# Cyber Security Threat Radar 2023/2024

Renforcer la cyberrésilience

swisscom

# Table des matières

# Cyber Security Threat Radar

## Renforcer la cyberrésilience

En ces temps tourmentés et difficiles, les entreprises et les organisations doivent impérativement pouvoir se montrer résistantes. Outre la santé physique et des systèmes informatiques stables et redondants, cette résistance suppose des directives claires servant de garde-fous pour favoriser une meilleure orientation.

Le présent Cyber Security Threat Radar souligne le fait que la protection contre les risques cybernétiques et la réduction des risques ne sont pas des processus unilatéraux et ne relèvent pas de la responsabilité exclusive du service informatique. La cybersécurité est un enjeu majeur qui requiert l'implication de chaque membre de la direction de l'entreprise.

Cette année, le Cyber Security Threat Radar n'aborde pas le quatrième volet des cybermenaces, à savoir l'observation. Ce sujet fait déjà partie intégrante de l'ADN de Swisscom en matière de sécurité et constitue un élément clé de nos activités quotidiennes.

Le présent Radar identifie le thème «Désinformation & Déstabilisation» comme l'un des défis majeurs de notre époque. La diffusion de fausses informations, de contenus manipulés et d'actions de propagande ciblées peut exercer une influence sur des sociétés entières, perturber les processus politiques et miner la confiance dans les institutions. Cette menace a été classée comme le plus grand risque à court terme également par les spécialistes du Global Risks Report 2024 du Forum économique mondial (FEM). Les thèmes abordés dans cette édition du Radar ne sont bien entendu pas exhaustifs.

La loi révisée sur la protection des données, entrée en vigueur en Suisse en septembre dernier, et la nouvelle loi sur la sécurité de l'information (LSI) replacent les aspects liés à la gouvernance sur le devant de la scène. Les évolutions futures s'annoncent passionnantes. J'espère que vous trouverez dans cette nouvelle édition du Cyber Security Threat Radar de précieuses informations qui vous aideront à développer la cybersécurité dans votre entreprise ou votre organisation.

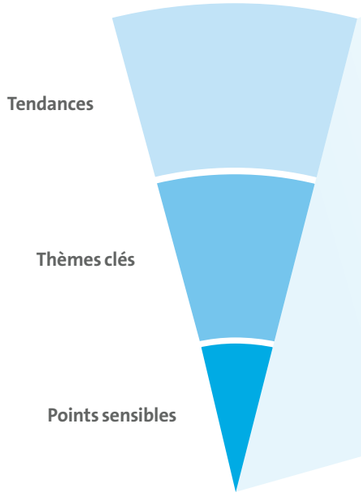
**Marco Wyrsch**
Head of Group Security
Swisscom (Schweiz) AG

*« C'est en surveillant et en observant notre réseau que nous pouvons améliorer en permanence la sécurité de la Suisse. Car les cyberrisques resteront dans les années à venir l'un des principaux dangers pour les organisations, les entreprises et la société en général. »*

# État des lieux – radar des menaces

Pouvoir recourir en temps utile à des stratégies et des procédures de sécurité consolidées et éprouvées nous aide à faire face aux événements imprévisibles, aussi appelés «cygnes noirs». Lorsque celles-ci s'accompagnent d'une culture de la sécurité rigoureuse, de transparence sur les erreurs et d'une formation adéquate du personnel, les bases de la résilience organisationnelle sont jetées.

Mais encore faut-il identifier en amont les menaces potentielles et les saisir de façon systématique. Pour faire le point sur le niveau de menace et son évolution, nous nous appuyons sur le Cyber Security Threat Radar.



