

Security Navigator 2026 : les données clés

Explosion de la Cyber extorsion Cy-X :

- Le Security Navigator 2026 révèle que les attaques Cy-X ont bondi, avec une augmentation de **44,5 % des victimes** observées entre octobre 2024 et septembre 2025, par rapport à la période précédente.
- Cela poursuit une tendance pluriannuelle, le nombre total de victimes ayant plus que **triplé depuis 2020 pour atteindre 19 000 victimes**.

Le paysage de la cybercriminalité se fragmente

- Auparavant, un seul groupe dominant définissait le paysage. Désormais, plusieurs acteurs soutiennent des opérations à grande échelle, le nombre d'acteurs **cybercriminels distincts ayant presque triplé, passant de 33 à 89 depuis 2020**.
- En Europe, les victimes de Qilin et d'Akira ont augmenté respectivement de 324 % et de 168 %.
- Cela est en partie dû à une **industrialisation du marché de la cybercriminalité** sur le modèle du « cybercrime en tant que service », qui a drastiquement abaissé les coûts d'entrée pour les attaquants - ce qui leur permet de se multiplier et de prospérer.
- Outre la baisse des coûts d'entrée, nous assistons à une **taylorisation** de la cybercriminalité avec des expertises spécialisées et qui démocratisent l'activité criminelle par le biais d'infrastructures partagées, de programmes d'affiliation et d'**outils vendus en kit**.

Les attaquants se diversifient et ciblent les plus vulnérables

- **Deux tiers des victimes du Cy-X** sont des petites et moyennes entreprises (PME), soit une augmentation de 9 % par rapport à l'année précédente.
- Aux États-Unis, les victimes des petites entreprises ont fait un bond spectaculaire de 91 %,
- En Europe, **l'Allemagne, première au rang** du nombre victimes Cy-X, et plus forte croissance soit **+57,7 %**.
- La **France** est 3^{ème} dans le top européen avec une croissance de 10%
- 35 nouveaux pays voient le Cy-X émerger dans notre étude, parmi lesquels **10 nouveaux pays en Afrique**.

Les hacktivistes : Le bras armé des États dans la géopolitique modern

- L'hacktivisme s'est transformé en un écosystème complexe **aligné sur les intérêts des États et les conflits géopolitiques**, dépassant les simples protestations pour se transformer en perturbation du monde réel et en influence cognitive.
- Les principaux incidents survenus en 2025 ont **des répercussions sur les entreprises** : campagnes DDoS à grande échelle, attaques cyber-physiques et efforts de désinformation ciblés -

- Par exemple, le 7 avril 2025, des attaquants ont ouvert à distance une vanne du **barrage de Bremanger en Norvège** pendant plusieurs heures avant que les opérateurs n'interviennent.
- Le 29 octobre 2025, le Centre canadien de cybersécurité a signalé que des groupes d'hacktivistes avaient violé des systèmes OT/ICS dans les domaines de l'eau, de l'énergie et de l'agriculture au Canada, **manipulant la pression de l'eau ainsi que la température et les niveaux d'humidité**.
- Les objectifs sont passés de la perturbation technique à l'**influence cognitive**, visant à éroder la confiance dans les institutions et à influencer la perception du public via des campagnes de désinformation touchant également les entreprises.
 - en octobre 2025, des groupes d'hacktivistes pro-russes ont lancé une **campagne de désinformation** en affirmant qu'ils avaient accédé aux systèmes **d'approvisionnement en eau** de plusieurs pays européens, dont la Norvège et la Belgique, et qu'ils les avaient manipulés.
- Avec des opérations de police internationales visant à interrompre leurs activités, comme Europol [Eastwood](#)

La coopération mondiale en matière d'application de la loi est en hausse

Pour la première fois, le Security Navigator 2026 comprend un ensemble de données analysées méthodiquement sur **418 opérations de lutte contre la cybercriminalité** menées entre 2021 et la mi-2025. Les données, collectées par les équipes de recherche d'Orange Cyberdefense, confirment une **augmentation annuelle claire et régulière de l'activité de cyberdefense** entre 2021 et mi-2025 :

- Les mesures prises comprennent des arrestations (29 %), des démantèlements (17 %), des inculpations (14 %), des condamnations (11 %), des sanctions (7 %) et des saisies (4 %).
- **Cy-X est l'acte criminel le plus abordé** par les opérations de police, avec 59 cas, et il est également le plus **susceptible de conduire à des arrestations**. Ces actions s'intensifient pour faire face à la menace croissante que représente Cy-X.
- Les données mettent également en évidence un **partenariat public-privé solide**, les organisations privées se classant au troisième rang des types d'institutions soutenant les efforts de perturbation des forces de l'ordre : **40 % des cas** impliquent la contribution d'un **acteur privé**.
- Toutefois, les acteurs peuvent se reconstruire plus rapidement que les bureaucraties ne réagissent, ce qui laisse un terrain important à couvrir pour les initiatives mondiales en matière d'opération de police