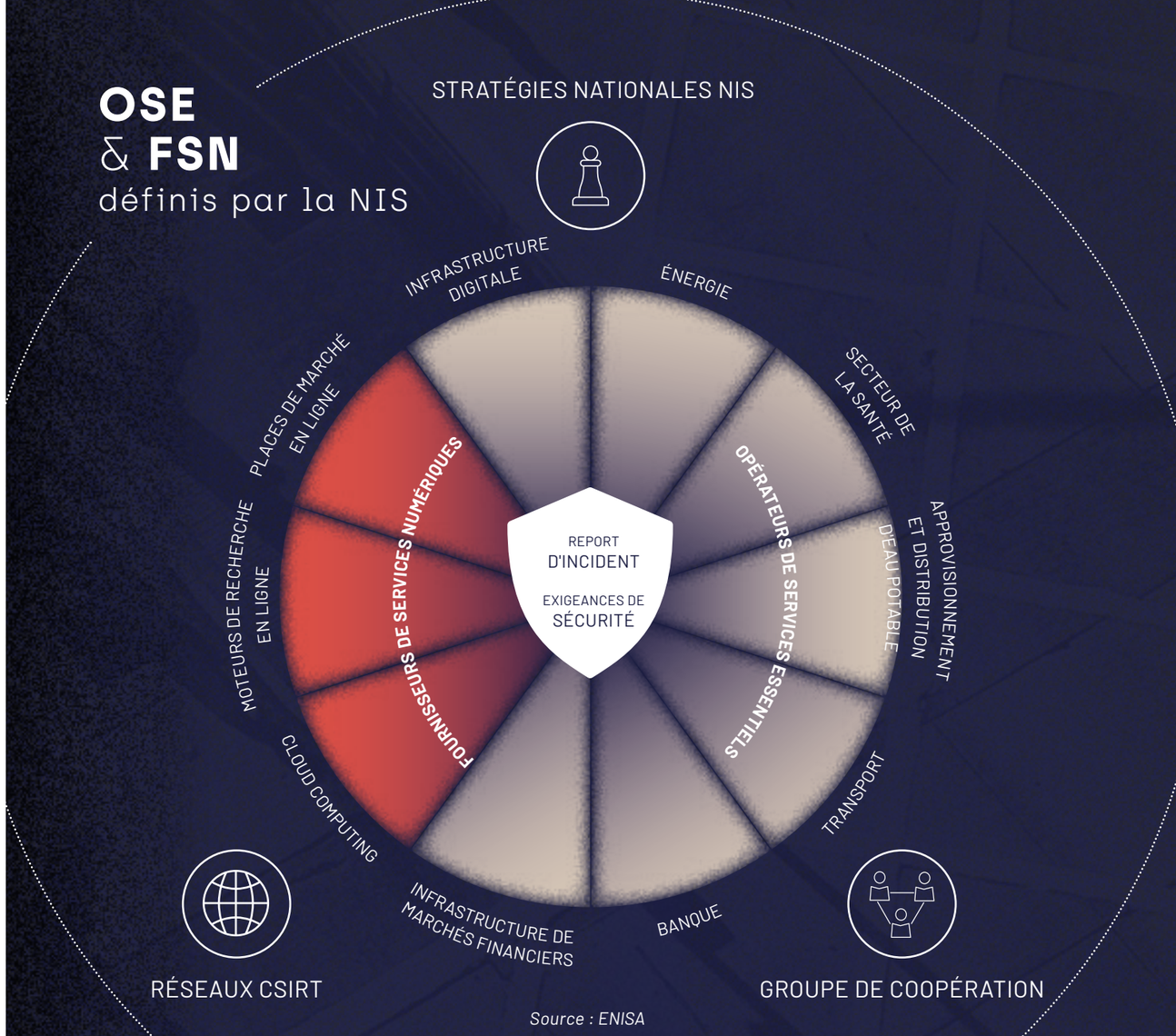
CYBERSÉCURITÉ

DIRECTIVE SUR LA SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION

NIS
[2016]

La directive de 2016 sur la sécurité des réseaux et des systèmes d'information (SRI ou NIS)[4] est la première réglementation européenne à imposer un niveau minimal de cybersécurité dans l'UE afin d'améliorer la cyber-résilience globale des États membres (EM) de l'UE[5]. Elle exige des États membres qu'ils élaborent une stratégie de cybersécurité, qu'ils soient équipés de manière adéquate pour faire face aux cybermenaces, qu'ils mettent en place une autorité nationale de cybersécurité et qu'ils désignent un CSIRT national[6]. La directive NIS vise également à renforcer la coopération entre les États membres avec la création du groupe de coopération NIS et du réseau de CSIRT, et à promouvoir une culture de la cybersécurité dans les secteurs des infrastructures critiques. Plus précisément, la directive NIS établit une distinction entre les **« opérateurs de services essentiels » (OSE) et les « fournisseurs de services numériques » (FSN).**

3. The European Cybersecurity Market, Enterprises Ireland, URL.
4. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures relatives à un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union, URL.
5. Ibid
6. Équipe d'intervention en cas d'urgence informatique : groupe d'experts chargé de gérer les incidents de sécurité informatique.



Source : ENISA

En vertu de la NIS, les OSE et les FSN doivent :

- **Sécuriser leur réseau et leurs systèmes d'information** en adoptant des mesures techniques et organisationnelles adaptées au risque.
- **Assurer la continuité du service** en prenant les mesures appropriées pour prévenir et minimiser l'impact des incidents de sécurité.
- **Notifier à l'autorité nationale compétente tout incident de sécurité** ayant un impact significatif sur la continuité des services essentiels fournis[7] [8].

Les États membres étaient chargés d'identifier eux-mêmes les OSE de leurs pays respectifs, ce qui a conduit à des interprétations nationales différentes[9] et fait l'obstacle à l'homogénéité du marché européen[10].

7. Il n'existe pas de directive européenne spécifique concernant le seuil de notification des incidents, chaque État membre applique ici ses directives aux OSE et FSN nationaux.
8. The EU NIS Directive, IT Governance, URL.
9. Briefing on the NIS2 Directive: A high common level of cybersecurity in the EU, Negreiro, URL.
10. NIS Directive, IT Governance, URL.

DEUXIÈME DIRECTIVE SUR LA SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION

NIS2

(2022)

La proposition de directive NIS2 (2020)[11] a été motivée d'une part par l'augmentation du nombre de cyberattaques visant l'Europe, d'autre part par l'interdépendance numérique croissante au sein de l'UE et au-delà, mais également afin de mieux prendre en compte l'évolution des services numériques désormais essentiels à nos sociétés numériques[12]. La directive NIS2 a été introduite pour clarifier et élargir le champ d'application de la première directive NIS. Elle codifie un régime d'obligations et de sanctions pour les fournisseurs de services essentiels, élargit le nombre d'organisations publiques et privées qui doivent améliorer leur niveau de sécurité, traite de la sécurité de la chaîne d'approvisionnement, rationalise les obligations de déclaration, et introduit desexigences d'application et une surveillance plus stricte[13].

NIS2 remplace les OSE et les FSN par deux nouvelles catégories : les entités « essentielles » et les entités « importantes »[14]. Les entités essentielles comprennent les OSE couvertes par la première NIS (énergie, transport, banque, finance, infrastructure de marché, santé, eau potable et infrastructure numérique) et, en plus, les entités des secteurs de la gestion des eaux usées, de l'administration publique et certaines infrastructure numériques (telles que les fournisseurs de *cloud* et de centres de données, les fournisseurs de points d'échange Internet, les registres de noms de domaine de premier niveau) et du secteur spatial[15]. Les entités importantes correspondent aux opérateurs des secteurs des services postaux et de messagerie, de la gestion des déchets, de la fabrication, de la production et de la distribution de produits chimiques, de la production, de la transformation et de la distribution de produits alimentaires, et des fournisseurs numériques (tels que les fournisseurs de réseaux sociaux et de plateformes de services, de marchés en ligne et de moteurs de recherche)[16].

11. Proposition de directive du Parlement européen et du Conseil concernant des mesures pour un niveau commun élevé de cybersécurité dans l'Union, abrogeant la directive (UE) 2016/1148,, URL.
12. Briefing on the NIS2 Directive: A high common level of cybersecurity in the EU, Negreiro, URL.
13. Ibid
14. Cybersecurity in the EU – Why we need NIS2 and what changes does it mean for the tech sector?, EURACTIV, URL.
15. EU Country Commercial Guide - Cyber Security, International Trade Administration, URL.
16. Ibid

COMPARAISON DES DIRECTIVES NIS ET NIS2

	NIS (2016)	NIS (2022)
Objectifs	> Augmenter le niveau général de cybersécurité et de cyber-résilience dans l'UE. > Harmoniser le niveau de cybersécurité entre les États membres en garantissant un niveau minimal de cybersécurité. > Veiller à ce que les États membres et les entreprises soient correctement équipés pour faire face aux cybermenaces. > Renforcer la coopération entre les États membres dans le domaine de la cybersécurité > Promouvoir une culture de la cybersécurité à l'échelle de l'UE dans certains secteurs critiques fournissant des services essentiels.	> Renforcer la cyber-résilience dans toute l'UE en étendant le champ d'application de la directive en termes de secteurs et d'entreprises couverts, et en limitant la fragmentation due aux différences d'interprétation entre les États membres. > Réduire les incohérences, harmoniser les exigences en matière de rapports sur la sécurité et les incidents, le suivi et les capacités de cybersécurité des États membres. > Améliorer la coopération et le partage d'informations
Désignation des entités	Les "opérateurs de services essentiels" (OSE) Les "fournisseurs de services numériques" (FSN)	Entités essentielles Entités importantes
Secteurs couverts	**OSE :** Infrastructures numériques, énergie, secteur de la santé, approvisionnement et distribution d'eau potable, transport, banques, infrastructures des marchés financiers. **FSN :** *Cloud computing*, marché en ligne, moteurs de recherche en ligne	**Entités essentielles :** OSE existants (secteurs de l'énergie, du transport, de la banque, de la finance, de l'infrastructure de marché, de la santé, de l'eau potable et de l'infrastructure numérique) + secteurs des eaux usées, de l'administration publique (tels que les fournisseurs de *cloud* computing et de centres de données, les fournisseurs de points d'échange Internet, les registres de noms de domaine de premier niveau) et du spatial. **Entités importantes :** Services postaux et de messagerie, gestion des déchets, fabrication, production et distribution de produits chimiques, production, transformation et distribution de produits alimentaires, et fournisseurs numériques (tels que les fournisseurs de réseaux sociaux et de plateformes de services, de places de marché en ligne et de moteurs de recherche).
Résultats	Mise en place de stratégies de cybersécurité, d'autorités nationales de cybersécurité et de CSIRTs dans les États membres de l'UE. Amélioration du niveau général de cybersécurité dans l'UE. Création d'un groupe de coopération NIS et d'un réseau de CSIRT.	*Prévu :* Règles harmonisées d 'interprétation et de mise en œuvre de la directive, réduction de la fragmentation. Amélioration du niveau de cybersécurité et de cyber-résilience de l'UE. Amélioration du partage d'informations et de la coopération entre les États membres. Renforcement du groupe et du réseau existants et création du réseau EU-CyClone pour soutenir la coordination et la gestion des incidents à grande échelle.[17]
Impact négatif	Fragmentation due aux différences d'interprétation nationale des directives[18]. (Ex : différences dans la classification des OSE) Absence de régime de supervision et d'application efficace[19] Partage limité de l'information entre les États membres[20]	*Prévu :* Une mise en œuvre inégale du premier NIS signifie des conditions inégales pour la mise en œuvre du NIS2. Les nouvelles obligations pèseront sur les organisations, à moins que le nouveau NIS ne soit associé à un soutien efficace.

Le NIS2 devrait être adopté par le Parlement européen en octobre 2022, et sa transposition dans le droit national des États membres devrait avoir lieu en 2024[21].

17. Briefing on the NIS2 Directive: A high common level of cybersecurity in the EU, Negreiro, URL.
18. Ibid
19. Ibid
20. Ibid
21. Révision de la directive sur la sécurité des réseaux et des systèmes d'information, Train législatif du Parlement européen, URL.