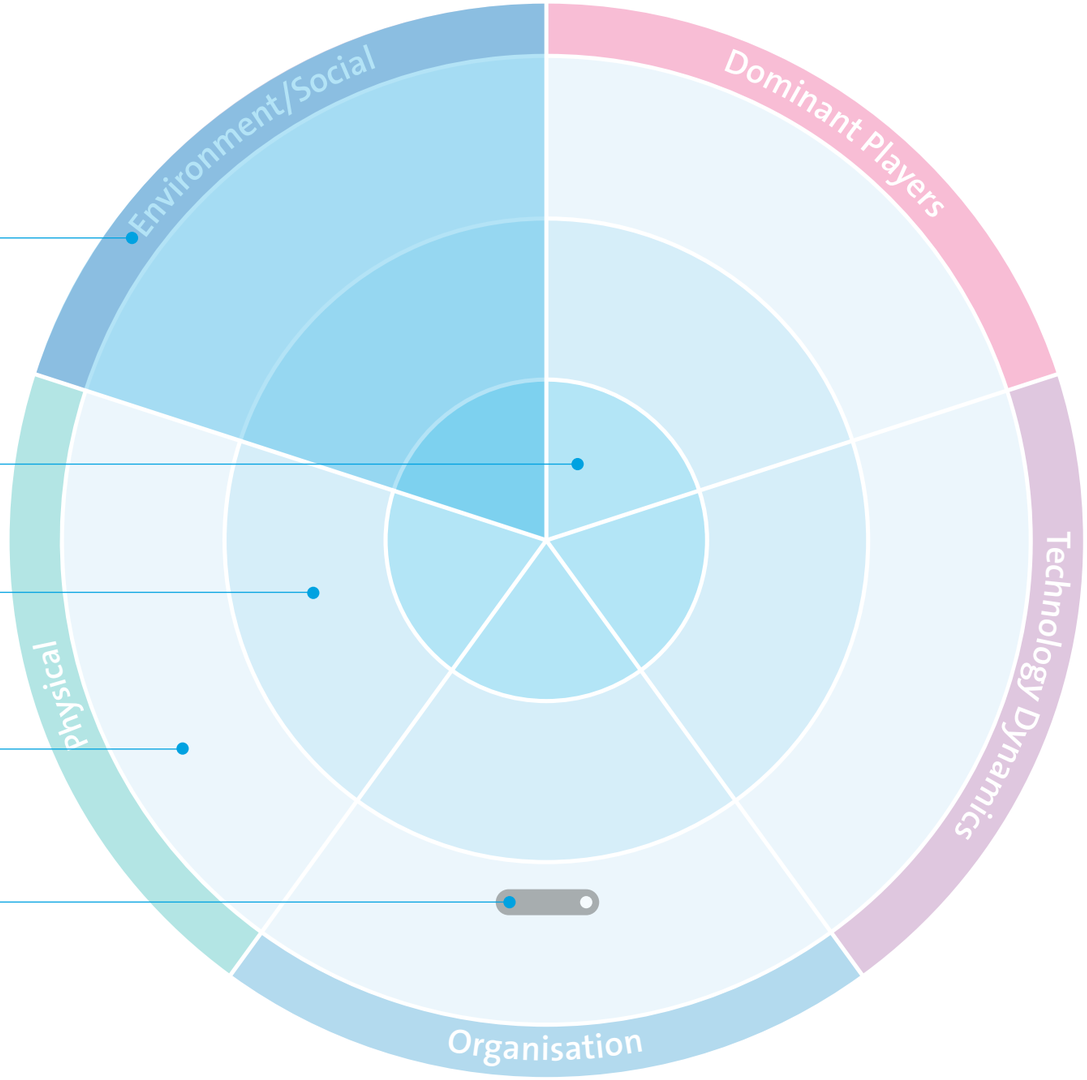

# Méthodologie

Le radar des menaces se divise en cinq **segments** qui délimitent les différents domaines de menace. Dans chaque **segment,** les menaces associées peuvent être affectées à l'un des trois cercles concentriques. Les cercles indiquent si la menace en question est actuelle ainsi que le degré d'incertitude quant à son évaluation. Plus la menace est proche du centre du cercle, plus elle est concrète et plus il est important de prendre les contre-mesures adéquates.

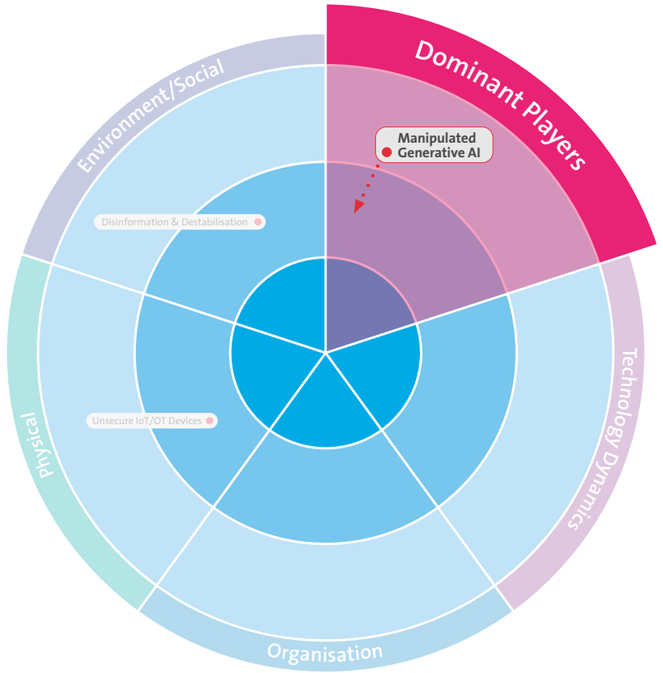
**Ces cercles mettent en évidence:**

- des **points sensibles** pour les menaces déjà réelles dont la gestion nécessite de mobiliser des ressources relativement importantes.
- des **thèmes clés** pour les menaces déjà survenues de manière ponctuelle et dont la gestion nécessite de mobiliser des ressources normales. Il existe souvent des processus bien définis pour gérer efficacement les menaces de ce genre.
- des **tendances:** détection précoce des menaces qui ne sont pas encore survenues ou dont l'impact reste très faible à ce stade. Des projets ont été lancés pour pouvoir réagir très tôt à ces menaces, qui vont gagner en importance dans le futur.

Par ailleurs, les différentes **menaces** identifiées par ces points suivent une **tendance** dont la criticité est en progression, en baisse ou stable. La longueur du faisceau de la tendance symbolise la rapidité avec laquelle le niveau de criticité de la menace va évoluer.



# Manipulated Generative AI ou dans quelle mesure peut-on manipuler l'intelligence artificielle?




Ces 15 dernières années, la généralisation de la numérisation, de la virtualisation et de l'utilisation du Cloud a contribué à la propagation rapide de l'IA générative. Le lancement de ChatGPT en novembre 2022 a connu un écho médiatique retentissant. L'IA générative a rapidement fait son entrée dans la société. De nombreuses entreprises innovantes se sont laissé gagner par l'enthousiasme et commercialisent depuis un grand nombre de nouvelles applications.

L'intérêt mondial pour l'IA a également placé le thème de la sécurité au cœur du débat. Des questions sur les risques de sécurité se sont rapidement posées et ont appelé des réponses, les innovations ayant comme toujours un côté obscur. En dépit des progrès significatifs accomplis par l'IA et l'apprentissage automatique, ces technologies restent vulnérables aux attaques. De nouvelles normes, telles que l'AI Act au niveau réglementaire, sont encore en cours du développement dans de nombreux sous-secteurs. Il faut donc s'attendre à quelques inconnues auxquelles on ne peut se préparer que partiellement.

Dans le contexte de la cybersécurité, les systèmes d'IA sont visibles dans trois domaines:

1. Utilisation de systèmes d'IA pour le lancement d'attaques: citons par exemple le perfectionnement d'attaques connues telles que la fraude au CEO et la compromission de messagerie d'entreprise (BEC, Business Email compromise) par le biais de vidéos générées par l'IA au lieu de simples e-mails; mails d'hameçonnage plus réalistes → attaques basées sur l'IA.

2. Utilisation de l'IA pour identifier les attaques (p. ex. dans les filtres anti-spam et anti-hameçonnage) et se défendre, détecter des anomalies dans le trafic du réseau, soutenir le flux de travail dans la cyberdéfence (p. ex. en tant que copilote), automatiser les étapes d'analyse, établir la chronologie des incidents ou communiquer avec les utilisateurs. D'autres solutions de sécurité intelligentes et automatisées devraient voir le jour.

3. Les failles de sécurité dans les systèmes d'IA utilisés – nous parlons ici de l'intelligence artificielle manipulable, concrètement abordée dans:
   l'OWASP Top 10 pour les applications LLM (owaspai.org) et/ou le MITRE ATLAS (atlas.mitre.org).
   Il s'agit donc des risques liés à la sécurité de l'IA et non à l'utilisation des systèmes d'IA.

