Veille Newsletter
www.veillemag.com
Le magazine des professionnels de l'information stratégique

Par Jacqueline Sala

Focus Cybersécurité septembre 2025. Entre menaces géopolitiques, IA malveillantes et polémiques autour du projet de loi « Chat Control » par Yannick Pech

Ce mois deseptembreaura étédensesurle frontdelacybersécurité : laFrance a simuléunecyberattaquemajeure pour tester sa résilience, de vifsdébats se sont cristallisés autour du projet européen controversé Chat Control, tandis que les cybermenaces se robotisent de plus en plus en incluant des agents IA.

FRANCE : REMPAR25, UN EXERCICE DE CRISE INÉDIT

Le 18 septembre, l'ANSSI a piloté l'exercice national Rempar25, rassemblant environ 5 000 acteurs de 1 000 organisations à travers le pays. Le scénario simulait une panne causée par un antivirus compromis, puis l'enchaînement d'un vol de données, une demande de rançon et parallèlement la distillation d'informations fausses destinées à déstabiliser les organisations touchées.

L'objectif déclaré n'était pas tant de tester des réponses techniques que d'examiner la capacité des acteurs (collectivités, entreprises, services publics) à gérer la crise dans ses dimensions humaine, légale, médiatique et de gouvernance. Le déblocage par l'Agence de 6,8M€ en début de mois pour l'accompagnement cyber de proximité s'inscrit bien dans cette perspective.

L'exercice confirme une tendance : la cybersécurité ne se limite plus aux équipements techniques tels les pare-feux ou aux correctifs logiciels, mais implique la préparation de scénarios de crise multidimensionnels axés sur les aspects humains et organisationnels.

Enjeux stratégiques et menaces globales

MULTIPLICATION D'ATTAQUES CIBLÉES MATÉRIELLES ET LOGICIELLES

De nouvelles atteintes sur des câbles de fibre optique en mer Baltique ont été détectées : elles soulignent la nécessité de **renforcer la redondance réseau** pour atténuer la vulnérabilité des infrastructures physiques du cyberespace (Internet). Plusieurs cyberattaques significatives ont par ailleurs été signalées, en France et à l'étranger. Des entités publiques ont été ciblées, notamment dans le domaine de la santé, avec des tentatives de vol de données médicales. Des **vulnérabilités logicielles critiques** ont aussi été découvertes et parfois exploitées avant la mise à disposition de correctifs, ou *a posteriori* par **défaut d'automatisation des mises à jour** de la part des organisations.

IA : DES CYBERATTAQUES « AUGMENTÉES »

L'intelligence artificiellecontinue de jouer un **rôle ambivalent et dual** : elle sert autant à renforcer les défenses qu'à piloter les attaques.
L'émergence d'outils malveillants alimentés par IA, comme SpamGPT, illustre cette tendance. Dans ce contexte, la *cyber threat intelligence* (CTI, ou **renseignement sur la cybermenace**) devient cruciale pour guider la réponse des organisations, lesquelles se dotent progressivement de telles équipes spécialisées.

GOUVERNANCE, RÉGLEMENTATION ET DONNÉES

Entréen vigueur le12 septembre,le**Data Act**encadre l'accès et le partage des données issues d'objets connectés et de services numériques. En France, l'ANSSI a lancé une **plateforme appelée** MesServicesCyberpour accompagner les entreprises et les collectivités dans la gestion de leur cybersécurité.
En parallèle, des événements comme les **Cybermatinées Sécurité** ou la conférence **FranSec** ont confirmé la prise en compte des préoccupations autour de la résilience, de l'automatisation et du rôle croissant de l'humain dans les réponses aux cybermenaces.

Débat autour de « Chat Control » : vers une surveillance de masse en Europe ?

QU'EST CE QUE « CHAT CONTROL » ?

Leprojeteuropéen CSAR (*Child Sexual Abuse Regulation*) dit « Chat Control » vise à lutter contre la pédocriminalité en imposant le contrôle automatique des fichiers et contenus *avant* leur envoi, même sur les services de messageries chiffrées comme Signal ou WhatsApp.
Concrètement, cela signifie que des technologies de détection constituant ni plus ni moins des *backdoors* (portes dérobées informatiques) seraient intégrées dans les applications pour identifier les contenus signalés comme illégaux, avant même qu'ils ne soient transmis.