LOI SUR LA CYBERSÉCURITÉ DE L'UE

(2019)

La loi sur la cybersécurité[22] a été adoptée en 2019 pour soutenir et faire progresser les dispositions de la directive NIS de 2016. La loi sur la cybersécurité établit un cadre juridique pour le marché unique numérique (MN) de l'UE, afin de supprimer les obstacles existants entre les États membres dans le secteur numérique et d'encourager les transactions commerciales transfrontalières[23]. Elle renforce le mandat de l'Agence de l'Union européenne pour la cybersécurité (ENISA) et introduit un cadre européen uniformisé de certification de cybersécurité pour les produits, services et processus des technologies de l'information et de la communication (TIC), définis comme[24] :

PRODUCT TIC

Élément ou groUpe d'éléments d'un réseau ou d'un système d'information

SERVICE TIC

Service consistant entièrement ou principalement dans la transmission, le stockage, la récupération ou le traitement d'informations au moyen de réseaux et de systèmes d'information

PROCESS TIC

Ensemble d'activités de conception, développement, fourniture ou maintien d'un produit ou service TIC

Le cadre européen de certification en matière de cybersécurité délivre des certifications reconnues dans toute l'UE, ce qui permet aux produits, services et processus numériques d'être certifiés une seule fois pour l'ensemble du marché européen[25]. Ces certifications assurent un niveau minimum de cybersécurité des solutions numériques et un niveau de confiance dans ces solutions au niveau de l'UE. Les certifications sont délivrées par des autorités nationales de certification en matière de cybersécurité (ANCC) désignées par les États membres pour superviser la conformité des certificats[26]. Pour l'instant, la certification des produits, services et processus numériques reste volontaire[27] mais pourrait devenir obligatoire pour les produits, services et processus numériques à haut niveau de risque d'ici 2023[28].

Trois systèmes de certification européens sont actuellement en cours d'élaboration :

- **Schéma de certification européen de cybersécurité basé sur les critères communs (EUCC) :** il est basé sur le schéma international existant des critères communs, la méthodologie commune d'évaluation de la sécurité des technologies de l'information, et les normes correspondantes ISO/IEC 15408 et ISO/IEC 18045[29]. Une première version a été livrée à la Commission européenne en mai 2021 mais doit encore être approuvée pour être effective[30].
- **Système européen de certification de la cybersécurité pour les services de *cloud* (EUCS) :** le système est toujours en cours d'élaboration à la suite des consultations publiques qui ont pris fin en février 2021. De vives discussions sur ce texte sont toujours en cours entre les États membres, notamment en ce qui concerne les exigences de souveraineté qui limiteraient ou empêcheraient d'éventuelles interférences des États non-membres de l'UE avec les services de *cloud* certifiés[31 32 33].
- **Certification européenne en matière de cybersécurité de la 5G (EU5G) :** le système est encore en cours d'élaboration. Un groupe de travail ad hoc (AHWG)[34] - un groupe de parties prenantes dirigé par l'ENISA pour partager leur expertise et aider à créer des schémas de certification - a été établi en octobre 2021 pour élaborer ce schéma[35].

22. Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) et à la certification en matière de cybersécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n° 526/2013 (loi sur la cybersécurité), URL.
23. Le marché européen de la cybersécurité, Enterprises Ireland, URL
24. Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) et à la certification en matière de cybersécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n° 526/2013 (loi sur la cybersécurité), URL.
25. La loi sur la cybersécurité de l'UE, Commission européenne, URL.
26. EU Cybersecurity Certification - FAQ, ENISA, URL.
27. Understanding the EU Cybersecurity Act and Its Effect on Businesses Dunkelberger, URL.
28. The European Cybersecurity Act, EUROSMART, URL.
29. Cybersecurity Certification: Candidate EUCC Scheme V1.1.1, ENISA, URL.
30. Public Consultation on the draft Candidate EUCC Scheme, ENISA, URL.
31. Consultation on the draft of the candidate Certification Scheme on Cloud Services (EUCS) - Closed, ENISA, URL.
32. Germany calls for political discussion on EU's cloud certification scheme, Bertuzzi, URL.
33. Sovereignty requirements remain in cloud certification scheme despite backlash, Kabelka, URL.
34. Ad-hoc Working Group calls, ENISA, URL.
35. Ad-Hoc Working Group 03 - on 5G Cybersecurity Certification, ENISA, URL.

LOI SUR LA CYBER-RÉSILIENCE

(EN COURS)

La loi sur la cyber-résilience, introduite en septembre 2022, est le dernier texte réglementaire qui vient compléter l'arsenal législatif européen en matière de cybersécurité[36].

La loi sur la cyber-résilience vise à établir des normes communes pour les produits de cybersécurité, d'harmoniser les politiques, et de renforcer le pouvoir normatif de l'UE en matière de cybersécurité[37]. La loi sur la cyber-résilience imposera des règles et des obligations aux fabricants et aux vendeurs de produits, afin de répondre aux besoins du marché et de protéger les utilisateurs[38], par exemple par l'introduction de dispositions sur l'évaluation de la conformité ou la surveillance du marché[39].

Les objectifs de la Commission européenne sont triples[40] :

1. Améliorer et garantir un niveau élevé et constant de cybersécurité des produits numériques et des services auxiliaires.
2. Permettre aux utilisateurs de faire correspondre le niveau de sécurité de ces produits à leurs besoins, notamment en améliorant la transparence sur les caractéristiques de cybersécurité des produits.

   L'objectif est de protéger les utilisateurs contre les produits et services non sécurisés et d'inciter les vendeurs à proposer des produits plus sûrs, pour augmenter ainsi la confiance dans le marché unique du numérique.
3. Améliorer le fonctionnement du marché intérieur en uniformisant les conditions de concurrence pour les vendeurs de produits et services numériques.

La proposition de loi sur la cyber-résilience garantirait :

4. Des règles harmonisées pour la mise sur le marché de produits ou de logiciels ayant une composante numérique ;
5. Un cadre d'exigences de cybersécurité régissant la planification, la conception, le développement et la maintenance de ces produits, avec des obligations à respecter à chaque étape de la chaîne de valeur ;
6. Un devoir de diligence pour l'ensemble du cycle de vie de ces produits[41].

Le Conseil de l'UE et le Parlement européen doivent encore délibérer. Après l'adoption, les États membres auront 24 mois pour transposer le règlement dans leur législation nationale.

36. Cyber Resilience Act, European Commission, URL.
37. The new European Cyber Resilience Act, European Parliament Train Schedule, URL.
38. Législation sur la cyber-résilience - nouvelles règles en matière de cybersécurité concernant les produits numériques et les services accessoires, Commission européenn, URL.
39. Ibid
40. Ibid
41. Loi sur la cyber-résilience de l'UE, Commission européenne, URL.

IMPACTS DE LA RÉGLEMENTATION EUROPÉENNE EN MATIÈRE DE CYBERSÉCURITÉ SUR LA PROTECTION DES CITOYENS DE L'UE

Les réglementations européennes en matière de cybersécurité ne visent peut-être pas directement les citoyens, mais elles ont un impact positif direct sur leur niveau global de protection. Les réglementations de l'UE relèvent le niveau général de cybersécurité au sein des États membres et garantissent un niveau minimal de sécurité des produits ou solutions utilisées par les consommateurs. Ainsi, les directives NIS et NIS2, sécurisent par exemple les infrastructures critiques fournissant des services essentiels aux citoyens européens, tandis que les certifications européennes garantissent la sécurité des produits utilisés par les consommateurs.

PROTECTION DES DONNÉES

RGPD

[2016]

En 2016, l'UE a adopté l'une des réglementations les plus complètes au monde en matière de protection des données et de la vie privée. Le règlement général sur la protection des données (RGDP)[42] renforce les droits et le contrôle des individus sur leurs données personnelles en imposant des obligations aux organisations, où qu'elles se trouvent, lorsqu'elles ciblent ou collectent des données sur des individus dans l'UE. Le RGDP introduit des dispositions et des exigences liées au traitement des données personnelles des individus et prévoit des amendes importantes pour les organisations qui ne respectent pas les normes de confidentialité et de sécurité[43]. Le RGDP a été une source d'inspiration en termes de gouvernance des données personnelles dans le monde entier, et démontre le pouvoir normatif de l'UE et sa capacité à établir et promouvoir des normes internationales conformes à ses valeurs.

LES APPROCHES NATIONALES

Les gouvernements ont le devoir de protéger leurs citoyens, y compris dans le cyberespace. Les cadres réglementaires nationaux ont un impact direct sur la manière dont les citoyens naviguent dans les environnements en ligne, et visent à protéger les populations contre les cybermenaces, qu'elles soient d'origine étatique ou criminelle. La plupart des réglementations nationales donnent toutefois la priorité à la protection des infrastructures critiques plutôt qu'à celle des citoyens, dans l'idée que si ces entreprises sont sécurisées, les citoyens seront protégés.

PROTECTION DES INFRASTRUCTURES CRITIQUES

La protection et des infrastructures critiques est indispensable pour garantir que les données des citoyens sont protégées et qu'ils peuvent évoluer dans l'espace numérique en toute sécurité. Les règlements de l'UE définissent les responsabilités des services essentiels, mais quel est l'état de la situation au-delà de l'UE, dans un monde ultra-connecté ? Si certains pays ont modifié les réglementations existantes pour définir les infrastructures critiques, incluant les fournisseurs de services numériques, d'autres ont adopté des législations dédiées pour définir la cybersécurité et les exigences en matière de déclaration des incidents. Ces différences d'approches expliquent qu'il est aujourd'hui complexe pour les fournisseurs de comprendre à quelles obligations ils sont soumis, et qu'il est difficile pour les citoyens d'estimer le niveau de protection des solutions numériques qu'ils utilisent. Dans la plupart des pays, les politiques de cybersécurité ne sont pas axées sur les citoyens en premier lieu. Les États-Unis et Israël offrent des études de cas comparatives intéressantes.

IMPACTS DU RGPD
SUR LA PROTECTION DES CITOYENS DE L'UE

L'un des impacts les plus visibles du RGPD est l'obligation de stocker toute donnée collectée dans l'UE et de limiter le transfert ou l'utilisation non autorisée de ces données. 65 % des répondants à l'enquête menée par le FIC estiment que leurs données sont en sécurité lorsqu'elles sont stockées dans l'UE[44]. Le contraste est saisissant avec les États-Unis, où 85 % des personnes interrogées dans le cadre d'une enquête menée par Ipsos en 2022 se disent préoccupées par la sécurité et la confidentialité des données qu'elles partagent en ligne[45]. Le RGPD a sans aucun doute joué un rôle dans la sécurisation des citoyens européens dans leurs activités en ligne en fixant des normes élevées en matière de protection de la vie privée. L'adoption de réglementations calquées sur le RGPD au-delà de l'UE témoigne du pouvoir normatif de l'Europe et de sa capacité à promouvoir les droits des personnes concernées au niveau mondial.

42. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ce (règlement général sur la protection des données), URL.
43. What is GDPR, the EU's new data protection law?, GDPR.EU, URL.
44. Enquête OpinionWay pour le FIC réalisée en septembre 2022, URL.
45. A majority of Americans are concerned about the safety and privacy of their personal data, Ipsos, URL.

ÉTATS-UNIS

Aux États-Unis, l'Agence pour la cybersécurité et la sécurité des infrastructures (CISA), au sein du ministère de la sécurité intérieure (DHS), est chargée de définir la politique de cybersécurité nationale[46]. La CISA ne se contente pas de sécuriser les domaines du gouvernement fédéral, mais coordonne et définit également la politique de sécurité des grandes infrastructures nationales. Dans ce rôle, la CISA s'attache à collaborer avec des partenaires du secteur privé pour s'assurer que toute réglementation ou recommandation soit réaliste afin d' être réellement implémentée, de manière à renforcer leur cyber-résilience sans leur imposer une charge excessive.