Au-delà des nombreuses possibilités d'attaques, les thèmes suivants sont selon nous particulièrement pertinents dans le troisième domaine:

- **Manipulation des inputs (injections de prompts, p. ex.)**
  Ces attaques visent, via une manipulation des entrées, à contourner les mécanismes de sécurité existants afin d'amener l'exploitant du système d'IA à produire des résultats non intentionnels. Il peut par exemple s'agir de la divulgation d'informations confidentielles ou de la génération de contenus ou d'actions indésirables.

- **Attaques par empoisonnement**
  Dès la phase d'entraînement des systèmes d'IA, l'introduction de données malveillantes, fausses ou corrompues permet de manipuler le système. Un langage inapproprié peut par exemple être inséré dans des enregistrements vidéo de sorte qu'un chatbot interprète ces cas comme suffisamment généraux pour les utiliser dans les interactions avec la clientèle.

- **Supply chain attacks**
  Il s'agit d'attaques dirigées contre les composants externes du système d'IA, telles que l'introduction de codes malveillants dans des bibliothèques open source utilisées dans un modèle d'IA.

Par ailleurs, le risque de DoS (Denial of Service) subsiste. Un utilisateur peut par exemple épuiser avec une entrée, volontairement ou non, toutes les ressources disponibles et ainsi paralyser le système.

D'autres risques liés à l'IA doivent également être rapidement mentionnés, tels que le Shadow AI, qui désigne l'utilisation incontrôlée des systèmes d'IA par des membres du personnel, portant ainsi atteinte à la confidentialité des données de l'entreprise, de la clientèle, ou d'autres données sensibles. La sécurité du système se trouve alors compromise. Il convient de garantir la protection des données d'entreprise confidentielles et la fiabilité du système d'IA.

*« Les caractéristiques probabilistes de l'IA générative et des LLM créent de nouveaux défis et risques en matière de sécurité. Une connaissance approfondie du fonctionnement des LLM est indispensable pour pouvoir définir et mettre en œuvre les bonnes mesures de sécurité. »*

**Beni Eugster**
Swisscom Outpost



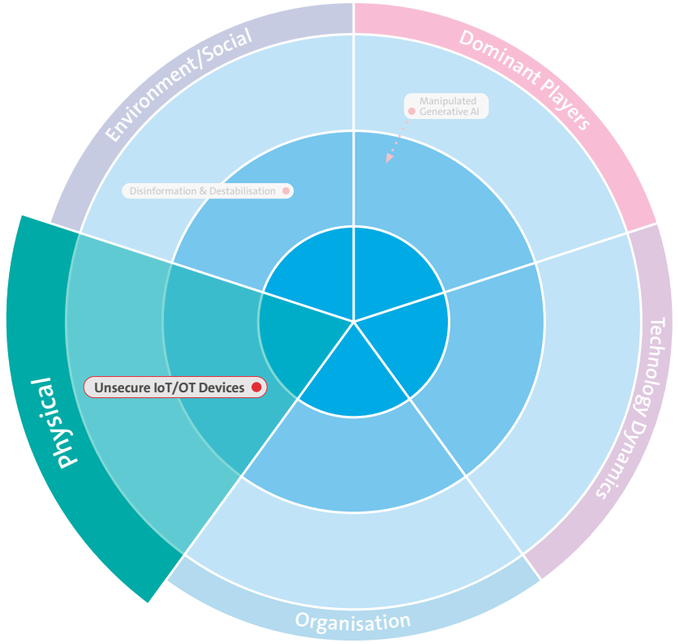
Sur quels aspects de la gestion des risques de l'intelligence artificielle les entreprises et les organisations doivent-elles se concentrer?

- Observer les évolutions actuelles et réagir rapidement aux changements.
- Former les collaboratrices et les collaborateurs
- Analyser minutieusement les risques avant d'utiliser les systèmes d'IA (y compris de tiers), afin d'identifier l'impact possible.
- Contrôler et mettre en œuvre des mesures de sécurité à tous les niveaux du cycle de vie de l'IA. Tenir compte des contrôles de sécurité de NIST AI RMF, MITRE ATLAS et OWASP pour la sécurité de l'IA.
- Entretenir de bonnes relations entre les équipes en charge de l'IA et de la sécurité. Adapter régulièrement les règlements et directives en fonction des nouveaux développements.
- Élaborer des instructions pour l'utilisation de l'IA au sein de l'organisation.
- Conditions-cadres légales: l'AI Act impose déjà des mesures de sécurité spécifiques pour les systèmes d'IA à risque ou restreint leur utilisation. La législation sur l'IA de l'UE a un effet extraterritorial et vaut ainsi, sous certaines conditions, pour les entreprises suisses. Les droits d'auteur et la responsabilité en cas d'utilisation du système d'IA de tiers en tant que solution SaaS constituent toutefois également des risques à ne pas négliger.

*« Les défis qu'implique la gestion des risques de sécurité de l'IA vont se multiplier sous l'effet de l'évolution rapide de l'environnement de l'IA, et ce à un rythme soutenu. Il convient donc d'observer en permanence les développements actuels afin de pouvoir réagir rapidement aux changements. »*

**Raiko Zwilling**
Security Officer Group Companies

# Risques de sécurité liés à la numérisation croissante, y compris dans les ateliers et les salles d'opération




Dans un monde actuel complexe et interconnecté, les appareils IoT (Internet of Things) et OT (Operational Technology) jouent un rôle central dans l'activité quotidienne de secteurs variés. Dans ce contexte, la technologie prend en charge un grand nombre de tâches, des plus simples au plus complexes: applications de Home Entertainment et Smart Home, contrôle des systèmes de fabrication dans les entreprises industrielles, ou encore surveillance des infrastructures critiques.

L'interconnexion croissante de ces appareils présente toutefois des risques importants en matière de sécurité. Les appareils IoT/OT non sécurisés ou faiblement protégés peuvent être compromis et sabotés, et ainsi offrir une porte d'entrée pour les cyberattaques. En plus d'être limités dans leur propre fonctionnement, au niveau de la disponibilité ou de l'intégrité des données par exemple ils peuvent représenter une menace pour la sécurité physique et le bien-être des personnes. Compte tenu des dommages considérables qui peuvent résulter des attaques sur les systèmes IoT/OT, leur sécurité est primordiale.

