IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Scénarios Prospectifs

KRACH SYSTÉMIQUE

Nous sommes en 2030

IN CYBER FORUM EUROPE

POINT DE DÉPART

ACCEPTATION SOCIALE

L'intégration de l'intelligence artificielle (IA) au sein de la société est devenue une norme, régie par une réglementation européenne rigoureuse.

SÉCURITÉ CYBERNÉTIQUE

La cybersécurité est contrôlée par quelques grandes entreprises non européennes, et dans ce secteur, il est fréquent qu'un même fournisseur soit privilégié. Malheureusement, les méthodes d'attaque contre le système financier se sont développées aussi rapidement que les applications de l'IA. Les logiciels malveillants tels que FraudGPT et WormGPT sont facilement accessibles sur le dark web et constituent une menace significative.

PROGRÈS TECHNOLOGIQUE

La loi de Moore reste pertinente, engendrant des capacités de calcul de plus en plus puissantes dans des volumes de plus en plus réduits.

UTILISATION DE L'IA DANS LE SECTEUR FINANCIER

L'IA est mise à profit dans de nombreux domaines, notamment par les institutions financières qui ont réussi à réduire de manière significative leurs coûts et à augmenter leurs bénéfices grâce à son utilisation. Les marchés boursiers et de commodités sont désormais dominés par des institutions qui utilisent l'IA pour gérer leurs transactions. Ces systèmes automatisés recherchent en continu (24h/24, 7j/7) des informations actualisées, qu'elles soient de signaux positifs ou négatifs concernant les activités économiques d'une entreprise, d'un secteur ou d'un pays, afin d'évaluer l'impact potentiel sur la demande d'une marchandise et de déclencher, de manière autonome, des opérations d'achat ou de vente avant que les autres acteurs du marché puissent réagir.

KRACH SYSTÉMIQUE

What if...

CYBERATTAQUE

ANTÉCÉDENTS

Depuis l'année 2023, nous nous sommes accoutumés à des attaques de plus en plus sophistiquées employant l'intelligence artificielle pour analyser les profils des individus ciblés sur les réseaux sociaux et pour orchestrer des attaques d'ingénierie sociale à grande échelle, dans le but de subtiliser des fonds.

SITUATION ACTUELLE EN 2030

Plusieurs institutions financières ont été alertées d'un problème affectant leur plateforme de trading automatisée par l'IA.
Il est rapporté que le système d'IA aurait subi des modifications non autorisées (par l'intermédiaire d'une backdoor) entraînant le déclenchement d'une cascade de transactions de vente.
Les infrastructures dépendant des IA ultrarapides et des connexions à très haut débit sont particulièrement vulnérables : si un système d'IA défaille, il est probable que les systèmes connexes réagissent en chaîne. La menace d'induire un krach sur les marchés financiers plane, à moins qu'une rançon ne soit versée dans un délai très court.

CONCERNANT L'AGRESSEUR

Le véritable problème réside dans l'incertitude entourant la prétendue modification de l'IA : jusqu'à présent, aucun comportement anormal n'a été détecté. Peut-on envisager que cette allégation soit un bluff ?

KRACH SYSTÉMIQUE

En conséquence....

SCÉNARIO DE BIFURCATION POSITIVE :

REDONDANCE DE L'IA

Chaque institution dispose de deux systèmes d'IA fonctionnant en parallèle : un système primaire et un système secondaire, chacun opérant de manière autonome. En cas de divergence significative entre les deux systèmes ou de dépassement des seuils d'alerte comportementale, une intervention humaine devient impérative.

MÉCANISME D'ARRÊT D'URGENCE

Un dispositif d'arrêt d'urgence est en place, permettant de suspendre l'ensemble du système de trading en cas de nécessité.

ANALYSE FORENSIQUE

Les systèmes d'IA sont élaborés de façon à permettre des analyses forensiques post-incident.

COORDINATION DES INTERVENANTS

Les équipes de cybersécurité des entités financières, situées au sein d'un centre opérationnel dédié, collaborent étroitement avec les éminents experts en cybersécurité du domaine local, ce qui facilite la communication rapide des dernières informations pertinentes et la diffusion immédiate des alertes aux autres institutions.

IN CYBER FORUM EUROPE

SCÉNARIO DE BIFURCATION NÉGATIVE :

FLASH CRASH

Les systèmes d'IA, devenant hors de contrôle, provoquent un effondrement instantané des marchés financiers — un « flash crash » — avant qu'une intervention humaine puisse avoir lieu.