Au-delà, le paysage réglementaire américain est encore largement en développement. Plusieurs politiques récentes contribuent à définir des obligations de cybersécurité à l'attention des opérateurs de services critiques et numériques. Plus particulièrement, le *Cyber Incident Reporting for Critical Infrastructure Act* of 2022 (CIRCIA, Loi sur le rapport de cyber-incidents pour les infrastructures critiques[47]) établit des exigences fortes en matière de déclaration des incidents. Toutefois, ce texte doit encore être clarifié lors du processus législatif. On peut s'attendre à des réactions de l'industrie contre ces nouvelles réglementations supplémentaires, ce qui pourrait entraîner des exceptions au régime prévu initialement ou un affaiblissement des exigences originales. La réglementation finale pourrait ne pas être disponible avant 2025.

ISRAËL

Israël est mondialement reconnu comme leader en matière de technologie et de cybersécurité. Son paysage réglementaire est presque aussi complexe que celui des États-Unis, notamment en raison de la façon dont les responsabilités en matière de cybersécurité sont réparties entre différents organismes gouvernementaux. Le principal organisme de réglementation de la cybersécurité est la Direction nationale israélienne du cyberespace (INCD), chargée de la protection des services essentiels. L'INCD a été créé en 2018 par la fusion de l'Autorité nationale de cybersécurité (NCSA), qui était l'organe opérationnel de la cyber protection, et du Bureau national du cyberespace (INCB), qui était responsable des politiques et de la constitution de capacités cybernétiques[48].

La protection des infrastructures critiques est une priorité en matière de cybersécurité pour Israël depuis près de 30 ans. Le gouvernement a adopté la résolution spéciale B/84 en 2003[49], qui définit les infrastructures critiques et impose à ces organisations de disposer d'un personnel dédié à la sécurité informatique[50]. En outre, Israël dispose de deux autres lois clés définissant le cadre réglementaire de la cybersécurité, notamment la loi informatique de 1995 (modifiée en 2012) et le règlement de 2018 sur la protection de la vie privée (sécurité des données) 5777 2017. Ensemble, ces textes définissent des exigences en matière de protection des infrastructures critiques similaires à celles de la directive NIS de l'UE.

46. Cybersecurity, CISA, URL.
47. PUBLIC LAW 117–103—MAR. 15, 2022, American Congress, URL.
48. Cyber force refers to the responsibility to develop a national cyber defence. See more here.
49. Israel Defense Forces and National Cyber Defense, Tabansky, URL.
50. Les secteurs d'infrastructures critiques en Israël comprennent les 11 secteurs définis dans la directive NIS plus les suivants : Approvisionnement et distribution des aliments, gouvernement, sécurité publique et application de la loi.

REGARDS CROISÉS SUR LA PROTECTION DES INFRASTRUCTURES CRITIQUES EN EUROPE, EN ISRAËL ET AUX ÉTATS-UNIS[51] ?

Israël fait une distinction claire entre les rôles des agences civiles et militaires dans la protection du cyberespace. En outre, le gouvernement israélien est bien conscient de la nécessité de protéger les libertés individuelles et en a fait une priorité depuis l'affaire Snowden de 2013[52].

Le système réglementaire américain est à la fois plus complexe et moins rigoureux que celui de l'UE, en grande partie à cause du système fédéral et de la nécessaire coordination entre les institutions au niveau fédéral et au niveau des États.

Certains secteurs industriels sont soumis à des obligations de déclaration propres qui précèdent les exigences fédérales, et certaines entreprises peuvent également être confrontées à des obligations au niveau de chaque État en plus des obligations fédérales[53]. Bien que l'on sache clairement quelles sont les organisations qui relèvent de la catégorie des « infrastructures critiques[54] », le cadre réglementaire reste opaque car les obligations spécifiques de protection des infrastructures critiques et des données des clients ne sont pas fermement définies. La réglementation actuelle permet notamment l'élaboration de profilage numérique des citoyens, qui sont régulièrement vendus à des annonceurs numériques, ce qui rend les données vulnérables aux pirates informatiques.

51. Ce rapport compare les réglementations israélienne et américaine au NIS, le NIS2 n'étant pas encore entré en vigueur.
52. Israel Defense Forces and National Cyber Defense, Tabansky, URL.
53. La loi de 2014 sur la modernisation de la sécurité des informations fédérales (FISMA) en est un exemple.
54. Aux États-Unis, les organisations d'infrastructures critiques sont définies comme suit : voir ici.

COMPARAISON DE LA CYBERSÉCURITÉ
DANS L'UE, AUX ÉTATS-UNIS ET EN ISRAËL

CRITÈRE	NIS UE	CADRE AMÉRICAIN	CADRE ISRAËLIEN
Réponse aux incidents CERT/CSIRT	Exige que les États membres soient équipés de manière appropriée, par exemple, avec une équipe de réponse aux incidents de sécurité informatique (CSIRT) et une autorité nationale compétente en matière de NIS.	La loi de 2014 sur la modernisation de la sécurité des informations fédérales (FISMA 2014) codifie l'US-CERT comme une fonction du DHS.	La résolution 2444, Advancing the National Preparedness for Cyber Defense, établit l'Agence nationale de cybersécurité (NCSA) qui est chargée de maintenir le CERT d'Israël.
Coopération	Assure la coopération entre les États membres en créant un groupe de coopération chargé de soutenir et de faciliter la coopération stratégique et l'échange d'informations.	La loi de 2018 sur l'Agence pour la cybersécurité et la sécurité des infrastructures fait de la coopération et du partage d'informations une mission essentielle de la CISA. L'*Executive Order on Improving the Nation's Cybersecurity* de 2021 [ordre exécutif sur l'amélioration de la cybersécurité de la nation] augmente le partage d'informations entre les fournisseurs de services informatiques fédéraux (contractants) et les agences gouvernementales concernées.	Aucune réglementation officielle en matière de coopération. Mais Israël donne la priorité à la coopération multipartite en matière de cybersécurité entre les gouvernements, le monde universitaire et les entités du secteur privé. En témoigne l'initiative CyberSpark qui a contribué à transformer Be'er Sheva en un centre majeur de cybersécurité.
Identification et classification des infrastructures critiques	Impose aux organisations visées de prendre des mesures de sécurité appropriées et de notifier les incidents graves à l'autorité nationale compétente.	La loi sur le rapport de cyber-incidents pour les infrastructures critiques de 2022 (CIRCIA) fixe des exigences en matière de déclaration des incidents ; les règles finales sont encore en cours d'élaboration. Le *Computer Security Incident Notification Requirements for Banking Organisations and Their Bank Service Providers* (2021) définit les exigences de notification pour le secteur bancaire.	Le règlement sur la protection de la vie privée (sécurité des données) dispose que les propriétaires de bases de données classées dans un niveau de sécurité "intermédiaire" ou "élevé" sont tenus de notifier les violations de données à la PPA (loi israélienne sur la protection de la vie privée, mise en œuvre par le règlement sur la protection de la vie privée).
Objectifs	Prévenir les risques et assurer la sécurité du réseau et des systèmes d'information.	La loi fédérale sur la modernisation des systèmes d'information (FISMA) de 2014 établit le rôle central de la CISA dans la sécurité des informations et des systèmes d'information des organismes fédéraux, exécutifs et civils. Il n'existe pas à ce jour de politique équivalente dans le secteur privé. La CISA est chargée du partage d'informations avec le secteur privé et est responsable de la cybersécurité des infrastructures critiques.	Le règlement sur la protection de la vie privée (sécurité des données) exige que toute personne qui possède, gère ou maintient une base de données contenant des données personnelles mette en œuvre diverses pratiques de sécurité de l'information, notamment l'enregistrement de la base de données, le maintien de contrôles de sécurité et l'adhésion à d'autres règlements.

PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

Le GDPR a eu un impact considérable sur l'amélioration de la protection de la confidentialité des données au niveau mondial.

L'intégration du droit à la vie privée dans la Convention européenne des droits de l'homme pose les bases du droit du citoyen à la vie privée numérique dans l'UE. Le RGDP consacre ce droit dans toute l'Union européenne, en étendant l'obligation de protéger les données des utilisateurs à toutes les entreprises opérant dans l'UE, même si elles sont situées ailleurs. Le RGDP a eu des répercussions considérables sur une meilleure protection de la confidentialité des données à l'échelle mondiale[55]. La diversité des approches en matière de réglementation de la protection de la vie privée en dehors de l'UE peut toutefois être source de confusion pour les utilisateurs.

COMMENT LA VIE PRIVÉE DES CITOYENS EST-ELLE PROTÉGÉE EN DEHORS DE L'UE ?

Les cadres réglementaires sur la protection des données et la vie privée dans le monde diffèrent largement[56]. Certains pays ont modelé leurs lois sur le RGDP, en s'appuyant sur les huit droits fondamentaux des utilisateurs définis par le RGDP[57] :

1. Le droit d'être informé
2. Le droit d'accès aux données
3. Le droit de rectification des données
4. Le droit à l'effacement des données
5. Le droit de restreindre le traitement de données
6. Le droit à la portabilité des données
7. Le droit d'opposition
8. Droits relatifs à la prise de décision automatisée et au profilage.

Israël et le Canada se distinguent par leur avancement en matière de cybersécurité, mais semblent comparativement plus faibles en ce qui concerne la vie privée des citoyens : Israël ne fait que confirmer les droits d'accès, de rectification et desuppression des informations personnelles ; le Canada va un peu plus loin en autorisant également le droit de restreindre le traitement des données.

Pourtant, ni l'un ni l'autre ne confirme le droit à la portabilité des données, ne fixe de limite d'âge pour le consentement dans la législation nationale sur la protection de la vie privée, ni ne prévoit de droit à ne pas être soumis à des décisions entièrement automatisées.

Les États-Unis se distinguent également par le fait qu'il n'existe pas de politique unique de protection de la vie privée au niveau fédéral. Certaines politiques en place concernent les informations de santé personnelles[58], les informations bancaires personnelles[59], et la vie privée en ligne des enfants[60]. Mais pour l'essentiel, les protections de la vie privée ont été adoptées au niveau des États. La Californie, le Colorado, l'Utah et la Virginie ont adopté et sont en train de mettre en œuvre des lois sur la protection de la vie privée similaires au RGDP, y compris généralement les mêmes protections pour les droits individuels à la confidentialité des données. Mais en raison d'un cadre de protection de la vie privée fragmenté[61], les entreprises américaines ont été lentes à adopter des mesures, et la protection des données reste secondaire par rapport aux intérêts commerciaux.

L'APPROCHE DU SECTEUR PRIVÉ

Le paysage des cybermenaces s'est considérablement élargi et les citoyens disposent de peu d'options pour contrôler les données qu'ils partagent et limiter leurs vulnérabilités en ligne. Les fabricants et les fournisseurs ont la responsabilité de concevoir des produits et des services en tenant compte de la sécurité et de la vie privée des citoyens.

Les appareils intelligents ont fait apparaître une nouvelle couche de vulnérabilité. Les montres intelligentes, les trackers de fitness, les sonnettes, les haut-parleurs ou les assistants virtuels peuvent entraîner des pertes de données, notamment de mots de passe ou d'images. Ces données peuvent être utilisées pour compromettre des appareils interconnectés ou être vendues à des acteurs criminels. En outre, les citoyens partagent souvent plus de données qu'ils ne le pensaient et peuvent, sans le savoir, donner leur accord pour que le fabricant ou le fournisseur de services puisse vendre ces données. Celles-ci peuvent être rendues publiques à leur insu, manipulées et utilisées à mauvais escient.

55. What is GDPR, the EU's new data protection law?, GDPR.EU, URL.
56. Global Comprehensive Privacy Law Mapping Chart, IAPP, URL.
57. What is GDPR, the EU's new data protection law?, GDPR.EU, URL.
58. Your rights under HIPAA, US Department of Health & Human Services, URL.
59. The Right to Financial Privacy Act, EPIC, URL
60. Children's Online Privacy Protection Rule («COPPA»), US Federal Trade Commission, URL.
61. Divided we fall: Why fragmented global privacy regulation won't work, Kieran, URL.