Les risques liés aux appareils IoT/OT non sécurisés sont multiples et peuvent varier selon le champ d'application. Les principaux dangers sont les suivants:

- **Interruption de l'exploitation**
  Une atteinte à la sécurité peut entraîner un arrêt temporaire ou permanent des systèmes critiques et ainsi provoquer des pertes de production et des préjudices financiers considérables.

- **Vol de la propriété intellectuelle et perte ou vol de données**
  Les accès non autorisés aux appareils IoT/OT peuvent entraîner le vol de données sensibles, y compris de la propriété intellectuelle et d'informations confidentielles, ce qui peut affaiblir l'avantage concurrentiel d'une entreprise et générer des violations de la protection des données et des pertes financières.

- **Manipulation des données de l'appareil et sabotage**
  Les pirates informatiques peuvent manipuler les appareils IoT/OT pour produire de fausses informations, dont résultent des décisions ou des produits erronés. Dans les environnements industriels, les pirates peuvent paralyser ou manipuler des infrastructures critiques, ce qui peut provoquer des pannes, voire mettre en péril la sécurité humaine.

- **Infiltration du réseau**
  Une fois compromis, les appareils IoT/OT servent de tremplin pour pénétrer plus profondément dans les réseaux et causer d'autres dommages. Les appareils peuvent être infiltrés par des ransomwares qui bloquent des fonctions importantes ou verrouillent des données jusqu'au paiement d'une rançon. Ils sont parfois intégrés dans des réseaux de robots et menacent alors les autres systèmes.

- **Violations de la conformité**
  Dans les entreprises actives dans des secteurs réglementés, des failles de sécurité dans les systèmes IoT/OT peuvent entraîner des violations des lois sur la protection des données ou des normes industrielles et exposer ces entreprises à des amendes et à des sanctions. Le Cyber Resilience Act européen jouera à l'avenir un rôle particulièrement important dans le domaine de la responsabilité du produit. Les dommages potentiels et l'impact financier des appareils IoT/OT non sécurisés sont considérables: pertes économiques, atteinte à la sécurité publique, interruption de services critiques ou encore perte de la confiance du public. Dans les cas extrêmes, les attaques sur les systèmes OT de l'infrastructure critique peuvent même entraîner des catastrophes écologiques ou des risques pour la vie humaine.

Outre les charges directes qu'impliquent la résolution des violations de la sécurité et la remise en état des systèmes touchés, les entreprises font également face à des charges indirectes, tels que les pertes de chiffre d'affaires liées aux interruptions de l'exploitation, les indemnités versées aux clients ou partenaires commerciaux concernés, et les hausses des primes d'assurance.

Les difficultés qu'impliquent les systèmes OT sont les suivantes:

- ils disposent parfois d'accès au service à distance, disponibles via Internet;
- ces systèmes sont dotés de technologies à la fois très anciennes mais aussi nouvelles et complexes; il existe des protocoles et des appareils hérités, où certains mécanismes de sécurité (cryptage, authentification, etc.) font défaut, et des réseaux autrefois séparés sont désormais interconnectés sous l'effet de la numérisation croissante;
- la quasi-totalité des spécialistes et du soutien technique disponibles a disparu (p. ex. versions obsolètes de Windows, ordinateur portable avec connexion RS232, etc.);
- un décalage subsiste entre la sécurité et la sûreté, générant des objectifs contradictoires, tels que la protection de l'accès par mot de passe vs. la possibilité d'intervenir rapidement en cas de danger.
- la génération des babyboomers, qui maîtrise ces systèmes, part en retraite;
- une pression réglementaire accrue pour les exploitants (NIS2, DORA, etc.) et les fabricants (RED2, CRA, etc.);
- une méconnaissance de l'importance de la sécurité ou une attribution mal définie des responsabilités en matière de sécurité dans les organisations.



Compte tenu de ces défis, les entreprises doivent adopter des mesures proactives pour sécuriser leurs appareils IoT et OT:

- **Évaluation des risques**
  Évaluations de la sécurité et audits réguliers afin d'identifier les failles potentielles et d'y remédier.

- **Directives de sécurité**
  Il est important de développer et de mettre en œuvre des directives de sécurité qui reposent sur des normes éprouvées telles que la série IEC 62443. Ces directives permettent une configuration et une gestion sécurisées des appareils IoT/OT. L'approche «security by design» favorise par ailleurs la sécurité dès le développement des appareils.

- **Maintien à jour de la technologie**
  Actualiser et patcher les systèmes devenus obsolètes, maîtriser la gestion des vulnérabilités, et le cas échéant, segmenter le réseau.

- **Formation des collaboratrices/collaborateurs et des techniciens de service**
  Sensibiliser et former à l'utilisation des appareils IoT/OT afin de limiter les erreurs humaines.

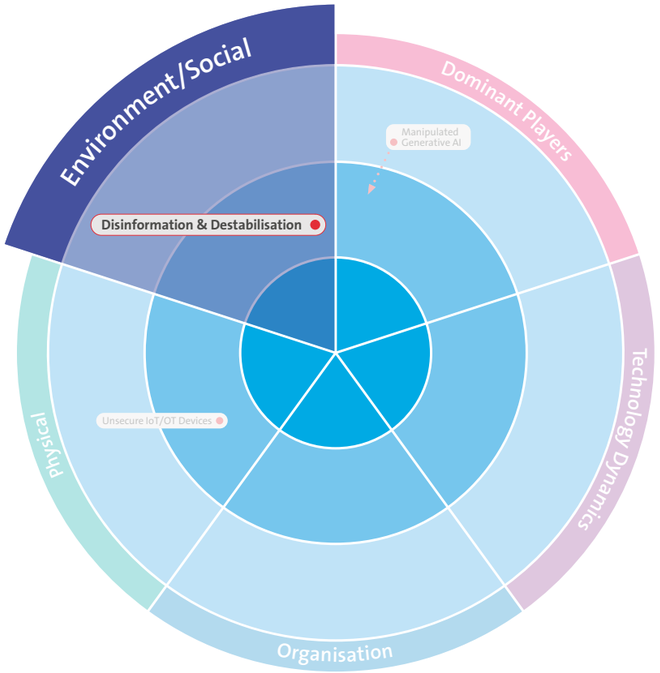
- **Surveillance active et contrôles**
  Effectuer des contrôles de sécurité réguliers et surveiller en permanence les systèmes.