RÉPERCUSSIONS MÉDIATIQUES

La crise est massivement relayée par les médias, établissant des comparaisons avec la crise financière de 2008.

EFFET DOMINO

Dans le pire des cas, la situation engendre une crise de confiance généralisée entraînant des retraits massifs de capitaux par le public, menaçant de précipiter l'effondrement du système financier.

RECHERCHE DE BOUCS ÉMISSAIRES

Suite à l'effondrement financier, l'ensemble des applications d'IA se voient discréditées.

DÉMOCRATIES EN DANGER

Nous sommes en 2030

IN CYBER FORUM EUROPE

POINT DE DÉPART

ACCEPTATION SOCIALE

L'intégration de l'intelligence artificielle (IA) dans la société s'effectue de façon continue, encadrée par une réglementation européenne distincte des réglementations américaine et chinoise. Cependant, cette intégration soulève des préoccupations relatives à la perte d'emplois et à l'impact énergétique associé.

INNOVATION TECHNOLOGIQUE

L'automatisation gagne du terrain de manière significative avec l'avancement rapide de l'Internet des objets ; un nombre croissant d'objets sont désormais dotés de microprocesseurs qui collectent des données précieuses.

APPLICATIONS DE L'IA

Étant donné l'abondance et la diversité des données disponibles, l'IA est de plus en plus utilisée pour détecter des modèles au sein de ces données. Par exemple, des analyses par IA permettent de modéliser les zones de consommation de stupéfiants en analysant la qualité de l'eau des égouts. L'utilisation de données historiques contribue à identifier les intersections les plus dangereuses ou les rues les plus susceptibles de subir un cambriolage.
De plus, les médias traditionnels se voient de plus en plus contraints de s'appuyer sur l'IA pour la production de contenu, face à une diminution constante de leurs revenus.

CYBERSÉCURITÉ

En Europe, les algorithmes et les jeux de données d'entraînement des IA doivent faire l'objet d'un audit par une entité indépendante et se conformer à la législation sur le droit d'auteur, ainsi qu'à d'autres critères tels que la prévention de la discrimination.

DÉMOCRATIES EN DANGER

What if...

CYBERATTAQUE

ANTÉCÉDENTS

Depuis l'année 2023, des extrémistes issus de divers milieux exploitent l'intelligence artificielle pour déstabiliser le paysage politique. Certains pratiquent la désinformation traditionnelle, créant des vidéos et des articles de type « deepfake » qui sapent la crédibilité des personnalités politiques opposées, avec une sophistication telle que l'authenticité parait indubitable. D'autres groupes utilisent l'IA pour

SITUATION ACTUELLE EN 2030

Il est à présent possible de synthétiser les résultats de diverses IA et les données issues de l'Internet des Objets (IoT) afin de déduire les inclinations politiques de quasiment tous les citoyens. De surcroît, l'IA facilite une personnalisation de masse des messages envoyés pour maximiser l'indignation. Avec le déclin progressif du journalisme professionnel, il devient de plus en plus ardu de dénicher des entités indépendantes capables de procéder à une vérification rigoureuse des faits.

CONCERNANT L'AGRESSEUR

L'existence des extrémistes politiques perdure, et l'on suspecte qu'ils bénéficient de l'appui de certains États autoritaires cherchant à ébranler les démocraties.

DÉMOCRATIES EN DANGER

En conséquence....

SCÉNARIO DE BIFURCATION POSITIVE :

INTELLIGENCE COLLECTIVE

Nous bénéficions des progrès en matière de guerre cognitive, mettons en œuvre des initiatives publiques et privées pour combattre la désinformation, et renforçons l'éducation sur cette problématique tant dans les établissements scolaires qu'auprès du public général.

SOUTIENS TECHNO-JURIDIQUES

L'adoption d'une identité numérique européenne, garantissant la propriété des données personnelles aux individus plutôt qu'aux entreprises, réduit la possibilité de profiler des comportements individuels. De surcroît, les systèmes de watermarking numérique se montrent performants pour repérer et supprimer les contenus falsifiés, tels que les « deepfakes », en collaboration avec les fournisseurs de services Internet qui endossent une responsabilité concernant les contenus en ligne.