SÉCURITÉ

PROBLÈME

Dans le monde actuel marqué par la généralisation du travail à distance, la dépendance croissante à l'égard du *cloud computing*, et l'utilisation professionnelle d'appareils personnels, les moyens traditionnels de sécurisation des systèmes informatiques (par exemple via un VPN ou un pare-feu de l'entreprise) ne suffisent plus. Le "périmètre de sécurité" s'est élargi.

BONNE PRATIQUE

ARCHITECTURE ZERO TRUST[62] : L'architecture zéro trust (ZTA) est un modèle de sécurité réseau dans lequel l'accès aux services ou systèmes informatiques est soumis à une stricte authentification et vérification. Le ZTA est conçue pour prévenir les violations de données au niveau interne d'une entreprise[63] : si les utilisateurs internes ont accès à l'environnement de données, ils peuvent ne pas avoir accès aux données sensibles.

SÉCURITÉ

PROBLÈME

La sécurité a longtemps été une réflexion conduite après la conception des logiciels et du matériel. Cela conduit à des produits plus faibles et plus vulnérables aux attaques et aux violations.

BONNE PRATIQUE

LA SÉCURITÉ DÈS LA CONCEPTION (*« SECURITY BY DESIGN »*) : Cette pratique implique que les fabricants intègrent dès le départ des fonctions de sécurité dans les logiciels et le matériel. En substance, la sécurité dès la conception doit suivre cinq principes généraux[64].

- Le contexte doit être établi pour déterminer tous les éléments qui composent le système, afin d'éviter les angles morts dans les mesures défensives ;
- Le système doit être conçu pour rendre la compromission difficile. Il doit notamment être résistant aux attaques par déni de service (DoS) et aux pics d'utilisation. Il doit également faciliter la détection de la compromission et identifier les activités suspectes lorsqu'elles se produisent.
- Le système doit être conçu de manière à réduire l'impact de la compromission si un attaquant parvient à prendre pied.

Les solutions développées par Apple, par exemple, intègrent le principe de "*security by design*" : l'entreprise propose des produits qui sont déjà équipés de systèmes de sécurité réseau afin de prévenir les vulnérabilités[65].

Les citoyens sont le maillon faible de la cybersécurité, et la sécurité par la conception peut grandement contribuer à améliorer leur protection.

SÉCURITÉ & VIE PRIVÉE

PROBLÈME

Trop d'informations personnelles et de données de valeur sont stockées en clair, ce qui permet aux pirates de voler, d'utiliser ou de vendre plus facilement les données après une violation.

BONNE PRATIQUE

CHIFFREMENT DES DONNÉES ET *SANDBOXING* : Le chiffrement peut rendre l'accès aux données plus difficile pour les pirates après une violation, tandis que le *sandboxing* limite l'accès aux données. Le chiffrement est essentiel, d'autant que de nombreux dispositifs utilisent désormais des informations personnelles identifiables (IPI), y compris des données biométriques.

Le *sandboxing* des données implique la mise en œuvre de permissions sélectionnées qui définissent les personnes autorisées à accéder à certaines données, limitant ainsi l'exposition en cas de cyberattaque. Si les citoyens n'ont pas besoin de comprendre les détails du chiffrement ou du *sandboxing*, ils doivent être informés de la valeur ajoutée de ces pratiques pour leur sécurité.

SÉCURITÉ & VIE PRIVÉE

PROBLÈME

De nombreux appareils IoT utilisent des mots de passe par défaut et les citoyens ne savent pas forcément qu'ils doivent les changer. Les mots de passe faibles restent le meilleur moyen d'accéder et de voler des données.

BONNE PRATIQUE

MOTS DE PASSE UNIQUES ET AUTHENTIFICATION MULTIFACTORIELLE (AMF) :
L'industrie pourrait contribuer à la protection des citoyens en supprimant les mots de passe par défaut sur leurs produits, et en exigeant l'utilisation de mots de passe uniques et forts. L'AMF ajoute une couche de sécurité supplémentaire qui rend plus difficile l'accès d'un attaquant à un compte ou à un appareil.

62. Le modèle Zero Trust, ANSSI, URL.
63. Zero Trust Architecture, Rose et al., URL
64. Secure design principles, UK National Cyber Security Centre (NCSC), URL.
65. Aperçu de la sécurité matérielle, Apple, URL.

VIE PRIVÉE

PROBLÈME

Les entreprises collectent et utilisent les données des citoyens à des fins autres que celles strictement nécessaires, notamment pour les vendre ou les exploiter à des fins de marketing.

BONNE PRATIQUE

RGDP[66] & POLITIQUES DE CONFIDENTIALITÉ CENTRÉES SUR LE CITOYEN :
Se conformer au RGDP implique de :

- Garantir le « droit à l'oubli », c'est-à-dire que les citoyens peuvent contrôler leurs données et demander leur suppression.
- Stocker les données uniquement dans les pays qui ont mis en œuvre le RGDP, et donc respecter le droit de ne pas vendre les données du citoyen.

Pour les citoyens, une politique de confidentialité plus faible signifie que leurs données sont souvent utilisées à leur insu, ce qui entraîne à son tour un risque d'exposition au vol de données. Les citoyens peuvent utiliser des services VPN conformes au RGDP, qui sont moins susceptibles d'enregistrer des informations inutiles et qui limiteront les informations que leur FAI peut collecter. Mais les VPN peuvent ajouter un coût et une charge supplémentaire pour les citoyens.

En ce qui concerne les médias sociaux en particulier, des plateformes comme Facebook ont mis en place des contrôles supplémentaires de la vie privée pour les citoyens, mais ils sont compliqués, difficiles d'accès, et la méfiance demeure quant à la volonté de la plateforme de limiter le suivi et de respecter les droits des citoyens.

VIE PRIVÉE

PROBLÈME

Pendant trop longtemps, la confidentialité des données a été une préoccupation secondaire dans le développement des systèmes d'information. Conséquences : des pratiques peu rigoureuses en matière de protection de la vie privée qui nécessitent l'élaboration a posteriori de solutions permettant d'adapter les produits aux nouvelles normes de protection des données.

BONNE PRATIQUE

LE RESPECT DE LA VIE PRIVÉE DÈS LA CONCEPTION ET « PAR DÉFAUT » :
Tout comme la sécurité « by design » qui doit être intégrée dès la conception des produits, la protection de la vie privée « by design » implique que la protection de la vie privée est prise en compte dès la conception des systèmes et process numériques. Cette approche garantit par exemple que les produits sont conformes au RGDP et que les droits des personnes concernées sont protégés.

Imposer le respect de la vie privée « par défaut » implique que toute entité traitant des données à caractère personnel doit veiller à ce qu'elles ne soient pas traitées inutilement. Par exemple, les paramètres par défaut d'un réseau social doivent garantir que les informations collectées, partagées ou affichées ne dépassent pas le strict nécessaire. Ce dispositif protège les citoyens en garantissant que, même en cas de partage d'IPI ou d'autres informations précieuses, seul le minimum est suivi, stocké ou partagé.

PROTÉGER LES CITOYENS : L'UNION EUROPÉENNE EN FAIT-ELLE ASSEZ ?

Les citoyens européens ne sont peut-être pas directement au cœur de la réglementation actuelle de l'UE et des États membres en matière de cybersécurité, mais ils sont plus en sécurité et leurs droits sont mieux protégés qu'ailleurs dans le monde. Si les entreprises doivent globalement améliorer leur niveau de cybersécurité, les efforts doivent également porter sur les appareils et les services que les citoyens utilisent au quotidien. La loi sur la cyber-résilience pourrait être une bonne première étape pour garantir une couche supplémentaire de protection. Cependant, toute nouvelle réglementation représente probablement une charge financière et de mise en conformité importante pour les entreprises, et un soutien devra être mis à leur disposition pour en assurer une mise en œuvre rapide.

66. Complete guide to GDPR compliance, GDPR.EU, URL.

AUX ARMES CITOYENS !

DONNER AUX CITOYENS LES MOYENS D'ASSURER LEUR PROPRE SÉCURITÉ

Malgré un cadre réglementaire qui concerne principalement les gouvernements et les infrastructures critiques, de nombreuses initiatives ont été lancées pour replacer les citoyens au cœur de la cybersécurité.

La responsabilité de cybersécurité ne peut en effet pas uniquement reposer sur les gouvernements et les entreprises : les citoyens doivent jouer un rôle de premier plan dans la sécurisation de leurs propres données et dans leur propre protection en cas d'attaques. En tant que potentielles victimes, les citoyens doivent donc être informés des mesures d'atténuation et de réponse à déployer en cas d'attaque. Malheureusement, seule une personne sur trois interrogée dans le cadre du sondage réalisé par le FIC se souvient avoir vu ou entendu parler d'une campagne de sensibilisation, ce qui signifie que la plupart d'entre eux ne sont probablement pas informés des ressources dont ils disposent pour assurer leur propre cyber sécurité[67].

Il existe en fait de nombreuses initiatives gouvernementales, ou issues de la société civile et du secteur privé, conçues pour avancer vers une société numériquement sûre. Ces initiatives peuvent être réparties en deux grandes catégories :

- **Prévention:** initiatives visant à aider les utilisateurs à se préparer et à prévenir une cyberattaque ou une violation de données, et
- **Atténuation et réponse :** initiatives qui aident les utilisateurs à réagir et à agir en cas de cyber-attaque.

MIEUX VAUT PRÉVENIR QUE GUÉRIR

Le vieil adage « mieux vaut prévenir que guérir » se vérifie aussi en matière de cybersécurité. La plupart des gouvernements ont ainsi lancé des programmes destinés à former, informer et protéger les citoyens sur Internet. Ces programmes s'ajoutent au soutien qu'offrent déjà ces gouvernements aux entreprises et aux opérateurs d'infrastructures critiques.

67. Enquête OpinionWay pour le FIC réalisée en septembre 2022, URL.

LES INITIATIVES DES GOUVERNEMENTS NATIONAUX

La sélection d'initiatives gouvernementales ci-dessous liste les projets qui visent à renforcer la responsabilisation des citoyens dans le cyber espace.

	FRANCE	BELGIQUE	ESPAGNE	ROYAUME-UNI	ÉTATS-UNIS
Sensibilisation	**Hack Academy :** Une initiative d'intérêt public soutenue par l'ANSSI et le ministère de l'Intérieur qui utilise l'humour pour former les utilisateurs aux cyber-risques quotidiens et aux moyens de s'en protéger.	**KIT Cyber Security :** Ce kit d'outils, créé par la Cyber Security Coalition et le Centre pour la Cybersécurité Belgique (CCB), vise à sensibiliser les PME et autres organisations à la cybersécurité.	**Internet Security 4 Kids (IS4K) :** Ce site axé sur la sensibilisation des enfants, créé par l'INCIBE, le ministère des affaires économiques et de la transformation numérique et d'autres partenaires, propose tout ce dont les parents ont besoin pour assurer la sécurité de leurs enfants en ligne. Il comprend des guides (contrôle parental, harcèlement en ligne, etc.), des outils (quizz et jeux), etc.	**Cyber Aware :** Le Centre national de cybersécurité du Royaume-Uni donne des conseils sur la manière de rester en sécurité dans ses activités en ligne. Ce site aide les utilisateurs à rendre leurs services numériques plus sûr	**Programme de sensibilisation à la cybersécurité :** Un effort national de sensibilisation du public visant à améliorer la compréhension des cybermenaces et à donner au public américain les moyens d'évoluer de façon sécurisé en ligne.
Formations	**CyberEdu :** Une initiative de formation lancée par l'ANSSI, qui vise à renforcer la prise en compte de la sécurité numérique dans toutes les formations supérieures françaises en informatique afin de construire une société mieux sensibilisée aux enjeux de cybersécurité.		**Cours gratuits en ligne sur la cybersécurité :** INCIBE propose des cours sur la cybersécurité gratuits pour les indépendants et les micro-entreprises, et fournit de la documentation aux enseignants et aux parents. Elle publie également des guides sur la confidentialité et la sécurité en ligne.		
Jeux		**SafeonWeb.Be :** Un centre qui offre notamment des ressources, afin d' aider à prévenir les cyber-attaques et à réagir après un piratage. Safeonweb comprend également des quizz.	**Ciberemprende :** Ce programme d'INCIBE vise à attirer des talents innovants dans le domaine de la cybersécurité en organisant un concours d'idées et de projets entrepreneuriaux en phase d'amorçage, afin de les aider à les développer.	**CyberSprinters :** Un jeu numérique pour les 7-11 ans qui peut être utilisé sur des téléphones, des tablettes et des ordinateurs, et qui est accompagné d' activités pour le personnel enseignant. Les parents et les accompagnateurs peuvent également utiliser les puzzles CyberSprinter avec leurs enfants à la maison.	**Le défi cybernétique de la Coupe du Président :** Le CISA dirige et accueille la President's Cup pour identifier, reconnaître et récompenser les meilleurs cyber talents à travers les États-Unis. Les défis sont basés sur des mises en situations réelles du cadre de l'initiative nationale pour l'éducation à la cybersécurité (NICE), afin de favoriser la montée en compétences par le biais de tests ludiques et créatifs.
Autres	**Visa de sécurité ANSSI :** Permet aux utilisateurs de d'identifier les produits ou services rigoureusement testés, certifiés et approuvés par l'ANSSI.	**Application SafeonWeb :** Le CCB a développé une application qui permet aux utilisateurs d'enregistrer leurs réseaux domestiques et de recevoir des notifications si une menace a été détectée. Les utilisateurs peuvent également recevoir des mises à jour régulières qui les informent des cybermenaces en Belgique.	**Centre de cyberdéfense active (ACD) :** Le programme ACD vise à réduire les dommages causés par les cyber-attaques en fournissant aux utilisateurs éligibles des outils et des services qui les protègent contre certaines attaques.		