- **Collaboration avec des prestataires de confiance**
  Choisir des appareils et des logiciels de prestataires qui accordent une importance avérée à la sécurité et fournissent des mises à jour régulières.

*« La sécurité des infrastructures IoT et OT constitue pour les entreprises une tâche qui ne doit pas être sous-estimée. Son importance est cruciale pour le maintien de la sécurité opérationnelle et le succès commercial à long terme. La sécurité des systèmes OT n'est pas une option et il convient de lui accorder la même importance qu'à celle des systèmes informatiques. »*

**Thomas Dummermuth**
Head Physical Security & Safety, BCM

# Désinformation et déstabilisation: une réalité?




La désinformation est à l'heure actuelle un enjeu majeur pour les entreprises. Compte tenu de la croissance exponentielle des plateformes numériques et de la rapidité à laquelle les informations peuvent se propager, les entreprises doivent relever un double défi: protéger l'intégrité de leurs informations tout en luttant contre les fausses informations qui peuvent porter atteinte à leur marque, leur activité et leurs normes de sécurité.

Le Global Risks Report 2024 du Forum économique mondial (FEM) souligne que la désinformation constitue un défi social et ainsi une menace pour les entreprises et les organisations. Les fake news générées par l'IA et les cyberattaques représentent le plus grand risque immédiat, en particulier dans la perspective des élections à venir dans plusieurs grands pays tels que les États-Unis, la Grande-Bretagne et l'Inde.

Les entreprises sont elles aussi de plus en plus la cible de campagnes de désinformation visant à nuire à leur image, tromper les consommateurs, voire à influencer leur valeur boursière. À une époque où les informations sont diffusées dans le monde entier en quelques secondes, la capacité d'une entreprise à réagir efficacement à la désinformation est capitale pour préserver son intégrité et la confiance des parties prenantes.

Outre les menaces externes, telles que l'altération de la perception du public, les risques liés à la désinformation présentent également des menaces internes, comme la diffusion, au sein d'une entreprise, de fausses informations pouvant entraîner de mauvaises décisions et des failles de sécurité. Les spécialistes en sécurité soulignent que la sécurité des données et des infrastructures des entreprises est étroitement liée à la capacité d'identifier et de combattre la désinformation. C'est précisément le développement rapide de l'IA et l'évolution des IA génératrices d'images et de vidéos qui en résulte qui permettent de mener des attaques par deep fake et des campagnes de désinformation difficiles à identifier avec des moyens traditionnels.

Dans le contexte de la cybersécurité, les campagnes de désinformation peuvent potentiellement nuire à l'opinion publique, mais aussi aux protocoles de sécurité internes des entreprises et des organisations. Les pirates informa-

tiques peuvent utiliser la désinformation pour orchestrer des attaques par hameçonnage, semer l'incertitude, et inciter le personnel à divulguer des informations confidentielles ou à exécuter des actions préjudiciables. Le thème «Disinformation & Destabilisation» se retrouve également dans les vecteurs d'attaque «AI-Based Attacks» et «Big Data Analytics». L'identification de la désinformation et le processus de défense correspondant doivent par conséquent constituer une composante importante des normes de sécurité des entreprises.

### Stratégies de gestion de la désinformation pour les entreprises

1. **Renforcement des canaux de communication internes:** une stratégie de communication interne claire et transparente est essentielle pour s'assurer que les collaboratrices et les collaborateurs reçoivent et diffusent des informations correctes.

2. **Formation et sensibilisation:** les collaboratrices et les collaborateurs doivent être formés régulièrement afin de pouvoir identifier la désinformation et y réagir correctement. Ils doivent pour cela bien comprendre les risques qu'implique la diffusion de fausses informations.

3. **Utilisation des technologies:** l'intelligence artificielle et l'apprentissage automatique peuvent aider les entreprises à identifier rapidement des campagnes de désinformation. L'IA peut aider à analyser la diffusion de fausses informations, à identifier leurs sources et à prendre les contre-mesures appropriées.

4. **Relations publiques proactives et gestion de crise:** en cas d'attaque de désinformation, une réaction rapide et décisive s'impose. Les entreprises doivent concevoir des plans préparatoires afin de pouvoir réagir à la désinformation, y compris en collaborant avec les médias et en utilisant leurs propres canaux, et ainsi diffuser des informations correctes.

5. **Partenariats et coopérations:** la collaboration avec des spécialistes externes ou d'autres entreprises et organisations peut offrir des perspectives intéressantes sur les meilleures pratiques en matière de gestion de la désinformation et encourager la définition de normes et de réactions communes.



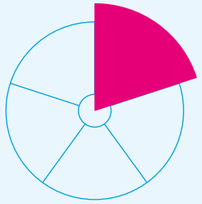
Les entreprises doivent identifier la désinformation comme une menace sérieuse pour leur activité commerciale et leur réputation. Dans son étude de sécurité sur les attaques de désinformation dans les entreprises, l'Allianz für Sicherheit in der Wirtschaft e. V. (Alliance pour la sécurité dans l'économie) a, dès 2019, introduit la protection contre la désinformation comme quatrième quadrant de son focus sur la sécurité – à juste titre.

Le Global Risks Report 2024 du FEM rappelle que la lutte contre la désinformation constitue une composante cruciale de la sécurité et de la stratégie des entreprises. La mise en œuvre d'une stratégie globale intégrant l'information, la technologie et l'engagement proactif garantit aux entreprises une protection efficace, pour elles-mêmes et pour leurs parties prenantes. À une époque où la frontière entre la vérité et les fausses informations s'estompe de plus en plus, les entreprises doivent impérativement être en première ligne pour préserver l'intégrité et la fiabilité de leurs informations.

