🎓 BTS SIO – Services Informatiques aux Organisations

Option : SISR (Solutions d’Infrastructure, Systèmes et Réseaux)

🧠 Sujet de la veille

Veille Technologique

L'intelligence artificielle dans la cybersécurité

👤 Présenté par

Nom : Amir Tajik

🏫 Établissement

Mediaschool

📅 Année scolaire

2025 – 2026

👨‍🏫 Enseignant référent

Boris Malik

📝 Titre du dossier

Veille Technologique : L’intelligence artificielle dans la cybersécurité

Outils de veille utilisés

Outil	Utilisation
Google Alerts	Surveillance des actualités
RSS	Suivi automatique des publications
LinkedIn	Veille professionnelle
ANSSI	Informations officielles
CERT-FR	Alertes de sécurité
LeMagIT	Actualités IT

Sommaire

Veille technologique

Sujet : L'intelligence artificielle dans la cybersécurité

1. Introduction

Aujourd'hui, l'intelligence artificielle occupe une place de plus en plus importante dans le domaine informatique. Elle est utilisée dans de nombreux secteurs : la santé, l'éducation, les transports, les services en ligne, mais aussi la cybersécurité.

Dans le domaine de la sécurité informatique, l'IA représente à la fois une opportunité et une menace. D'un côté, elle permet aux entreprises de mieux détecter les attaques, d'analyser plus rapidement les incidents et d'automatiser certaines tâches de protection. De l'autre côté, elle peut aussi être utilisée par des cybercriminels pour rendre leurs attaques plus efficaces, plus rapides et plus difficiles à détecter.

Cette veille technologique a pour objectif de comprendre comment l'intelligence artificielle transforme la cybersécurité, quels sont ses avantages, ses risques, et pourquoi ce sujet est important pour les professionnels de l'informatique. Cette veille a été réalisée dans le cadre de ma formation BTS SIO option SISR afin de suivre l'évolution des technologies liées à la cybersécurité.

2. Problématique

Comment l'intelligence artificielle transforme-t-elle la cybersécurité et quels sont les nouveaux risques liés à son utilisation ?

3. Définition du sujet

L'intelligence artificielle désigne un ensemble de technologies capables d'imiter certaines capacités humaines, comme l'analyse, l'apprentissage, la reconnaissance de modèles ou la prise de décision.

En cybersécurité, l'IA peut être utilisée pour :

- détecter des comportements suspects ;
- analyser des fichiers malveillants ;
- identifier des tentatives de phishing ;
- surveiller un réseau informatique ;
- répondre plus rapidement à un incident ;
- aider les analystes SOC dans leur travail quotidien.

Mais l'IA peut également être utilisée par des attaquants pour :

- créer des emails de phishing plus crédibles ;
- générer du code malveillant ;
- automatiser la recherche de vulnérabilités ;
- produire de fausses identités ;
- contourner certains systèmes de détection.

L'ANSSI considère que l'IA est devenue un sujet important pour la cybersécurité et travaille sur la sécurisation des systèmes d'IA, la certification et la sensibilisation des acteurs du numérique.

4. Pourquoi ce sujet est important ?

Ce sujet est important car les attaques informatiques deviennent de plus en plus nombreuses et sophistiquées. Les entreprises, les administrations et les particuliers dépendent fortement des systèmes numériques. Une faille de sécurité peut provoquer des pertes de données, une interruption de service, une perte financière ou une atteinte à la réputation.

L'intelligence artificielle peut aider à renforcer la sécurité, mais elle crée aussi de nouveaux risques. Par exemple, les cybercriminels peuvent utiliser l'IA générative pour rédiger des messages de phishing sans fautes, dans plusieurs langues, avec un style très réaliste.

Selon l'ANSSI, aucun système d'IA générative connu ne permet actuellement de mener de manière totalement autonome toutes les étapes d'une cyberattaque, mais ces technologies peuvent améliorer la quantité, la diversité et l'efficacité des attaques.

5. Les usages positifs de l'IA en cybersécurité

5.1 Détection des menaces

L'IA permet d'analyser de grandes quantités de données en peu de temps. Dans un réseau informatique, il existe beaucoup de journaux d'événements : connexions, tentatives d'accès, flux réseau, alertes antivirus, activités utilisateurs, etc.

Un humain ne peut pas tout analyser manuellement. L'IA peut aider à repérer des comportements inhabituels, par exemple :

- une connexion depuis un pays inhabituel ;
- un utilisateur qui télécharge beaucoup de fichiers soudainement ;
- une machine qui communique avec un serveur suspect ;
- une tentative d'accès répétée à un compte.

5.2 Analyse des malwares

L'IA peut aussi être utilisée pour analyser des fichiers suspects. Elle peut comparer le comportement d'un fichier avec des milliers d'exemples connus de logiciels malveillants.