LES INITIATIVES DE L'INDUSTRIE

Certaines entreprises ont lancé des initiatives de formation à la cybersécurité à l'attention des utilisateurs, souvent dans le cadre de programmes de responsabilité sociale des entreprises. D'autres proposent également des produits gratuits à leurs utilisateurs (exemple : Bitwarden). Ces initiatives ont tendance à se concentrer sur la formation de la prochaine génération de professionnels de la cybersécurité, mais elles offrent également des possibilités à ceux qui souhaitent changer de carrière ou acquérir de nouvelles compétences. En voici quelques exemples :

FORMATION

- *Orange CyberDefense #SuperCoders*[68]: Orange Cyber Defense organise des ateliers pour les enfants âgés de 9 à 14 ans afin de les initier au codage. Grâce à ce programme, les enfants apprennent les bases du codage, les bonnes pratiques de sécurité sur internet et à agir de manière responsable dans l'espace numérique.
- *Samsung Solve for Tomorrow*[69]: Ce concours destiné aux collégiens et lycéens des États-Unis encourage les participants à résoudre les problèmes de leur communauté à l'aide de la technologie. Ce programme stimule l'engagement communautaire et encourage l'investissement dans l'enseignement des STEM (Science, technologie, ingénieurie et mathématiques) afin de contribuer à la montée en compétence de cette génération. Les élèves reçoivent également une formation de base en technologie, qui comprend les meilleures pratiques en matière de cybersécurité.
- *Microsoft Philanthropies Technology Education and Literacy in Schools (TEALS)*[70]: Cette initiative élabore des programmes informatiques dans les lycées en zone isolée en aidant les enseignants à enseigner l'informatique. En outre, Microsoft se concentre sur la formation à l'alphabétisation et l'aide à l'acquisition de compétences numériques et technologiques pour réduire la fracture numérique.
- *Samsung Innovation Campus*[71]: le Samsung Innovation Campus dispense un enseignement sur le numérique aux étudiants et aux jeunes sans emploi. Outre les compétences de base telles que l'IA, l'IoT, le Big Data, le codage et la programmation, le programme forme les participants à une série de compétences non techniques.

FORMATION - FEMMES & MINORITÉS

- *Orange CyberDefense Women's Digital Centres programme*[72]: Ce programme a développé des "Centres numériques" en Europe et en Afrique pour former des femmes sans qualification ni emploi. La formation dure de six mois à un an et permet d'acquérir des compétences essentielles comme les mathématiques, l'écriture, l'utilisation d'ordinateurs et de tablettes, de logiciels et d'internet. Ce programme permet de lutter contre l'écart entre les sexes dans le domaine de la technologie et de former des citoyens plus avertis en matière de numérique.
- *Programme d'inclusion numérique de Capgemini*[73]: Ce programme vise à jeter un pont entre la technologie et la société, et travaille en étroite collaboration avec des ONG, des organisations d'innovation sociale et des clients à travers quatre grands axes : (1) Digital Literacy, (2) Digital Academy, (3) Tech4Positive Futures et (4) Advocacy & Thought Leadership. Pour soutenir l'alphabétisation numérique, Capgemini fournit des équipements électroniques et enseigne des compétences numériques de base. Il permet également aux utilisateurs d'acquérir les bonnes pratiques de base en matière de cybersécurité, comme la bonne gestion des mots de passe.
- *Google "Code with Google"*[74]: Le programme phare de Google développe l'enseignement de l'informatique au sein des communautés en zone isolée.

ACCESSIBILITÉ

- *Google soutient "Newswise"*[75]: Google collabore avec Newswise pour offrir aux jeunes une formation à l'éducation aux médias, afin de les aider à repérer la désinformation en ligne, à distinguer les vraies sources d'information des fausses.
- Certificats de carrière Google[76]: Google soutient des programmes de formation en ligne permettant d'acquérir des compétences professionnelles dans des domaines à forte croissance tels que l'analyse des données, le marketing numérique et le e-commerce, l'assistance informatique, la gestion de projet et la conception UX. Ces programmes sont accessibles au public sur Coursera.org.

Outre les programmes lancés par les entreprises, certaines associations du secteur de la cybersécurité ont lancé des initiatives liées à la sensibilisation, à la formation des jeunes et à la parité. L'Organisation européenne de cybersécurité (ECSO)[77], par exemple, soutient divers programmes de formation et de sensibilisation, dont son initiative Youth4Cyber. Cette initiative vise à élever le niveau d'hygiène numérique et à susciter l'intérêt des jeunes Européens pour les carrières dans le domain de la cybersécurité, grâce à des modules adaptés à leur âge, à leurs besoins et à leurs intérêts. Les associations sectorielles ont tendance à concentrer leurs efforts sur des initiatives orientées vers les entreprises, qui doivent profiter à leurs propres membres.

68. #SuperCoders: Corporate Social Responsibility, Orange, URL.
69. Thriving together: Samsung CSR US, URL.
70. TEAL Program, Microsoft, URL.
71. Cultivate key human resources who will lead the 4th Industrial Revolution, Samsung, URL.
72. The Women's Digital Centres programme: actively supporting women's empowerment, Fondation Orange, URL.
73. Capgemini - Social, Capgemini, URL.
74. Code with Google, Google, URL.
75. Philanthropic initiatives for local communities, Google, URL.
76. Google Career Certificates, Google, URL.
77. European Cyber Security Organisation (ECSO) - About, ECSO, URL.

ORGANISATIONS DE LA SOCIÉTÉ CIVILE

Un nombre croissant d'organisations de la société civile proposent des outils pour aider les utilisateurs à se protéger contre les cybermenaces. Il s'agit, entre autres, de :

- ***Global Cyber Alliance (GCA) :*** La GCA propose diverses boîtes à outils de cybersécurité pour faciliter la recherche et la mise en œuvre d'audits de cybersécurité, afin d'aider les organisations et les citoyens à se défendre contre les cybermenaces. Elle propose également des formations pour aider les citoyens à améliorer leur sécurité numérique et à protéger leur vie privée. En outre, elle a publié un guide de mise en œuvre de la norme DMARC (Domain-based Message Authentication, Reporting and Conformance), disponible en 18 langues. La GCA a également lancé Quad9, un service gratuit que les utilisateurs peuvent installer pour bloquer l'accès aux sites Web malveillants, contribuant ainsi à protéger les utilisateurs contre l'exposition involontaire de leurs données.
- ***National Cybersecurity Alliance :*** La NCA propose plusieurs ressources permettant aux utilisateurs d'améliorer leur cybersécurité. Elle publie des guides sur tous les sujets, des mots de passe et gestionnaires de mots de passe jusqu'au phishing et à la détection des virus sur les ordinateurs personnels. La NCA propose également des formations et des conseils en matière de gestion des carrières pour tous ceux travaillant ou souhaitant travailler dans le domaine de la cybersécurité, contribuant ainsi à pallier en partie au manque de ressources humaines et de combler le manque de professionnels du secteur.
- ***Cyber Peace Institute :*** Le Cyber Peace Institute propose des solutions de cybersécurité aux organismes à but non lucratif pour les aider à se protéger contre les cybermenaces, par exemple dans le secteur de la santé. Le CPI publie le Cyber Incident Tracker (CIT) #HEALTH, pour aider à identifier et à suivre les cybermenaces croissantes pour les organisations de santé.
- ***Center for Internet Security (CIS) :*** Le CIS est surtout connu pour avoir publié les 18 Critical Security Controls®. Ces contrôles sont conçus pour protéger les entreprises, mais certains peuvent être mis en œuvre par les particuliers pour mieux protéger leurs systèmes domestiques et leurs données personnelles. Les contrôles reprennent des bonnes pratiques développées par un consortium d'experts industriels, universitaires et gouvernementaux.

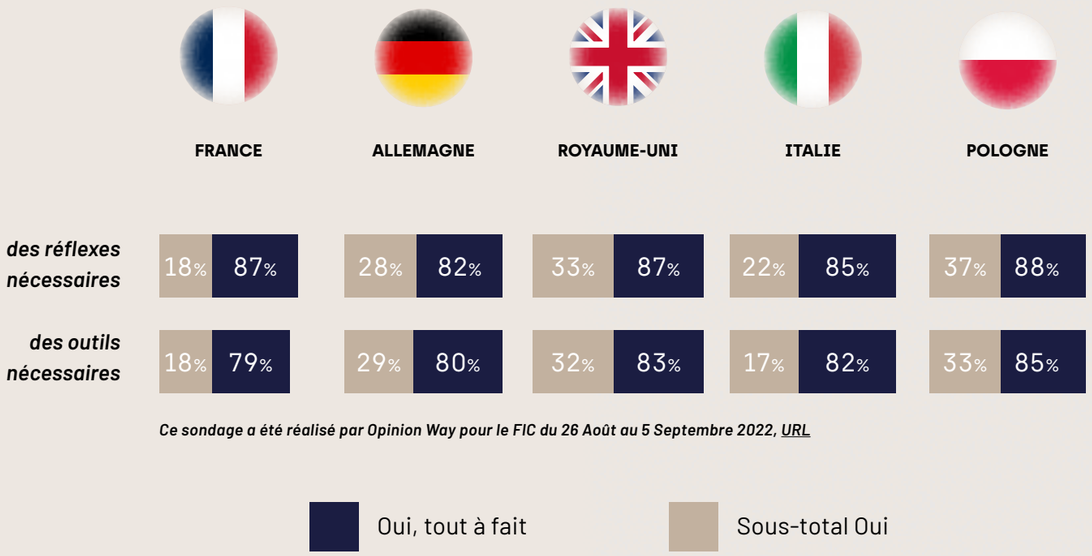
AIDER LES CITOYENS À PRÉVENIR LES CYBER-ATTAQUES

- Lancés par les gouvernements, les entreprises et les organisations de la société civile, de nombreux outils sont disponibles pour protéger les citoyens contre les cyber-attaques.
- L'industrie s'est attachée à aider les citoyens à sécuriser leurs équipements, mais elle pourrait faire davantage pour créer des produits sécurisés dès leur conception.
- L'industrie contribue à former la prochaine génération de professionnels de la cybersécurité, mais des partenariats supplémentaires avec les gouvernements et les organisations de la société civile pourraient renforcer ces efforts.