*« La diffusion délibérée de fausses informations, également appelées fake news, peut entraîner une déstabilisation économique et sociale. Le cyberespace est également utilisé à cette fin. Les entreprises doivent avoir conscience de ce danger afin de pouvoir se préparer et réagir de manière appropriée à ce type de menace. »*

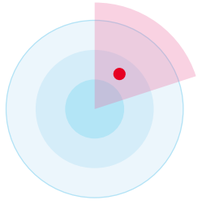
**Marcus Beyer**
Security Professional &
Security Awareness Officer

# Détails, y compris tendances et comparaison par rapport à l’année précédente



## Dominant Players

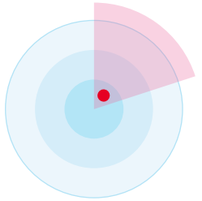
**Ce segment inclut les menaces résultant des interdépendances entre les principaux fabricants, services ou protocoles.**



**Concentration Data & Cloud Services**
La forte centralisation des données dans le Cloud induit des risques cumulés. La défaillance d’un service notamment centralisé peut avoir des répercussions dans le monde entier.

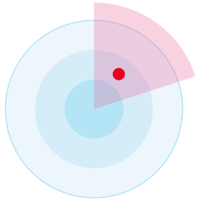
► Inchangé





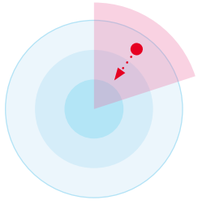
**Infrastructure Integrity**
Des vulnérabilités peuvent avoir été intégrées délibérément ou par négligence dans des composants essentiels des infrastructures critiques, compromettant ainsi la sécurité du système.

► Inchangé



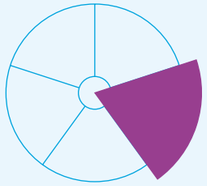
**Legacy Protocols**
En raison de dépendances logicielles, des protocoles totalement obsolètes et vulnérables (p. ex. NTLMv1, SMBv1, RC4) sont encore utilisés. Quelques applications peuvent ainsi compromettre la sécurité d’infrastructures complètes.

► Inchangé



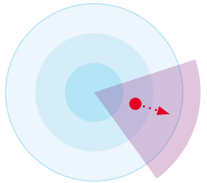
**Manipulated Generative AI**
Des manipulations ciblées permettent de modifier les résultats d’un système d’IA. L’objectif est alors d’introduire des données malveillantes, fausses ou corrompues dès la phase d’entraînement, de voler des modèles LLM, ou de générer des prompts qui peuvent avoir des effets indésirables et juridiquement contraignants.

▲ Croissant



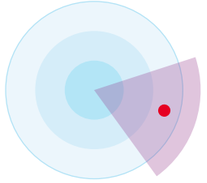
# Technology Dynamics

**On entend par là les menaces qui découlent d'une innovation technologique fulgurante et profitent de la disponibilité de plus en plus simple et bon marché des supports et de l'expertise informatiques. Conséquence: davantage de surfaces d'attaque, disponibilité accrue des outils correspondants et nouvelles opportunités pour les hackers de créer de nouvelles menaces inhérentes au développement.**



**5G Security**
La 5G est une technologie mobile encore récente. Son déploiement génère de nombreuses opportunités, mais s'accompagne aussi de menaces encore inconnues.

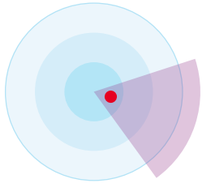
▼ Décroissant



**Quantum Computing**
Les ordinateurs quantiques peuvent rendre inutiles les procédés cryptographiques actuels car ils sont en mesure de les contourner en très peu de temps.

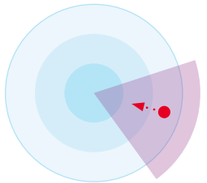
► Inchangé





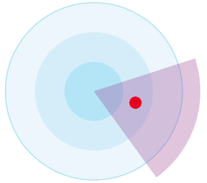
**Ransomware**
Les données critiques sont cryptées en masse puis (éventuellement) décryptées moyennant le versement d'une rançon.

► Inchangé



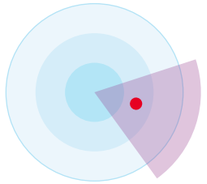
**Increased Complexity**
La complexité des systèmes, en particulier au-delà des limites des technologies et des entreprises, ne cesse de croître. Les paysages IT se complexifient d'autant plus dans un environnement hybride/multicloud intégrant de nombreux fournisseurs de cloud. L'exposition aux risques augmente d'autant et la recherche d'erreurs devient plus difficile.

▲ Croissant



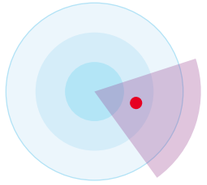
**AI-Based Attacks**
Les attaques basées sur l'intelligence artificielle (IA) sont plus ciblées et donc plus difficiles à détecter. L'IA les rend plus efficaces sur les vecteurs d'attaque classiques tels que le ransomware, le phishing, le spear-phishing, ainsi que sur de nouveaux modes opératoires moins répandus comme les deepfakes et la désinformation.

► Inchangé



**Targeted Attacks**
Attaques ciblées et complexes poursuivant un objectif concret. Des personnes clés sont identifiées et ciblées directement ou indirectement (Lateral Movement, méthodes d'ingénierie sociale) afin d'obtenir des informations sensibles ou de causer un maximum de dommages. L'une des principales caractéristiques de ces attaques est la persistance: les hackers agissent le plus longtemps possible sans se faire repérer et un changement est opéré au niveau des canaux d'attaque (du mail au SMS et même au courrier).

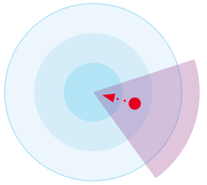
► Inchangé



**Attaques DDoS**
Une attaque par Distributed Denial-of-Service (DDoS) est une tentative malveillante visant à perturber le trafic de données normal d'un serveur, d'un service ou d'un réseau cible en inondant la cible ou son infrastructure d'un flot de trafic Internet. L'efficacité des attaques DDoS repose sur l'utilisation de plusieurs systèmes informatiques compromis comme sources de trafic hostile. Les machines exploitées peuvent être des ordinateurs et d'autres ressources situées sur le réseau telles que les appareils IoT. Une croissance forte associée à une faible protection des appareils IoT accroît les prises de contrôle potentielles par le biais des botnets.