Cela permet de détecter certains malwares même s'ils sont nouveaux ou modifiés.

5.3 Aide aux analystes SOC

Dans un centre opérationnel de sécurité, appelé SOC, les analystes doivent surveiller les alertes de sécurité. Ils peuvent recevoir beaucoup d'alertes chaque jour.

L'IA peut aider à :

- classer les alertes par niveau de gravité ;
- supprimer les faux positifs ;
- proposer des actions de correction ;
- résumer un incident ;
- accélérer la réponse à une attaque.

5.4 Automatisation de la réponse aux incidents

L'IA peut également être intégrée dans des outils de type SOAR. Ces outils permettent d'automatiser certaines réponses, par exemple :

- bloquer une adresse IP ;
- désactiver un compte compromis ;
- isoler une machine infectée ;
- envoyer une alerte à l'administrateur ;
- créer un ticket d'incident.

Cela permet de gagner du temps, surtout lors d'attaques rapides.

6. Les risques liés à l'IA

6.1 Phishing plus réaliste

Avant, certains emails de phishing étaient faciles à repérer à cause des fautes d'orthographe ou d'un style peu naturel. Avec l'IA générative, les attaquants peuvent créer des messages plus crédibles.

Ils peuvent aussi adapter le message à la victime : langue, poste, entreprise, contexte professionnel.

Cela rend la sensibilisation des utilisateurs encore plus importante.

6.2 Automatisation des attaques

L'IA peut aider les attaquants à automatiser certaines étapes :

- recherche d'informations sur une cible ;
- génération de scripts ;
- analyse de vulnérabilités ;
- création de messages frauduleux ;

- adaptation d'une attaque selon la réaction de la victime.

L'ENISA indique que l'intelligence artificielle est devenue un élément important du paysage de la menace, notamment dans les campagnes de phishing et d'ingénierie sociale.

6.3 Fuite de données dans les outils IA

Un autre risque concerne l'utilisation non contrôlée des outils d'IA par les salariés. Par exemple, un employé peut copier un document confidentiel, du code source ou des données clients dans un outil d'IA public.

Ce phénomène est parfois appelé Shadow AI. Il correspond à l'utilisation d'outils d'intelligence artificielle sans autorisation ou sans contrôle de l'entreprise.

Selon un rapport cité par Reuters, le Shadow AI est devenu une cause importante de perte de données non malveillante, notamment lorsque des informations sensibles sont envoyées dans des outils d'IA.

6.4 Dépendance excessive à l'IA

L'IA ne doit pas remplacer totalement l'humain. Elle peut se tromper, produire de fausses informations ou mal interpréter une situation.

En cybersécurité, une mauvaise décision peut avoir des conséquences graves. Il est donc nécessaire de garder un contrôle humain, surtout pour les décisions importantes.

7. Actualités récentes

Actualité 1 : L'ANSSI et l'IA

L'ANSSI travaille sur plusieurs axes liés à l'intelligence artificielle : accompagnement des administrations, sécurisation des systèmes d'IA, certification, sensibilisation et participation aux travaux européens et internationaux. L'agence insiste sur la nécessité de prendre en compte la cybersécurité dès la conception des systèmes d'IA.

Actualité 2 : L'IA générative face aux attaques informatiques

En 2026, le CERT-FR a publié une synthèse sur l'IA générative face aux attaques informatiques. Le document explique que l'IA ne mène pas encore seule une cyberattaque complète, mais qu'elle peut renforcer les capacités des attaquants.

Actualité 3 : Panorama de la cybermenace 2025

Le CERT-FR et l'ANSSI indiquent dans leur panorama de la cybermenace 2025 que l'IA générative peut accélérer les capacités offensives liées aux cybermenaces. Cela nécessite une réévaluation régulière des risques.

Actualité 4 : NIST et cybersécurité à l'ère de l'IA

Le NIST a publié des recommandations pour aider les organisations à intégrer l'IA dans leurs activités tout en réduisant les risques de cybersécurité. Ces recommandations abordent la protection des systèmes d'IA, l'utilisation de l'IA pour défendre les systèmes informatiques et la prévention des menaces utilisant l'IA.

8. Outils utilisés pour la veille

Pour réaliser cette veille technologique, plusieurs outils peuvent être utilisés :

8.1 Google Alerts

Google Alerts permet de recevoir automatiquement des articles récents sur un sujet précis. Par exemple :

- "intelligence artificielle cybersécurité"
- "IA générative phishing"
- "cyberattaque intelligence artificielle"
- "ANSSI IA cybersécurité"

8.2 Sites officiels

Les sites officiels sont importants car ils donnent des informations fiables :

- ANSSI ;
- CERT-FR ;
- ENISA ;
- NIST.