PAS DE PANIQUE ! RÉPONSES AUX CYBER-ATTAQUES

COMME LE RÉVÈLE L'ENQUÊTE EXCLUSIVE DU FIC, LES UTILISATEURS ESTIMENT GÉNÉRALEMENT DISPOSER DES OUTILS ET DES COMPÉTENCES NÉCESSAIRES POUR SE PROTÉGER EN LIGNE ET PRÉVENIR UNE CYBERATTAQUE[78].

POUR ASSURER VOTRE SÉCURITÉ, DISPOSEZ-VOUS... ?



Ce sondage a été réalisé par Opinion Way pour le FIC du 26 Août au 5 Septembre 2022, URL

Ils sont toutefois moins sûrs de la façon dont ils doivent réagir lorsqu'ils découvrent que leurs informations (mots de passe, numéros d'identification, autres IPI) ont pu être compromises. Les organisations, en particulier dans le secteur privé, restent réticentes à admettre les violations de données et peuvent donc tarder à en informer les autorités et leurs clients, ce qui complique d'autant plus la tâche des citoyens qui souhaitent prendre les mesures appropriées. Quelques conseils et initiatives sont disponibles pour soutenir les citoyens, principalement de la part des gouvernements et des organisations de la société civile.

78. Enquête OpinionWay pour le FIC réalisée en septembre 2022, URL.

AU NIVEAU DES GOUVERNEMENTS

Vous trouverez ci-dessous une sélection d'initiatives gouvernementales au niveau national qui visent à renforcer le pouvoir des citoyens.

FRANCE

Site web Cybermalveillance et outil de diagnostic de l'ANSSI : L'Agence nationale de la sécurité des systèmes d'information (ANSSI) (agence nationale française de cybersécurité) a mis en place un site web permettant aux citoyens de s'informer sur les cyber-attaques. Les utilisateurs répondent à une série de questions pour décrire le problème, puis se voient proposer des recommandations personnalisées sur la manière de gérer la situation. L'outil peut également recommander des prestataires locaux spécialisés et agréés par Cybermalveillance.gouv.fr si nécessaire.

BELGIQUE

Dans le cadre du portail en ligne **SafeonWeb** le Centre pour la cybersécurité en Belgique propose une section "Premiers secours" destinée à aider les citoyens confrontés à des problèmes spécifiques de cybersécurité. Les utilisateurs peuvent notamment vérifier si leurs données ont été volées et recevoir des conseils sur les prochaines étapes, trouver des informations pour réduire la quantité de spams et d'e-mails de phishing qu'ils reçoivent, et obtenir des conseils sur la marche à suivre en cas de détection de virus.

SUÈDE

La Suède propose plusieurs guides sur la marche à suivre en cas de piratage ou de cyberattaque, sur le site web **www.sakerhetskollen.se**. Ces guides aident les utilisateurs à repérer les signaux pouvant indiquer que leurs informations ou leur système ont pu être compromis, et fournissent des instructions étape par étape sur la marche à suivre et la façon de gérer la situation.

AUSTRALIE

L'Australie propose via le site www.cyber.gov.au, des aides pour trouver l'accompagnement adapté en fonction du type de cyberattaque subie. Outre des guides et instructions permettant de récupérer des comptes compromis ou d'apprendre à réagir en cas de données personnelles compromises, ils proposent un **quizz de 2 minutes** destiné à aider les utilisateurs à déterminer s'il a été piraté. Le quizz se termine par des conseils détaillés sur les prochaines étapes à suivre.

LE SECTEUR PRIVÉ

De nombreux acteurs du secteur privé proposent des services payants pour accompagner les citoyens dans leur réponse aux cyber-attaques ou aux violations de données. En raison de la croissance rapide de ces offres, il peut être difficile de distinguer les services et les entreprises de bonne réputation. Le système européen de certification de la cybersécurité sera essentiel pour aider les citoyens à savoir à quels produits et services se fier. En attendant, les systèmes nationaux de certification de la cybersécurité peuvent constituer un guide utile. Le « Visa de sécurité » de l'ANSSI[79], par exemple, qualifie et vérifie les solutions de sécurité au moyen de tests rigoureux effectués par des tiers.

LES ORGANISATIONS DE LA SOCIÉTÉ CIVILE

- ***National Cybersecurity Alliance :*** La NCA partage ici la marche à suivre pour signaler aux autorités des activités cybercriminelles, et des conseils sur les mesures à adopter en cas de piratage pour répondre à l'attaque.
- ***Have I Been Pwned (HIBP) :*** Ce site web aide les utilisateurs à identifier si leur adresse électronique ou leur numéro de téléphone a été compromis dans le cadre d'une violation de données.
- ***Forum des équipes de sécurité et de réponse aux incidents (FIRST) :*** FIRST est un consortium d'équipes de sécurité et de réponse aux incidents destiné à faciliter le partage d'informations et l'élaboration de politiques et de réglementations mondiales. Il propose un service de notification des victimes en cas de violation des données. Les utilisateurs peuvent enregistrer leur(s) adresse(s) IP et leur numéro de système autonome (ASN) pour recevoir une notification automatique en cas de violation. Bien que destiné aux gestionnaires de systèmes, il est ouvert à tous et pourrait constituer une solution pour les alertes précoces sur les cybermenaces, permettant une réponse plus rapide.

UN MANQUE DE RESSOURCES POUR RÉPONDRE AUX CYBERATTAQUES

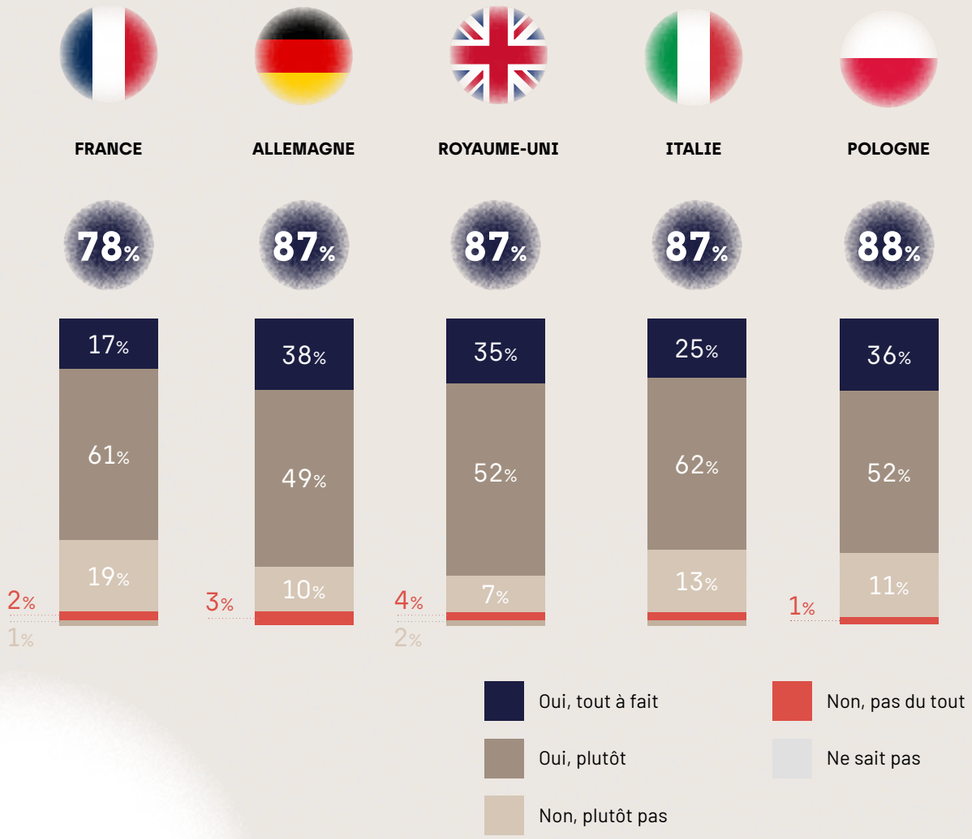
- **Les gouvernements, les entreprises et les organisations de a société civile proposent de nombreuses solutions aux utilisateurs victimes de cyberattaques.**
- **Les gouvernements montrent l'exemple en proposant des lignes d'assistance et des ressources fiables, mais il est possible de faire davantage pour aider les citoyens à connaître et à utiliser ces services.**

79. Security Visa, ANSSI, URL.

SOYEZ PRUDENTS ! ACCROÎTRE LA SENSIBILISATION À LA CYBERSÉCURITÉ

L'environnement réglementaire a évolué rapidement et commence à s'intéresser à la cybersécurité de tous. Les initiatives et les solutions des gouvernements, de l'industrie et des organisations de la société civile portent sur de multiples aspects de la cybersécurité et offrent aux citoyens des solutions aux problèmes les plus courants. Il est donc logique qu'un nombre écrasant d'utilisateurs, 85 % des personnes interrogées dans un sondage réalisé par le FIC, se sentent en sécurité en ligne[80].

EN GÉNÉRAL, SENTEZ-VOUS EN SÉCURITÉ QUAND VOUS UTILISEZ VOS OUTILS NUMÉRIQUES (TÉLÉPHONE PORTABLE, ORDINATEUR, WEBCAM, OBJETS CONNECTÉS...) ?



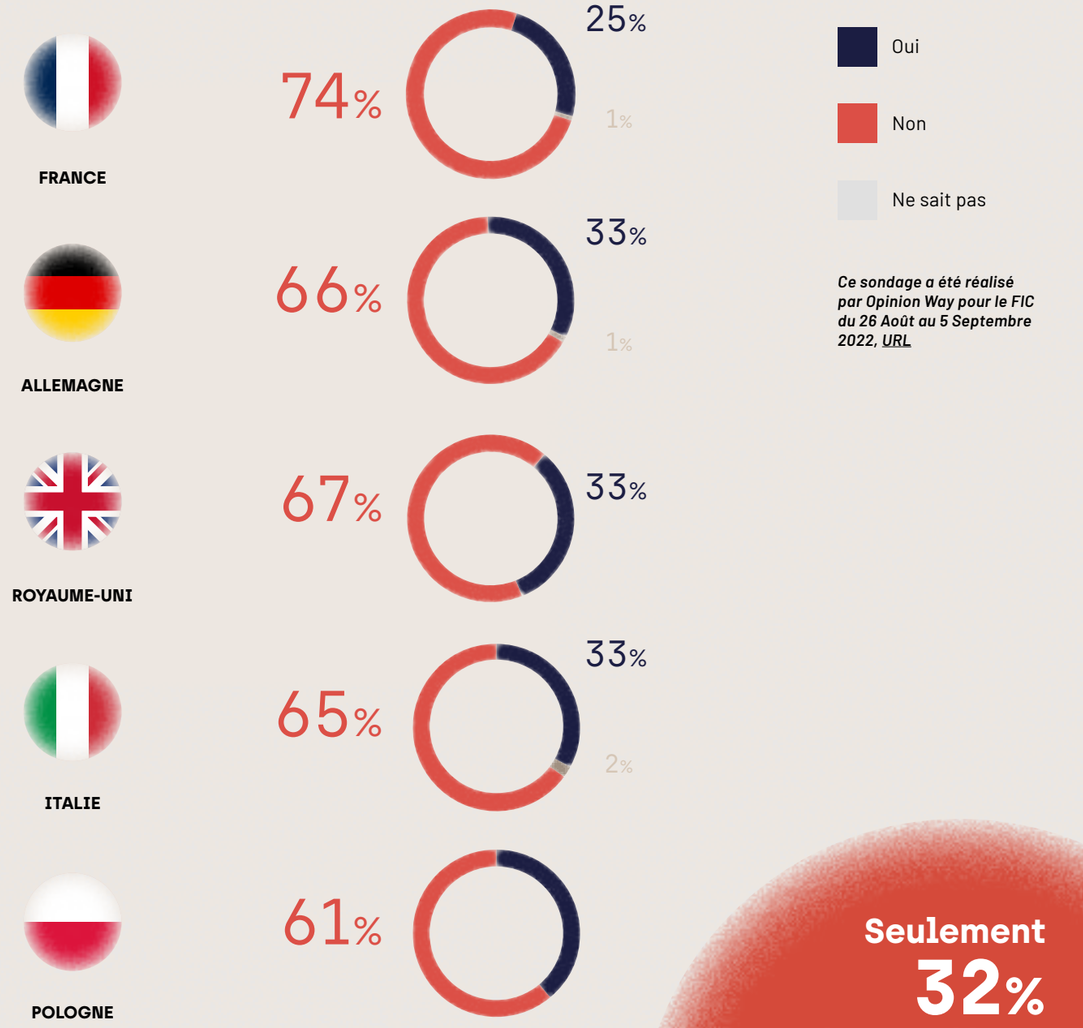
85% oui **14% non**

80. Enquête OpinionWay pour le FIC réalisée en septembre 2022, URL.

Mais si un utilisateur sur deux a été victime d'actes cyber-malveillants, dans quelle mesure sont-ils réellement en sécurité ?