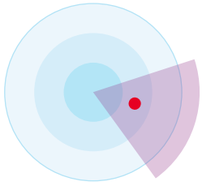
► Inchangé





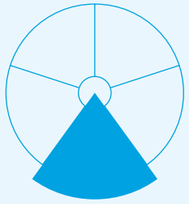
**Supply Chain Attacks**
Les attaques sur la chaîne d'approvisionnement visent à tirer parti des relations de confiance et d'affaires entre une entreprise et des parties externes. Il peut s'agir de partenariats, de relations avec les fournisseurs ou de l'utilisation de logiciels de tiers.

▲ Croissant



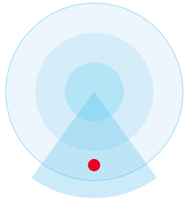
**Subscriber Compromise**
Des logiciels malveillants se créent un accès aux données privées des utilisateurs mobiles ou sont utilisés pour cibler les infrastructures IT ou de télécommunication. Les attaques de phishing, smishing, vishing et MFA Bypass ciblent les Subscriber Credentials. Des identités numériques complètes sont dérobées et reprises aux cours des attaques consécutives.

► Inchangé



# Organisation

**Menaces résultant des changements dans l'organisation ou exploitant les failles qui y sont présentes.**



**Workplace Heterogeneity**
Malgré les nombreuses opportunités qu'offrent les nouveaux modèles de travail comme le «Bring Your Own Device» (BYOD) et le recours accru au télétravail, la mise en place incontrôlée de ce type de modèles expose davantage aux risques.

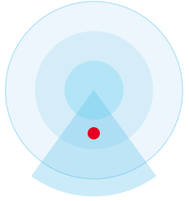
► Inchangé

**Decentralised Development & Operations**
Les départements de développement classiques périclitent tandis que le développement des applications est davantage confié aux Business Units, avec des cycles de release de plus en plus courts. Le contrôle et la gestion de la sécurité deviennent ainsi compliqués.

► Inchangé

**Insider Threat**
Des partenaires ou des collaborateurs manipulent, détournent ou vendent des informations par négligence ou de façon intentionnelle.

► Inchangé



**Digitalisation**
L'interconnexion croissante entre le monde réel et le monde virtuel dans la vie privée et professionnelle multiplie l'éventail des vecteurs d'attaque. Le nouveau modèle «New Work» et la transposition opérée dans des environnements de télétravail renforcent également les cyberrisques et la vulnérabilité de l'infrastructure IT en raison des équipements terminaux non sécurisés.

► Inchangé

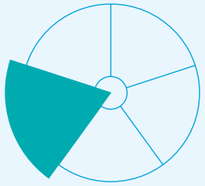
**Security Skills**
La complexité des cyberattaques et la progression de la numérisation rendent les Security Skills et le recours à des cyberprofessionnels indispensables dans l'organisation. Une menace de «Downskilling», à savoir le désapprentissage des connaissances lié à l'automatisation dans l'informatique peut générer de nouveaux vecteurs d'attaque, par exemple si les installations SCADA ne peuvent plus être utilisées et entretenues par le personnel qualifié.

► Inchangé

**Infrastructure Misconfiguration**
Exploitation de composants de l'infrastructure mal configurés et/ou de vulnérabilités identifiées et corrigées tardivement. L'automatisation renforcée des processus d'exploitation techniques aura des conséquences plus importantes en cas d'attaques efficaces ou de configurations erronées.

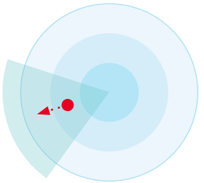
► Inchangé





# Physical

**Ce terme désigne les attaques sur l'infrastructure du cyberespace qui causeront de plus en plus de dommages dans le monde physique. Il inclut également les menaces émanant de l'environnement physique et généralement davantage axées sur des cibles physiques.**



**Energy Instability**
Attaques sur des infrastructures critiques telles que celles des exploitants du réseau électrique. La sûreté de fonctionnement est essentielle et la Business Continuity alimente de plus en plus le débat sur la cyberrésilience. La pénurie d'électricité, le blackout (panne générale d'électricité) ou même blue-out (défaillance générale de l'alimentation en eau), entre autres, sont des points importants. Selon les médias, les infrastructures critiques sont nettement plus vulnérables aux cyberattaques.

▼ Décroissant



**Targeted Sabotage**
Attaques ciblées contre des infrastructures, des installations d'approvisionnement et des connexions, qui peuvent restreindre de manière considérable le fonctionnement d'Internet. Le sabotage ciblé des câbles à fibre optique sensibles se développe actuellement et constitue un danger qui doit être surveillé. Compte tenu de la difficile mise en œuvre des contre-mesures, il convient de miser sur une détection rapide et sur des solutions alternatives.

► Inchangé





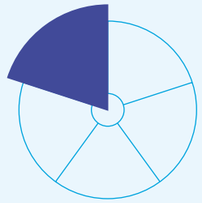
**Unsecure IoT/OT Devices**
Qu'il soit déployé dans des technologies opérationnelles (OT) pour la surveillance et la gestion de processus, des appareils et infrastructures physiques ou dans des appareils IoT, l'Internet des objets est omniprésent. Des tâches très variées – des plus simples au plus complexes – y sont exécutées, des applications de Home Entertainment à la surveillance d'infrastructures critiques (CI), en passant par le pilotage de robots dans les ateliers de production. Les appareils faiblement protégés, quelle que soit leur nature, peuvent être compromis et sabotés. Ils peuvent ainsi voir leurs propres fonctions restreintes, par exemple leur disponibilité ou l'intégrité des données.

► Inchangé



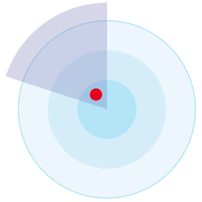
**Environmental Influence**
La crise climatique entraîne une augmentation des phénomènes et des influences météorologiques imprévisibles (chaleur, fortes pluies, tornades, grêle, éclairs de forte intensité, etc.), qui peuvent occasionner des dommages à l'infrastructure des organisations et des entreprises et ainsi avoir un fort impact sur l'environnement externe et interne d'un système d'information ou d'un réseau.

