Cigref
RÉUSSIR
LE NUMÉRIQUE

COMMUNIQUÉ DE PRESSE

Paris, le 21 juillet 2026

Face aux attaques Cyber propulsées par l'IA, le Cigref alerte sur la vulnérabilité de l'Europe

À l'occasion de la publication de sa nouvelle note d'information et d'actualité intitulée « *Sécurité numérique et IA : mutations de la menace et perspectives* », le Cigref dresse un diagnostic sur la transformation du paysage de la menace cyber. L'industrialisation des attaques à la « vitesse machine » et les tensions géopolitiques autour des modèles d'intelligence artificielle de pointe imposent une révision des doctrines de sécurité numérique des grandes organisations et la constitution rapide d'une capacité européenne autonome d'IA pour la cyberdéfense.

« D'une activité humaine augmentée, la cybersécurité est devenue une activité algorithmique supervisée par l'homme. Sans un accès garanti et autonome à des modèles d'IA de pointe, c'est l'ensemble de notre économie et de nos infrastructures critiques qui se retrouve exposé à une paralysie stratégique. »

Henri d'Agrain, Délégué général du Cigref

Un basculement vers la « vitesse machine »

Fondé sur les retours d'expérience de ses 155 membres publics et privés, le constat du Cigref met en évidence une évolution majeure. Désormais, la sécurité informatique s'est affranchie du seul périmètre technique pour s'inscrire au cœur d'une compétition géopolitique et économique.

Les événements récents confirment l'obsolescence des postures défensives réactives traditionnelles. Dans cette note, le Cigref identifie et analyse huit mutations systémiques de la menace cyber, notamment :

- **L'effondrement du *Time to Exploit* (TTE) :** le délai entre la découverte d'une vulnérabilité et son exploitation est désormais négatif. Les attaquants agissent avant la publication des correctifs, rendant le traitement réactif inopérant face aux cycles de déploiement en entreprise qui nécessitent 60 à 150 jours.
- **La saturation par l'hyper-volumétrie :** l'automatisation des attaques et le détournement de sessions authentifiées saturent les capacités d'analyse humaine des centres d'opérations de sécurité (SOC).
- **L'arsenalisation de l'IA :** l'utilisation d'agents algorithmiques accélère la reconnaissance des cibles, le développement dynamique de malwares et l'exploitation massive de failles jusqu'ici tolérées.

L'intelligence artificielle, infrastructure critique de la cybersécurité

L'actualité de l'été 2026 marque un tournant stratégique. La suspension temporaire d'accès aux modèles d'Anthropic décidée par les autorités américaines en juin a démontré qu'un bouclier algorithmique peut faire l'objet de mesures de contrôle unilatérales au nom de la sécurité nationale.

En parallèle, la diffusion de modèles chinois performants en *open-weight* (tels que Kimi K3 de Moonshot AI) crée une illusion d'autonomie pour les organisations européennes. Fonder la résilience de l'Europe sur ces technologies exposerait les entreprises à un risque d'assujettissement, les laissant démunies le jour où Pékin déciderait de bloquer la diffusion des versions futures.

L'intelligence artificielle de pointe constitue désormais une **infrastructure critique de la cybersécurité**. Les organisations qui ne disposeront pas à court terme d'un accès garanti et pérenne à un modèle de pointe spécialisé en cyber seront dans l'incapacité d'absorber la vitesse des attaques.

Les conditions d'une réponse collective européenne

Face à l'ampleur des investissements requis pour développer des modèles frontière, aucun État européen ne peut supporter seul cet effort.

Le Cigref préconise :

1. **L'émergence d'une coalition industrielle :** regrouper les grands utilisateurs économiques et les acteurs technologiques pour mutualiser les ressources, créer la masse critique indispensable et engager des coopérations transfrontalières, notamment au niveau franco-allemand.
2. **L'appui des pouvoirs publics :** accompagner cette dynamique privée via le Plan d'action sur la cybersécurité et l'IA de la Commission européenne, en facilitant l'accès aux capacités de calcul.
3. **L'exigence du *Security by Design* :** soumettre l'industrie numérique à des normes strictes pour exiger la correction des vulnérabilités à la source et mettre fin à l'externalisation du risque technique sur les clients.

À propos : le Cigref est une association indépendante et sans activité commerciale, créée en 1970, qui accompagne ses 155 membres, grandes entreprises et administrations publiques françaises utilisatrices de solutions et services numériques, dans toutes leurs réflexions sur leurs enjeux numériques collectifs. Notre association œuvre, au profit de ses membres, en faveur d'un numérique durable, responsable et de confiance.

Plus d'informations sur https://www.cigref.fr

Contact Presse : Emilie GRANGE, chargée de communication et RP
egrange@cigref.fr / 06 70 41 06 92