DIFFÉRENTS NIVEAUX DE GOUVERNANCE

Pour les États européens vulnérables aux campagnes de désinformation, l'Union Européenne joue également un rôle de régulateur et de protecteur.

IN CYBER FORUM EUROPE

SCÉNARIO DE BIFURCATION NÉGATIVE :

ÉROSION DE LA CONFIANCE

Dans un climat de polarisation politique et géopolitique exacerbée, l'accord sur la perception de la réalité est compromis. Les faits indéniables sont remis en question et les rumeurs infondées sont prises pour argent comptant. La lutte contre le scepticisme croissant des citoyens envers le système (politique, médias, institutions, etc.) et le maintien de la confiance constituent un défi majeur.

LES EXTRÊMES AU POUVOIR

Dans une période de troubles accrus, les tensions numériques se matérialisent, provoquant des manifestations, des blocages urbains et des émeutes potentielles. Des mouvements politiques adhérant à une vision « démocratie illibérale » accèdent au pouvoir et utilisent l'IA pour « combattre la criminalité », ce qui se traduit par une surveillance accrue et une répression des dissidents.

L'IA INFLUENCÉ ET INFLUENCEUR

L'IA est désormais contrainte de s'aligner sur les perspectives gouvernementales, influençant ainsi les nouvelles et les recommandations qu'elle génère.

BROUILLARD DE LA GUERRE 2.0

Nous sommes en 2030

IN CYBER FORUM EUROPE

POINT DE DÉPART

ACCEPTATION SOCIALE

La mise en œuvre de l'intelligence artificielle dans la société suscite des réserves, essentiellement dues aux inquiétudes relatives à la suppression d'emplois et à l'augmentation de la surveillance par les systèmes d'IA. Toutefois, le rôle crucial de l'IA dans le domaine militaire est incontestable, en particulier l'utilisation des drones – qu'ils opèrent sur terre, dans les airs ou en mer – dont la présence en grand nombre est jugée indispensable.

INNOVATION TECHNOLOGIQUE

La poursuite de l'évolution prédite par la loi de Moore assure une augmentation constante de la puissance des microprocesseurs intégrés aux drones.

APPLICATION DE L'IA

L'autonomie progressive des drones est devenue essentielle pour pallier les interférences et répondre avec célérité aux offensives. De plus, ces drones sont à présent capables de mener de manière autonome l'ensemble du cycle OODA (observer, orienter, décider, agir). Le temps de réaction humain, malgré sa valeur, peut constituer un désavantage majeur pour ces dispositifs.

LA PROTECTION CYBER

L'époque où les projets militaires nécessitaient un nombre restreint d'engins performants, composés de pièces produites et régulées localement, est révolue. Il est désormais impératif de disposer d'un grand nombre de drones, souvent issus du commerce standard et économiques. Cela entraîne que de nombreuses composantes, en particulier les microprocesseurs, sont conçues et manufacturées à l'étranger. Toute tentative de s'écarter de cette tendance se confronte aux problèmes de coûts (prohibitifs) et de conception (obsolète comparée au secteur commercial). La sécurité cybernétique est généralement intégrée post-acquisition du drone, lors de sa conversion et de son équipement pour le service militaire.

BROUILLARD DE LA GUERRE 2.0

What if...

IN CYBER FORUM EUROPE

CYBERATTAQUE

ANTÉCÉDENTS

Depuis l'année 2023, il est devenu progressivement évident que les pays démocratiques font face à une problématique majeure. Leurs citoyens exigent que les lois de la guerre soient respectées et persistent à réclamer que la décision d'engager une attaque soit prise par un être humain. Cependant, il est de plus en plus manifeste que les ennemis potentiels ne rencontrent aucun scrupule à déployer des drones tueurs autonomes, et possèdent désormais la capacité technologique de le faire.

SITUATION ACTUELLE EN 2030

Des informations transmises par nos drones indiquent l'approche massive de centaines de drones ennemis aux abords de la frontière. Le centre de commandement a été informé. En cas d'assaut inopiné, le temps est compté, et il ne reste que quelques instants pour éviter la destruction de nos drones ou des unités frontalières. Une décision doit être prise sur-le-champ : soit laisser l'attaque se dérouler sans intervention, soit initier une offensive préventive.