8.3 Flux RSS

Les flux RSS permettent de suivre les nouvelles publications de sites spécialisés sans devoir les consulter un par un.

8.4 LinkedIn

LinkedIn permet de suivre des experts en cybersécurité, des entreprises, des chercheurs et des institutions.

8.5 Sites spécialisés

Des sites comme LeMagIT, ZDNet, BleepingComputer ou The Hacker News permettent de suivre l'actualité technique.

9. Analyse personnelle

L'intelligence artificielle est devenue un outil stratégique dans la cybersécurité. Elle permet de mieux détecter les attaques et d'aider les professionnels à travailler plus rapidement. Cependant, elle ne supprime pas les risques. Au contraire, elle crée une nouvelle forme de compétition entre défenseurs et attaquants.

Les entreprises doivent donc apprendre à utiliser l'IA de manière responsable. Il ne suffit pas d'installer un outil basé sur l'IA. Il faut aussi mettre en place des règles internes, former les utilisateurs, protéger les données sensibles et vérifier les résultats produits par l'IA.

Pour un étudiant en BTS SIO option SISR, ce sujet est particulièrement intéressant car il touche plusieurs domaines du programme :

- cybersécurité ;
- administration système ;
- réseau ;
- gestion des incidents ;
- protection des données ;
- sensibilisation des utilisateurs ;
- veille technologique.

10. Bonnes pratiques à mettre en place

Pour utiliser l'IA de manière sécurisée, une organisation peut appliquer plusieurs bonnes pratiques :

- définir une politique d'utilisation des outils d'IA ;
- interdire l'envoi de données sensibles dans des outils non validés ;
- former les employés aux risques liés à l'IA ;
- utiliser des solutions professionnelles et sécurisées ;
- surveiller les usages non autorisés ;
- mettre à jour les systèmes régulièrement ;
- vérifier les résultats produits par l'IA ;
- garder une validation humaine pour les décisions critiques ;
- intégrer la cybersécurité dès la conception des projets IA.

11. Conclusion

L'intelligence artificielle transforme profondément la cybersécurité. Elle représente une opportunité importante pour les entreprises, car elle permet de détecter plus rapidement les menaces, d'automatiser certaines tâches et d'aider les analystes à traiter les incidents.

Cependant, elle représente aussi un risque, car les cybercriminels peuvent l'utiliser pour améliorer leurs attaques. Le phishing, l'automatisation des attaques, la génération de code malveillant et les fuites de données liées aux outils d'IA sont des menaces importantes.

La cybersécurité de demain devra donc intégrer l'intelligence artificielle, mais avec prudence. L'humain restera essentiel pour analyser, décider et contrôler les actions réalisées par les outils automatisés.

Conclusion personnelle :

Cette veille technologique m'a permis d'approfondir mes connaissances sur l'utilisation de l'intelligence artificielle dans le domaine de la cybersécurité. En tant qu'étudiant en BTS SIO option SISR, ce sujet est particulièrement intéressant car il montre l'évolution des outils de protection des systèmes d'information ainsi que les nouvelles menaces auxquelles les entreprises doivent faire face. Cette veille m'a également permis de développer ma capacité à rechercher, analyser et synthétiser des informations techniques provenant de sources fiables.