► Inchangé



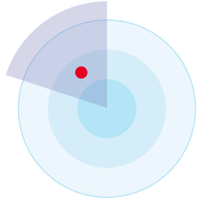
# Environment/Social

**Il s’agit des menaces émanant directement des changements sociaux et politiques ou consécutives à ces changements, qui simplifient la tâche des hackers et rendent donc les attaques plus profitables.**



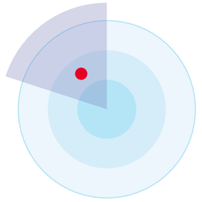
**Security Job Market**
Les besoins énormes en professionnels de la sécurité sont très difficiles à satisfaire. Il en résulte une perte de savoir-faire dans la lutte contre des attaques de plus en plus complexes et intelligentes.

► Inchangé



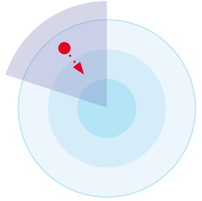
**Digital Identity**
Les identités numériques personnelles certifiées peuvent être usurpées ou volées, par exemple dans le but de conclure des contrats au nom de tiers.

► Inchangé



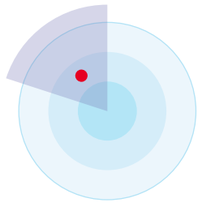
**Disinformation & Destabilisation**
La diffusion intentionnelle d’informations erronées peut entraîner une déstabilisation économique et sociale. Son utilisation ciblée dans les scénarios de crise, y compris via le cyberespace, se développe de plus en plus.

► Inchangé



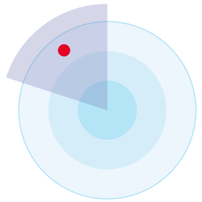
**Political Influence**
Les forces politiques peuvent influencer les décisions d’ordre technologique ou économique, par exemple dans le choix des fournisseurs de technologie. Il peut en résulter de nouveaux risques.

▲ Croissant



**Big Data Analytics**
Le volume accru de données et les modèles d'analyse améliorés peuvent être utilisés abusivement pour influencer le comportement des individus. Les décisions sont de plus en plus souvent confiées à des systèmes autonomes. Les données des «Big Data Lakes» sont utilisées de manière ciblée à des fins de désinformation, de fake news, d'analyses sociétales et psychosociales, ainsi que pour créer des modèles de mouvement. Ce dernier point induit une violation de la sphère privée.

- Inchangé



**Geopolitical Situation / State Level Attacks**
En périodes de guerres, de terreur et d'instabilité politique au sein des pays et des sociétés, les conséquences négatives dans le cyberespace tendent à s'accentuer. Il s'agit de piratages commandités par différents pays et groupes de hacktivistes à motivation politique, d'acteurs étatiques et de réseaux de criminalité organisée, qui exercent une pression accrue sur les entreprises et les organisations par le biais de travaux sur commande. Les dommages collatéraux qu'entraînent les stratégies de «hack back» suscitent également une attention accrue.

- Inchangé

# Conclusion

Une cyberrésilience forte suppose impérativement une mise en œuvre interdisciplinaire et interdivisionnelle. Le modèle suivant en cinq étapes peut être utile:

1. **Identify**
   L'identification inclut l'analyse des données existantes, leur importance en termes de protection ainsi que leur sauvegarde et leur traitement. La connaissance des risques et des menaces potentiels ainsi que la garantie de la protection dans la chaîne de livraison sont également des aspects importants.

2. **Protect**
   Les collaboratrices et collaborateurs de tous les niveaux hiérarchiques doivent être formés et sensibilisés au thème de la cybersécurité. Les programmes Bug Bounty et les attaques d'équipes rouges (Red Teaming) contribuent également à renforcer la résilience. L'intégration de nouvelles philosophies de sécurité, telle que le Zero Trust, est par ailleurs conseillée.

3. **Detect**
   La surveillance continue de sa propre infrastructure et du réseau interne est essentielle. Une automatisation renforcée du Security Operations Center est également pertinente.

4. **Respond**
   Il est indispensable de pouvoir réagir rapidement aux incidents de sécurité. Les «Near Misses» doivent également être identifiés et documentés afin d'en tirer les enseignements. Une gestion de crise opérationnelle doit en outre être élaborée et mise en œuvre.

5. **Recover**
   En cas de crise, une stratégie de communication bien préparée aide à maintenir la confiance. Des plans de continuité du service et des activités sont recommandés pour garantir un fonctionnement sans faille.

La sécurité physique ne doit pas être négligée, même si elle est souvent secondaire dans la cybersécurité. Les attaques physiques peuvent compromettre la capacité de résistance (résilience) des entreprises aux cybermenaces.

Des influences météorologiques extrêmes telles que la sécheresse, la chaleur, les inondations ou les périodes de froid peuvent par exemple causer des dommages à l'infrastructure, lesquels peuvent avoir un impact sur la stabilité des cyberservices, tant au niveau national qu'international. À l'inverse, les cyberincidents peuvent avoir de graves répercussions sur les secteurs physiques. Aussi est-il important de considérer à la fois la sécurité physique et la cybersécurité et de prendre des mesures appropriées afin de garantir la résilience des entreprises.




## Impressum

| | |
|---|---|
| **Éditeur** | Swisscom (Suisse) SA, Group Security |
| **Conception/réalisation** | Agence Nordjungs, Zurich |
| **Rédaction** | Swisscom (Suisse) SA<br>Marcus Beyer (Group Security)<br>Manuel Bühlmann (Group Communications)<br>Claudia Lehmann (B2B Communications) |
| **Traduction** | Apostroph Bern AG |
| **Copyright** | © Avril 2024 by Swisscom (Suisse) SA, Group Security,<br>Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch |
| **Édition** | OK DIGITALDRUCK AG, Zurich |
| **Tirage** | 200 exemplaires |

**En tant qu'«Innovator of Trust», Swisscom permet et façonne l'avenir numérique. Ses produits et services innovants associés à la confiance de sa clientèle créent une expérience unique pour cette dernière et ont un impact durable sur l'environnement et la société. En Suisse et dans le monde entier.**

Vous trouverez de plus amples informations sur nos produits, nos services et notre engagement pour la sécurité en Suisse sous swisscom.ch/securite

Tu recherches un emploi dans le secteur de la sécurité chez Swisscom? Alors jette un coup d'œil ici et dépose ta candidature: swisscom.ch/securityjobs

# #BeTheStrongestLink