OPPOSITION, CRITIQUES ET CONTROVERSES

Ce projet suscite devives réactionspour plusieurs raisons :

- il **oblitèrerait le chiffrement de bout-en-bout**, remettant en cause un pilier fondamental de la sécurité et de la confiance numériques ;
- il ouvre la voie à des risques de faux-positifs, des abus potentiels et à des effets de dérive vers une surveillance généralisée, et vraisemblablement **une autocensure citoyenne** ;
- il pourrait servir de précédent pour **étendre les technologies de contrôle** à d'autres domaines (dissidence, opposition politique...).

Des entreprises comme l'Allemande **Tuta** (ex-Tutanota) ont annoncé leur intention de saisir la justice si le texte est adopté. Plusieurs États membres, comme **la Belgique et la République tchèque**, se sont également opposés au projet. La **Signal Foundation** a, quant à elle, fait savoir qu'elle

OÙ EN EST LE PROCESSUS LÉGISLATIF ?

Le projet de règlement est toujoursen discussion au Conseil de l'UE, où un vote décisif pourrait intervenir en octobre. En 2023, le Parlement européen avait introduit plusieurs amendements pour limiter les tensions, mais la version actuelle reste controversée.
Un compromis respectant tant la protection des mineurs que le respect des droits fondamentaux – dont le chiffrement – pourra-t-il être trouvé ?

PERSPECTIVE : L'EUROPE À LA CROISÉE DES CHEMINS

L'actualité deseptembre confirme que la cybersécurité ne peut plus être pensée uniquement en termes techniques.
Elle est un **enjeu desouveraineté**, devient une **question derésilience** mais aussi de **choix de société**. Entre la préparation aux crises majeures, la montée en puissance des cybermenaces augmentées par IA et le débat autour du contrôle des communications privées, l'Europe et la France sont à un tournant. Les prochaines décisions politiques, notamment autour du projet *Chat Control*, pourraient redéfinir durablement l'équilibre entre sécurité, vie privée et libertés individuelles dans l'espace numérique européen.

En Résumé

1. La cybersécurité entre dans une ère de gestion de crise systémique

- L'exercice **Rempar25** montre une évolution claire : il ne s'agit **plus seulement de protéger** les systèmes, mais de **rendre les organisations plus résilientes** en cas d'attaque massive.
- Cette approche globale inclut désormais la **communication de crise, la coordination intersectorielle et la continuité d'activité**, illustrant une **maturité croissante des politiques cyber nationales**

2. Des menaces plus complexes, rapides et automatisées

- Les attaques deviennent **plus ciblées, fréquentes et sophistiquées**, toujours plus dopées à l'**intelligence artificielle**.
- L'IA devient une **arme offensive** : automatisation des attaques, création de contenus malveillants sur mesure, appui à la programmation.
- **Le temps entre la découverte d'une faille et son exploitation** se réduit, rendant **critiques la réactivité** et la **gestion des mises à jour** logicielles.
-

3. Cybersécurité et souveraineté numérique s'entremêlent

- Le **Data Act** européen et les plateformes comme **MesServicesCyber** en France renforcent la volonté des États de **reprendre le contrôle de la donnée** et d'organiser une gouvernance numérique claire.
- L'encadrement réglementaire se structure (Data Act, DORA, NIS2…), mais impose aux entreprises une **adaptation constante à des exigences de conformité croissantes**

4. La vie privée au cœur des tensions politiques européennes

- Le projet de règlement **Chat Control** marque une **rupture symbolique** entre **protection de l'enfance** et **respect du chiffrement et de la vie privée**.
- L'opposition croissante (États membres, entreprises, société civile) souligne une **crise de confiance envers les ambitions sécuritaires européennes**, accusées de glisser vers une **surveillance de masse**
- Ce débat pose une question de fond : **jusqu'où la cybersécurité peut-elle aller sans devenir une menace pour les libertés fondamentales ?**