Des entretiens avec des experts en la matière révèlent un écart entre les perceptions des citoyens et la réalité. Les personnes interrogées peuvent se sentir en sécurité en ligne, notamment parce que les personnes qui répondent à un sondage en ligne sont peut-être particulièrement compétentes en matière de technologie. L'enquête a également montré que seul un répondant sur trois se souvenait d'une campagne de sensibilisation à la cybersécurité, ce qui signifie qu'il pourrait aussi ne pas être conscient des vulnérabilités que présentent ses appareils et services.

VOUS SOUVENEZ-VOUS D'UNE CAMPAGNE DE COMMUNICATION VISANT À PROMOUVOIR LA CYBERSÉCURITÉ (SÉCURITÉ INFORMATIQUE ?)



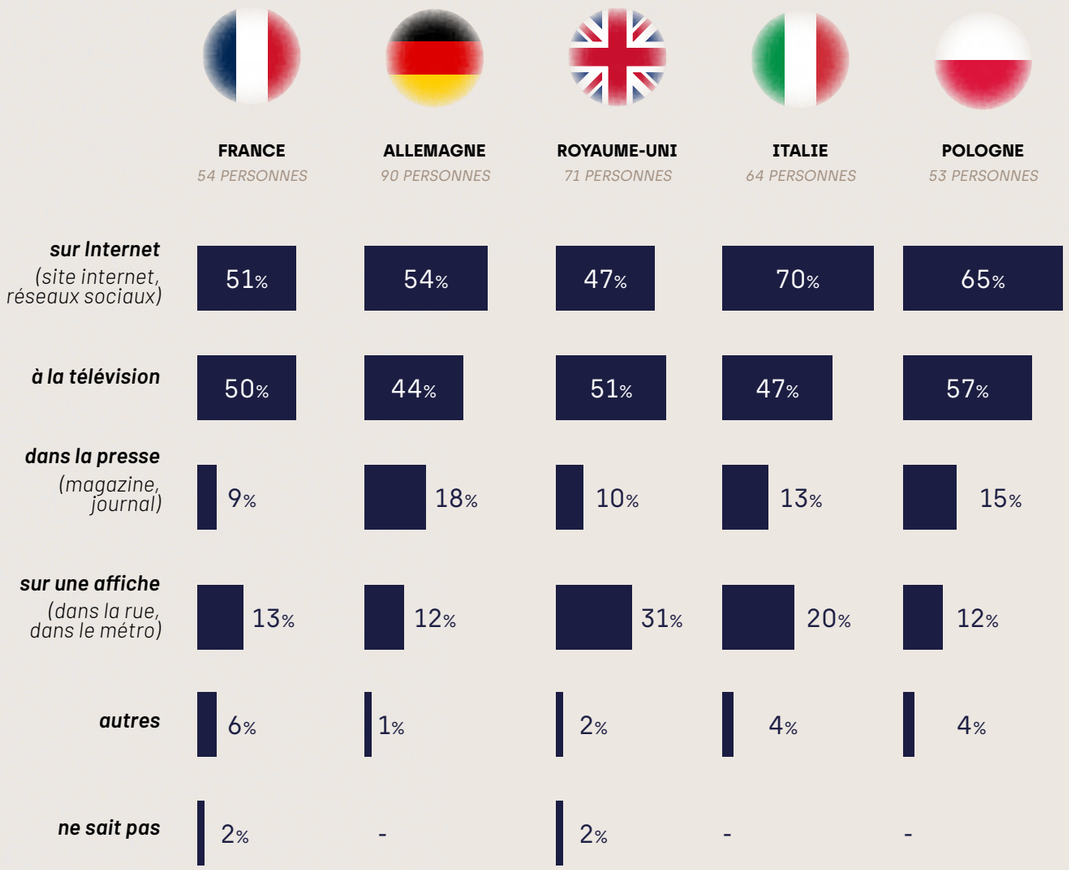
Ce sondage a été réalisé par Opinion Way pour le FIC du 26 Août au 5 Septembre 2022, URL

Seulement 32% des sondés se souviennent d'une campagne de sensibilisation à la cybersécurité

81. Enquête OpinionWay pour le FIC réalisée en septembre 2022, URL.

OÙ VOUS SOUVENEZ-VOUS AVOIR VU UNE CAMPAGNE VISANT À PROMOUVOIR LA CYBERSÉCURITÉ ?

QUESTION POSÉE UNIQUEMENT À CEUX QUI SE SOUVIENNENT D'UNE CAMPAGNE DE COMMUNICATION POUR PROMOUVOIR LA CYBERSÉCURITÉ (SÉCURITÉ INFORMATIQUE), SOIT 32% DE L'ÉCHANTILLON.
PLUSIEURS RÉPONSES POSSIBLES - TOTAL SUPÉRIEUR À 100%.



Ce sondage a été réalisé par Opinion Way pour le FIC du 26 Août au 5 Septembre 2022

Ce manque de sensibilisation est révélateur du fait que les citoyens n'ont pas conscience des conséquences directes que des cyberattaques contre des infrastructures collectives peuvent avoir sur leurs vies quotidiennes. Ce manque de sensibilisation met également en évidence un décalage entre les perceptions de sécurité dans le cadre privé ou professionnel. Les utilisateurs ne sont peut-être pas aussi préoccupés par leurs appareils personnels, mais comme le travail et la vie personnelle se mélangent désormais sans qu'il n'y ait parfois de séparation claire entre les appareils électroniques utilisés, les risques augmentent.

Le manque de sensibilisation à la cybersécurité est un problème bien connu. Les agences nationales de cybersécurité ont pris la tête de vastes campagnes de sensibilisation à la cybersécurité, souvent en partenariat avec des organisations du secteur privé et de la société civile. Ces campagnes ont tendance à se concentrer sur l'éducation du public aux bonnes pratiques d'hygiène numérique, de lutte contre hameçonnage et autres menaces, et sur la promotion de ressources gratuites.

Événement phare de la sensibilisation à la cybersécurité, le mois d'octobre a été désigné « Mois de la sensibilisation à la cybersécurité » *[Cyber Security Awareness Month]* . Cette initiative a vu le jour en 2004 à la suite d'une collaboration entre le ministère américain de la sécurité intérieure et la US National Cyber Security Alliance pour sensibiliser à l'importance de la cybersécurité . Depuis lors, cette pratique est devenue populaire et le mois d'octobre est reconnu comme le mois de la cybersécurité dans de nombreux pays. Au cours de cette période, les bonnes pratiques en matière de cybersécurité sont mises en avant par des entités privées et publiques afin d'informer et d'encourager les citoyens à se protéger en ligne. Au niveau de l'UE, l'initiative a fêté ses 10 ans d'existence en octobre 2022, avec le soutien de l'ENISA, de la Commission européenne et des États membres .

Les agences nationales de cybersécurité européennes profitent elles aussi du mois d'octobre, mois de sensibilisation à la cybersécurité, pour rappeler au grand public les bonnes pratiques en matière de cybersécurité, en complément des campagnes de sensibilisation qu'elles mènent tout au long de l'année. Certaines bonnes pratiques nationales se distinguent particulièrement :

- Belgique : Le CCB participe à l'amélioration des connaissances du grand public sur les principaux problèmes liés à la cybersécurité, notamment en utilisant l'humour pour diffuser ses messages clés, comme dans cette video ou à l'adresse suivante : https://www.safeonweb.be/en/campaign-material
- France : Comme le CCB, la France utilise l'humour pour diffuser ses messages. Ces campagnes aident les citoyens à se familiariser avec le centre d'information https://www.cybermalveillance.gouv.fr/. Des informations complètes sur le kit de sensibilisation sont disponibles ici : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation.
- États-Unis : le mois de la sensibilisation à la cybersécurité existe aux États-Unis depuis 2004, avec des thèmes variés. En 2022, la CISA met l'accent sur le rôle de l'utilisateur dans la cybersécurité, en encourageant les particuliers à s'impliquer dans leur protection. La campagne complète est disponible ici : https://www.cisa.gov/cybersecurity-awareness-month.

En plus de ces campagnes gouvernementales, la société civile et les organisations à but non lucratif s'associent régulièrement aux gouvernements et au secteur privé pour mener des campagnes de sensibilisation afin d'aider les utilisateurs à mieux se protéger.

82. Mois européen de la cybersécurité, URL.
83. Cybersecurity awareness month, CISA, URL.
84. Mois européen de la cybersécurité, URL.

LA VOIE À SUIVRE : RECOMMANDATIONS

Remettre les citoyens au cœur des efforts de cybersécurité nécessite une approche de la société dans son ensemble. Les gouvernements, les entreprises et les citoyens eux-mêmes ont un rôle à jouer pour améliorer collectivement la cybersécurité par la protection et la responsabilisation des citoyens. L'Agora du FIC propose 12 recommandations visant à encourager une cybersécurité davantage axée sur les personnes.

ÉDUCATION & SENSIBILISATION

1

Financer des programmes d'éducation à la cybersécurité dans les écoles. Bien qu'enfant du numérique, la génération Z, est celle dont les pratiques en matière de cybersécurité sont parmi les plus faibles de toutes les générations actuellement sur le marché du travail . Cette tendance risque malheureusement de se poursuivre si la formation à la cybersécurité ne commence pas à un âge plus précoce. Il apparaît nécessaire d'intégrer aux programmes scolaires des programmes d'éducation à la cybersécurité qui soient adaptés à chaque âge et inclusifs. Les financements de tels programmes pourront provenir de partenariats public-privé, car le secteur privé est responsable de la sécurité des produits ou services numériques utilisés par les citoyens.

2

Mettre en place au niveau européen des programmes de formation continue en matière de cybersécurité. Avec le développement rapide des nouvelles technologies, les bonnes pratiques en matière de cybersécurité ne cessent d'évoluer. Les citoyens doivent pouvoir, tout au long de leur vie, suivre l'évolution des réglementations, des outils et des solutions en matière de cybersécurité.

3

Faire passer les campagnes de sensibilisation de l'éducation à l'adoption. Alors que l'UE célèbre le 10e anniversaire de son « Mois de sensibilisation à la cybersécurité », la prochaine étape doit viser à s'assurer que les citoyens ne sont pas seulement conscients des meilleures pratiques en matière de cybersécurité, mais qu'ils adoptent et mettent effectivement en œuvre les solutions proposées. Les pouvoirs publics devraient profiter de la dynamique du « Mois de la cybersécurité » pour encourager les utilisateurs à mettre à jour leurs mots de passe, à activer les mises à jour automatiques ou à utiliser des logiciels antivirus.