CONCERNANT L'AGRESSEUR

L'escalade géopolitique atteint un niveau critique.
L'hypothèse d'une attaque imminente est prise au sérieux.
Toutefois, que se déroulerait-il si cette menace était fictive ?
Une simulation d'attaque par IA destinée à simuler un essaim de drones où il n'y en a que peu ? Et si l'objectif était de nous inciter à une riposte, offrant à l'adversaire l'occasion de se présenter comme le défenseur légitime de ses droits ?
Ou, situation encore plus préoccupante, s'il s'agissait simplement d'une défaillance logicielle ?

BROUILLARD DE LA GUERRE 2.0

En conséquence....

SCÉNARIO DE BIFURCATION POSITIVE :

DIPLOMATIE

La diplomatie réussit à établir une confiance mutuelle permettant d'établir des règles préventives contre une réaction immédiate et automatique, telles qu'une « ligne rouge IA », offrant ainsi le temps nécessaire pour désamorcer les tensions.

DISSUASION

Notre capacité de dissuasion est suffisamment solide pour dissuader toute tentative hostile. Grâce à un arsenal de drones variés et à des systèmes de cyberdéfense indépendants, la probabilité d'une infection généralisée est fortement réduite.

VEILLE

Une surveillance continue est exercée, également via des IA spécialisées dans la supervision et le contrôle de nos propres drones. De plus, nous disposons d'un personnel qualifié en nombre suffisant, capable de comprendre et d'interpréter les activités de nos drones.

IN CYBER FORUM EUROPE

SCÉNARIO DE BIFURCATION NÉGATIVE :

ESCALADE

En l'absence de normes internationales sur l'utilisation de l'IA et des systèmes militaires autonomes, la communication avec des adversaires potentiels s'avère difficile. La décision d'engager une attaque doit être prise sans délai.

SPIRALE DE GUERRE

Une fois que nous avons initié l'offensive, il est certain que l'adversaire répondra. Ses drones étant programmés pour réagir sans intervention humaine, la riposte est inévitable.

BLACKOUT EN SÉRIE

Nous sommes en 2030

IN CYBER FORUM EUROPE

POINT DE DÉPART

ACCEPTATION SOCIALE

La consommation énergétique élevée des systèmes d'intelligence artificielle a suscité des critiques de la part du public, entraînant le développement d'une nouvelle génération d'IA économes en énergie. Ces systèmes, souvent décentralisés, se caractérisent par des fonctions spécifiques et une formation basée sur un nombre restreint de paramètres.

APPLICATION DE L'IA

L'intelligence artificielle est devenue essentielle pour l'équilibrage du réseau électrique, qui intègre une part croissante de production d'énergie renouvelable. Face à l'intermittence de nombreuses sources d'énergie, l'IA se révèle particulièrement efficace pour ajuster les fluctuations de production, parfois en quelques secondes. D'autres formes d'IA sont employées pour la maintenance prédictive, permettant de réparer des équipements avant leur défaillance.

INNOVATION TECHNOLOGIQUE

L'expansion rapide de l'Internet des Objets se manifeste notamment par la généralisation des compteurs intelligents et du réseau électrique intelligent. Parallèlement, la transition accélérée vers la décarbonation conduit à une électrification croissante des objets, y compris dans les domaines de la mobilité et du chauffage.

LA PROTECTION CYBER

Le marché des fournisseurs de cybersécurité est dominé par un petit nombre de très grandes entreprises, toutes situées en dehors de l'Europe. De plus, il convient de souligner que la majorité des panneaux solaires, principalement fabriqués en Chine, sont équipés de systèmes de collecte et de transmission de données. Ainsi, en période de fort ensoleillement, la Chine est en mesure de collecter d'importantes quantités de données sur les réseaux énergétiques européens.

BLACKOUT EN SÉRIE

What if...

CYBERATTAQUE

ANTÉCÉDENTS

Depuis 2023, les cyberattaques ne constituaient pas la principale préoccupation ; le véritable enjeu résidait plutôt dans la discordance entre l'offre et la demande d'énergie. Durant les périodes estivales, les pénuries d'eau pour le refroidissement des centrales et les pics de consommation liés aux systèmes de climatisation, de plus en plus sollicités avec l'avancée du changement climatique, ont incité à l'utilisation de l'IA pour optimiser la gestion du réseau électrique.