5. Un glissement de la cybersécurité vers une problématique sociétale et éthique

- Les événements, tribunes et réactions politiques révèlent que la cybersécurité n'est plus un sujet purement technique ou stratégique.
- Elle devient **politisée, médiatisée et idéologisée**, car elle touche à des **valeurs fondamentales** : vie privée, contrôle démocratique, liberté d'expression.
- Le citoyen, l'entreprise et l'État sont désormais **co-responsables de l'équilibre à trouver** entre sécurité et liberté numériques.
-

Le Monde, « Comment la France se prépare au jour où le ciel lui tombera sur la tête
https://www.lemonde.fr/pixels/article/2025/09/19/cybersecurite-comment-la-france-se-prepare-au-jour-ou-le-ciel-lui-tombera-sur-la-tete_6641852_4408996.html

ANSSI, « Un exercice de crise cyber d'une ampleur inédite »
https://cyber.gouv.fr/actualites/rempar25-un-exercice-de-crise-cyber-dune-ampleur-inedite

Veillecyber.fr, n°561 (15 septembre 2025)
https://veillecyberland.wordpress.com/2025/09/16/veille-cyber-n561-15-septembre-2025/

Veillecyber.fr, n°562 (22 septembre 2025)
https://veillecyberland.wordpress.com/2025/09/23/veille-cyber-n562-22-septembre-2025/

LeMagIT, « Cyberhebdo du 19 septembre 2025
https://www.lemagit.fr/actualites/366631537/Cyberhebdo-du-19-septembre-2025

Euronews, « L'UE va-t-elle vraiment commencer à scanner vos messages texte ?
https://fr.euronews.com/my-europe/2025/09/12/verification-des-faits-lue-va-t-elle-vraiment-commencer-a-scanner-vos-messages-texte

Next.ink, « Chat Control : le projet de surveillance des messageries a encore du plomb dans l'aile
https://next.ink/198995/chat-control-le-projet-de-surveillance-des-messageries-a-encore-du-plomb-dans-laile/

Clubic, « Tuta Mail veut traîner l'UE en justice si Chat Control est adopté
https://www.clubic.com/actualite-578532-david-contre-goliath-tuta-mail-veut-trainer-l-ue-en-justice-si-chat-control-est-adopte.html

La Dépêche, « Vos messages privés bientôt lus par l'UE ?
https://www.ladepeche.fr/2025/09/19/vos-messages-prives-bientot-lus-par-lue-pourquoi-le-projet-chat-control-inquiete-les-defenseurs-des-libertes-12941204.php

Atlantico, « Alerte libertés publiques : opposition au projet Chat Control
https://atlantico.fr/article/decryptage/alerte-libertes-publiques-opposition-au-projet-chat-control-ue-monte-ailleurs-en-europe-mais-pas-en-france-messageries-whatsapp-telegram-liberte-expression-Fabrice-Epelboin

Le Monde, Tribune de Rodrigo Arenas
https://www.lemonde.fr/idees/article/2025/09/24/rodrigo-arenas-sous-l-etendard-de-la-protection-des-mineurs-l-ue-s-apprete-a-faire-un-pas-decisif-vers-une-societe-de-controle_6642716_3232.html

Preventica, « Cybersécurité & règlementations
https://www.preventica.com/magazine/thematique/environnement-de-travail/securite-incendie-surete/cybersecurite

DevInci.fr, Cybermatinées Sécurité 2025

https://www.devinci.fr/evenements/cybermatinees-securite-2025-8e-edition/

FranSec, **https://france.cyberseries.io/**

A PROPOS DE YANNICK PECH

Yannick PECH *est docteur en sciences de l'information-communication, spécialiste du renseignement et de la cybersécurité, certifié pentester junior. Chargé de cours en géopolitique, intelligence économique, sécurité numérique et OSINT dans le supérieur privé et public, chercheur au CEREGE de l'IAE de Poitiers, ancien veilleur-analyste et réserviste opérationnel de l'armée de Terre, il est désormais officier de la Réserve citoyenne de cyberdéfense au sein de la gendarmerie d'Occitanie. Il prépare actuellement les certifications EBIOS-RM et ISO-27001.*

29/09/2025