Information Presse

Synthèse des ateliers Congrès CESIN 2025

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

La cybersécurité dans les turbulences géopolitiques

Enseignements clés du 13e Congrès annuel du CESIN – Reims, décembre 2025

Lors du Congrès du CESIN, plus de 180 responsables cybersécurité ont travaillé sur huit ateliers thématiques, en lien avec les tensions géopolitiques et leurs répercussions directes sur la sécurité des organisations.

La cybersécurité n'est pas un sujet technique isolé. Elle est aussi un prolongement quotidien des rapports de force internationaux, des dépendances économiques et des stratégies d'influence qui s'exercent sur les entreprises.

Le Congrès 2025 du CESIN révèle une transformation profonde du rôle du RSSI, qui devient un acteur de souveraineté organisationnelle. La cybersécurité ne peut plus être pensée indépendamment des tensions internationales, des choix technologiques structurants, du risque informationnel et de la chaîne de valeur globale.

Les entreprises doivent désormais naviguer dans un environnement fragmenté où l'ingérence, la dépendance et la manipulation informationnelle sont devenues des réalités opérationnelles.

SYNTHESE / RESTITUTIONS DES ATELIERS

1. La souveraineté numérique, nouveau pilier des stratégies cyber

Les RSSI constatent une accélération nette des effets géopolitiques sur leurs décisions : dépendance aux technologies extra-européennes, complexité réglementaire, exposition accrue via les chaînes de valeur mondiales.

Trois tendances émergent :

• une nécessité de régionaliser les solutions et services, avec des freins, notamment liés à la complexité réglementaire et à la résistance au changement ;

• une évolution des critères de choix du cloud de confiance, désormais liés à la résilience et à l'autonomie numérique ;

• une obligation croissante de mesurer la dépendance technologique et d'introduire des clauses de réversibilité.

2. Cloud de confiance 2.0 - un choix stratégique, plus seulement réglementaire

Les offres de Cloud de confiance arrivent à maturité, quels seront les moteurs de choix ?

Trois enseignements :

• l'adoption éclairée, souscrire ou pas, les organisations doivent arbitrer entre coût, capacité opérationnelle et autonomie ;

• le RSSI est désormais appelé à diriger ou co-piloter la décision, à faire émerger la prise de conscience du Comex

• la résilience et l'indépendance juridique deviennent des critères déterminants.

Le débat ouvre une question centrale, accepterons-nous de payer davantage pour reconquérir une souveraineté à long terme ?

3. Plateformisation - un gain de simplicité, un risque de dépendance

La consolidation des solutions cyber autour de plateformes globales simplifie l'exploitation, mais elle crée :

• des dépendances économiques et géopolitiques nouvelles

• une moindre marge de négociation

• un risque d'appauvrissement fonctionnel pour les environnements complexes.

Les RSSI s'orientent vers des architectures hybrides, mêlant plateforme et solutions spécialisées, pour préserver leur agilité.

4. La CTI élargie pour couvrir les axes de désinformation et de destabilisation

La Cyber Threat Intelligence est incontournable doit désormais couvrir :

• la désinformation

• les narratifs hostiles

• les manipulations d'opinion

• les risques liés aux tiers en position dominante.

Les organisations doivent structurer une CTI adaptée à leur maturité et produire un renseignement stratégique ad hoc pour les bénéficiaires, dont les dirigeants. La CTI devient un outil d'aide à la décision, pas seulement un radar technique.

5. Menaces internes, un risque stratégique encore sous-estimé

Les tensions géopolitiques exacerbent les risques de sabotage, de fraude ou d'exfiltration, pourtant :

• peu d'organisations ont un programme d'Insider Threat

• parmi les menaces identifiées, exfiltration de données, fraude, sabotage... les enjeux RH (profil, contexte pays, radicalisation, départs sensibles) sont souvent gérés sans cadre commun

• les frontières entre risque géopolitique et risque interne deviennent floues

Les participants appellent à sortir du déni et des tabous sur les attaques internes, et à intégrer un cadre avec les RH, le juridique et la conformité dans une démarche commune.

6. Géopolitique et analyses de risques, une bascule méthodologique

De la cybercriminalité aux conflits d'Etats, les RSSI reconnaissent massivement que la reconfiguration mondiale influence leurs analyses de risques. Pourtant, seuls quelques-uns ont formalisé cette dimension dans leurs méthodes existantes.

Les priorités identifiées :

• cartographier les dépendances critiques (pays, fournisseurs, cloud, OT)

• introduire États, alliances et lutte informationnelle dans les scénarios de risques,

• renforcer les compétences internes (cyber + géopolitique),

• agir avec EBIOS RM, moduler la méthode pour intégrer l'axe géopolitique

• faire circuler l'information entre métiers, juridique, conformité et achats.

7. Guerre informationnelle, anticiper, détecter, réagir

Les entreprises sont des cibles directes de campagnes de déstabilisation, d'amplification de la désinformation, de deepfakes ou de narratifs hostiles.

Les RSSI doivent désormais :

• installer un socle commun de compréhension du risque et se synchroniser avec les équipes communication, RH, affaires publiques ;

• structurer une veille OSINT et réputationnelle ;

• détecter les signaux faibles (comportements humains, narratifs, surveillance des flux internes,...) ;

• organiser une réponse coordonnée incluant communication de crise et investigation.

8. Supply chain mondiale, une fragilité structurelle majeure

60% des attaques proviennent des tiers et 92% des entreprises ont recours à l'outsourcing.

Les organisations doivent :

• créer un registre de gestion des tiers,

• concentrer l'effort sur les prestataires réellement critiques,

• évaluer régulièrement leur posture de sécurité (questionnaires, scans, audits),

• impliquer le Board dans le suivi des tiers à fort impact.

NIS2 et DORA renforcent cette obligation de contrôle.