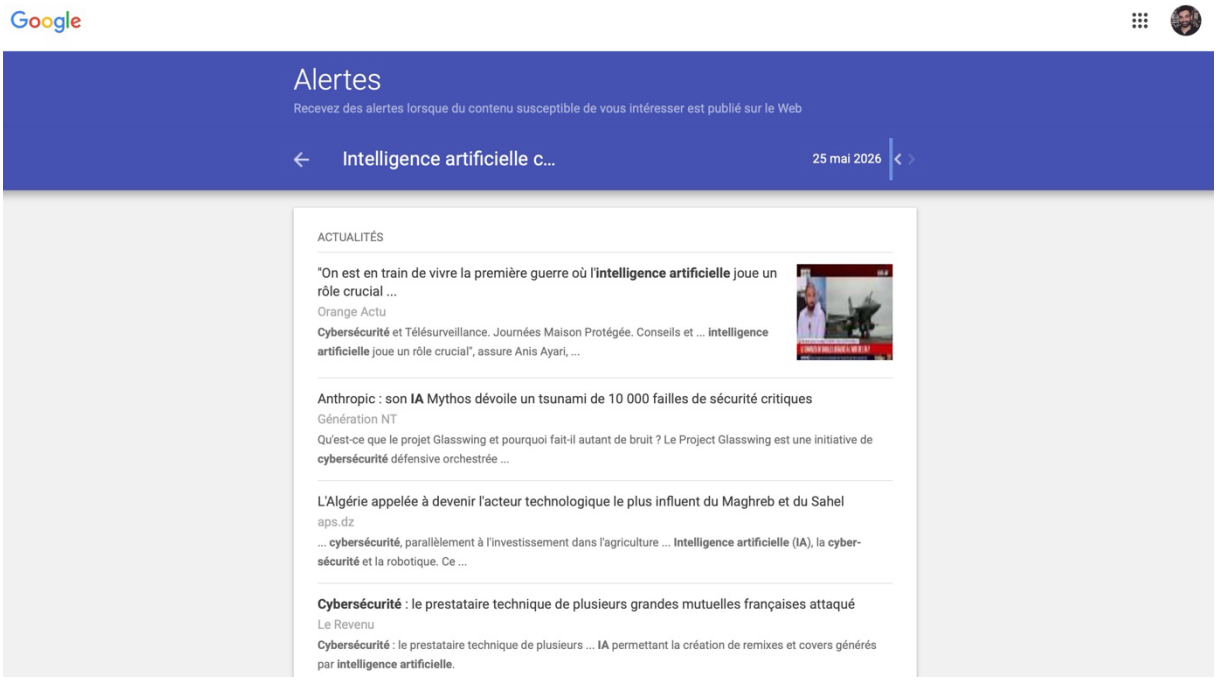

Figure 1 : Exemple d'alerte Google Alerts utilisée dans le cadre de la veille technologique.

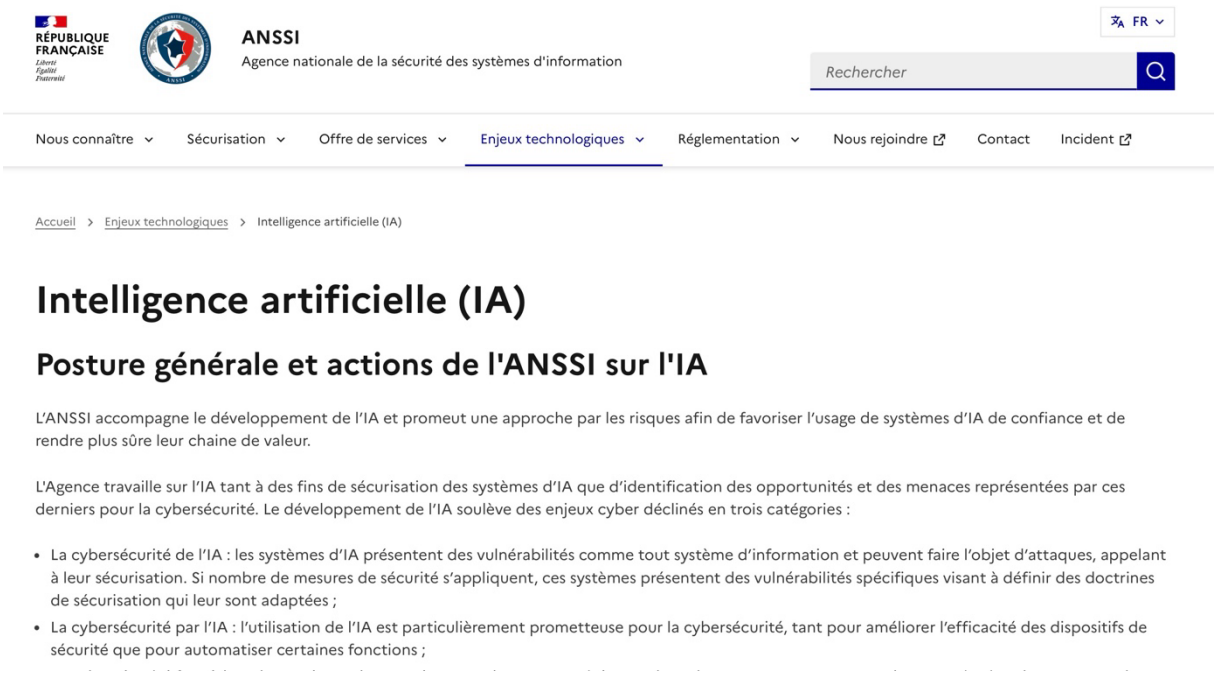

Figure 2 : Ressources officielles de l'ANSSI concernant l'intelligence artificielle et la cybersécurité.

Figure 3 : Rapport du CERT-FR sur l'impact de l'IA générative dans les cyberattaques.

12. Sources

- ANSSI – https://cyber.gouv.fr
- CERT-FR – https://www.cert.ssi.gouv.fr
- ENISA – https://www.enisa.europa.eu
- NIST – https://www.nist.gov
- LeMagIT – https://www.lemagit.fr