85. The Generational Gap in Cybersecurity and Privacy, Weir, URL.

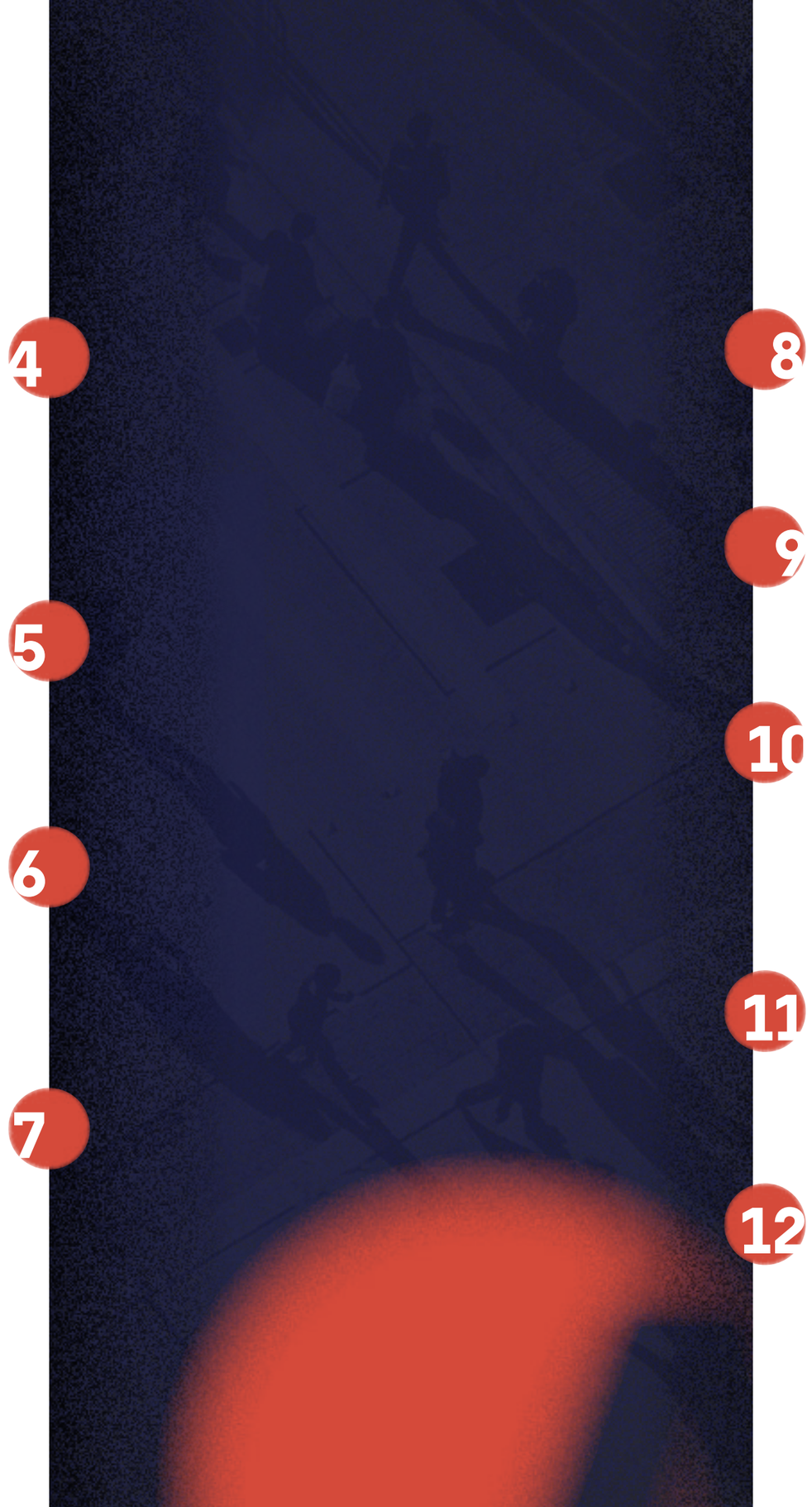
SOUTIEN AUX CITOYENS

Généraliser des « boîtes à outils » de cybersécurité à l'attention des citoyens. Certaines agences nationales de cybersécurité proposent déjà des boîtes à outils utiles, qui fournissent aux citoyens des outils leur permettant d'assurer efficacement leur sécurité en ligne, comme c'est le cas en Belgique ou au Royaume-Uni. Ces boîtes à outils devraient être facilement exploitables et très didactiques, permettant aux citoyens d'identifier les types d'attaques, de proposer des recommandations opérationnelles type « fiche réflex », et de détailler les procédures ou démarches à réaliser auprès des bon interlocuteurs.

Élaborer et promouvoir des mesures visant à garantir des normes élevées de cybersécurité pour tous les produits. Certaines évolutions du cadre réglementaire, actuellement en cours de déploiement telles que les schémas de certification de l'UE ou la réglementation européenne sur la cyber-résilience, constituent des premiers pas importants dans cette direction. D'autres mesures devront être élaborées pour suivre l'évolution des technologies et des produits et veiller à ce qu'ils continuent à respecter des normes élevées de cybersécurité.

Exiger des fournisseurs de services numériques plus de transparence sur leurs pratiques en matière de sécurité et de respect de la vie privée. Les fournisseurs de services numériques, y compris les fournisseurs d'accès à l'internet, disposent d'une certaine marge de manœuvre quant aux informations qu'ils peuvent recueillir et stocker, et à ce qu'ils peuvent en faire, en particulier s'ils opèrent en dehors de l'UE. Les citoyens doivent pouvoir être sûrs que lorsqu'ils se connectent à l'internet et utilisent des appareils électroniques, ils sont en sécurité. Ces fournisseurs devraient donc être plus transparents quant à leurs pratiques en matière de confidentialité et de sécurité.

Créer un « Cyberscore ».. Sur le modèle du Nutriscore, un « Cyberscore » pourrait indiquer le niveau de cybersécurité et de confiance dans un produit ou service via une classification sous forme de code couleurs. Ce système permettrait de fournir directement au consommateur une indication claire et lisible afin d'éclairer sa décision d'achat.



POLITIQUE & SENSIBILISATION

Élaborer un contrat social en ligne. L'élaboration d'un e-contrat social pourrait contribuer à améliorer la confiance numérique et à encourager le partage des responsabilités en ligne entre les pouvoirs publics, l'industrie et les citoyens. Les termes d'un tel contrat devraient être définis en consultation avec toutes les parties prenantes concernées, notamment les gouvernements, l'industrie, les organisations de la société civile et les citoyens.

Adopter et mettre en œuvre rapidement la loi sur la cyber-résilience et les futurs règlements européens. Les États membres utilisent des processus différents pour transposer et mettre en œuvre les règlements de l'UE, ce qui peut entraîner une mise en œuvre inégale, défavorable aux citoyens. Les États membres doivent mettre en œuvre rapidement les politiques de cybersécurité de l'UE.

Améliorer le partage d'informations sur les menaces entre les gouvernements, l'industrie et les citoyens. Les organismes gouvernementaux compétents doivent continuer à informer l'ensemble des organisations de l'état de la menace et des tendances observées, mais aussi en informer directement les citoyens. La Belgique, par exemple, propose une revue d'informations cybersécurité qui informe les citoyens des cyber menaces, comme ils le font par exemple pour les menaces météorologiques sérieuses. Un parallèle peut être fait avec les dispositifs d'alerte sur la menace terroriste à l'image du plan Vigipirate en France. Cette pratique devrait être étendue à l'ensemble de l'UE et permettrait de mieux informer les citoyens sur le niveau des cybermenaces.

Dégager des financements pour accompagner la mise en conformité des nouvelles normes. L'élaboration de systèmes de certification en matière de cybersécurité et l'introduction de nouvelles normes représentent souvent une charge financière pour les fournisseurs comme pour les utilisateurs. Des fonds dédiés devraient être mis à disposition pour permettre aux parties prenantes de suivre le rythme et de se conformer aux exigences législatives.

Promouvoir une approche locale pour la mise en œuvre des stratégies de cybersécurité. Les autorités locales, qui sont au plus proche des citoyens ont un rôle clé à jouer pour impliquer ces derniers dans les efforts de cybersécurité. Les autorités locales doivent être habilitées par les autorités européennes, nationales et régionales à communiquer avec les citoyens sur le « dernier kilomètre ».

RÉFÉRENCES

#SuperCoders: Corporate Social Responsibility, Orange, URL.

A majority of Americans are concerned about the safety and privacy of their personal data, Ipsos, URL.

Ad-Hoc Working Group 03 - on 5G Cybersecurity Certification, ENISA, URL.

Ad-hoc Working Group calls, ENISA, URL.

Briefing on the NIS2 Directive: A high common level of cybersecurity in the EU, Negreiro, URL.

Capgemini - Social, Capgemini, URL.

Children's Online Privacy Protection Rule («COPPA»), US Federal Trade Commission, URL.

Code with Google, Google, URL.

Complete guide to GDPR compliance, GDPR.EU, URL.

Consultation on the draft of the candidate Certification Scheme on Cloud Services (EUCS) - Closed, ENISA, URL.

Critical infrastructure sectors in Israel include the 11 sectors defined in the NIS Directive plus the following: Food Supply and Distribution, Government, Public Safety, and Law Enforcement.

Cultivate key human resources who will lead the 4th Industrial Revolution, Samsung, URL.

Cyber force refers to the responsibility to develop a national cyber defence. See more here.

Cyber resilience act – new cybersecurity rules for digital products and ancillary services, European Commission, URL.

Cyber Resilience Act, European Commission, URL.

Cybersecurity awareness month, CISA, URL.

Cybersecurity Certification: Candidate EUCC Scheme V1.1.1, ENISA, URL.

Cybersecurity in the EU – Why we need NIS2 and what changes does it mean for the tech sector?, EURACTIV, URL.

Cybersecurity, CISA, URL.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, URL.

Divided we fall: Why fragmented global privacy regulation won't work, Kieran, URL.

EU Country Commercial Guide - Cyber Security, International Trade Administration, URL.

EU Cyber Resilience Act, European Commission, URL.

EU Cybersecurity Certification - FAQ, ENISA, URL.

European Cyber Security Organisation (ECSO) - About, ECSO, URL.

European Cybersecurity Month, URL.

Federal Information Security Modernization Act (FISMA), CISA, URL.

Germany calls for political discussion on EU's cloud certification scheme, Bertuzzi, URL.

Global Comprehensive Privacy Law Mapping Chart, IAPP, URL.

Google Career Certificates, Google, URL.

Hardware security overview, Apple, URL.

Israel Defense Forces and National Cyber Defense, Tabansky, URL.

Le modèle Zero Trust, ANSSI, URL.

NIS Directive, IT Governance, URL.

Enquête OpinionWay pour le FIC réalisée en septembre 2022, URL.

Philanthropic initiatives for local communities, Google, URL.

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, URL.

Public Consultation on the draft Candidate EUCC Scheme, ENISA, URL.

PUBLIC LAW 117–103—MAR. 15, 2022, American Congress, URL.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (General Data Protection Regulation), URL.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (Cybersecurity Act), URL.

Review of the Directive on security of network and information systems, European Parliament Legislative Train, URL.

Secure design principles, UK National Cyber Security Centre (NCSC), URL.

Security Visa, ANSSI, URL.

Sovereignty requirements remain in cloud certification scheme despite backlash, Kabelka, URL.

TEAL Program, Microsoft, URL.

The EU Cybersecurity Act, European Commission, URL.

The EU NIS Directive, IT Governance, URL.

The European Cybersecurity Act, EUROSMART, URL.

The European Cybersecurity Market, Enterprises Ireland, URL

The new European Cyber Resilience Act, European Parliament Train Schedule, URL.

The Right to Financial Privacy Act, EPIC, URL.

The Women's Digital Centres programme: actively supporting women's empowerment, Fondation Orange, URL.

Thriving together: Samsung CSR US, URL.

Understanding the EU Cybersecurity Act and Its Effect on Businesses, Dunkelberger, URL.

What is GDPR, the EU's new data protection law?, GDPR.EU, URL.

Your rights under HIPAA, US Department of Health & Human Services, URL.

Zero Trust Architecture, Rose et al., URL

REMERCIEMENTS

L'équipe de l'Agora du FIC tient à remercier Phédra Clouner, directrice adjointe du Centre pour la cybersécurité en Belgique (CCB) et membre de l'Advisory Board du FIC, et Phil Reitinger, directeur général de la Global Cyber Alliance, pour leurs précieuses contributions à ce livre blanc.

L'équipe de l'Agora du FIC tient également à remercier Amélie Rives pour son soutien et ses conseils tout au long de ce processus, ainsi que Camille Monlouis-Félicité pour sa contribution à la recherche documentaire de ce document.

Agora FIC

Ne demandez pas ce que le numérique peut faire pour vous - demandez ce que vous pouvez faire pour le numérique.

Prochain événement...

FIC EUROPE

LILLE, FRANCE

5 - 7 AVRIL 2023