SITUATION ACTUELLE EN 2030

L'adversaire s'attaque au fondement de notre infrastructure : le réseau électrique. L'exploitation d'une faille dans un logiciel crucial pour la gestion du réseau permettrait de déclencher des interruptions de service aléatoires et continues. Les conséquences seraient systémiques : en l'absence d'électricité, la majorité des infrastructures vitales s'immobiliseraient, particulièrement après l'épuisement des réserves des générateurs de secours — plus d'accès aux services bancaires, aux pompes à essence, ni à l'approvisionnement en eau.

CONCERNANT L'AGRESSEUR

Il est plausible que l'acte soit l'œuvre d'un État hostile cherchant à exprimer son hostilité envers l'Union Européenne. Néanmoins, il est également possible que la faille ait été initialement introduite par une agence étrangère d'un autre pays et découverte par la suite par cet État hostile. La situation demeure incertaine.

BLACKOUT EN SÉRIE

En conséquence....

SCÉNARIO DE BIFURCATION POSITIVE :

IA EN COPILOTE

Les opérateurs chargés de surveiller nos réseaux électriques sont assistés par des IA copilotes, indépendantes du système potentiellement compromis, dont la fonction est également de détecter des anomalies dans la gestion du réseau.

EXPERTISE INCARNÉE

Des protocoles manuels de contrôle existent parallèlement, prêts à être activés si l'IA doit être déconnectée d'urgence. De plus, le personnel est spécifiquement formé pour reprendre la main en cas de nécessité.

DOCTRINE

Face à la menace ciblant les infrastructures essentielles et pouvant mettre des vies en péril, la doctrine autorise le recours au hack-back, une contre-attaque informatique visant à neutraliser la menace à sa source.

IN CYBER FORUM EUROPE

SCÉNARIO DE BIFURCATION NÉGATIVE :

CHAOS QUOTIDIEN

Les attaques sont ponctuelles et précises – un jour ciblant les feux de circulation d'une ville, le lendemain l'ensemble des hôpitaux du pays, puis les transports publics. L'incertitude règne quant à la prochaine cible.

FAUX POSITIFS

Faute d'outils adéquats pour l'identification précise des anomalies, nous sommes parfois confrontés à des alertes infondées, gaspillant ainsi nos ressources limitées

REMISE EN QUESTION DE L'IA

Des coupures de courant prolongées, induites par des dysfonctionnements de l'IA, pourraient engendrer un scepticisme généralisé sur la fiabilité de l'IA dans toutes ses applications, surtout si l'origine cybernétique des pannes ne peut être clairement établie.

BODY HACKING

Nous sommes en 2030

IN CYBER FORUM EUROPE

POINT DE DÉPART

ACCEPTATION SOCIALE

L'adoption de l'intelligence artificielle dans la vie de tous les jours est devenue une réalité, notamment dans le domaine médical où elle constitue désormais un support essentiel, renforcée par la mise en place de réglementations européennes rigoureuses concernant l'utilisation des données personnelles.

INNOVATION TECHNOLOGIQUE

L'innovation réside principalement dans l'interaction entre les humains et la technologie. Celle-ci n'est plus un outil utilisé occasionnellement, comme un ordinateur ou un smartphone, mais un compagnon en interaction constante avec nous, tel un ami anthropomorphe doté d'une voix agréable, une montre aux multiples fonctionnalités ou encore des microprocesseurs implantés dans le corps humain. L'edge computing et l'edge IA permettent à de petits systèmes de réaliser des tâches complexes indépendamment d'un ordinateur central.

APPLICATION DE L'IA

L'agrégation de données personnelles hétérogènes, souvent recueillies par des dispositifs portatifs, permet à l'IA de diagnostiquer des maladies en amont et d'affiner la téléconsultation. De plus, les chatbots anthropomorphes, qui se sont intégrés dans nos maisons, lieux de travail et espaces publics, sont fortement appréciés. Inclus dans le réseau de soins, ils servent, entre autres, à rappeler la prise de médicaments. Pour bon nombre d'individus, particulièrement les personnes âgées ou isolées, ces chatbots sont perçus comme de véritables compagnons.

LA PROTECTION CYBER

La cybersécurité doit être assurée dans chaque petit système autonome. C'est pourquoi il est fréquent de recourir à des IA recommandées par d'autres IA pour garantir cette protection.

BODY HACKING

What if...

IN CYBER FORUM EUROPE

CYBERATTAQUE

ANTÉCÉDENTS

Depuis 2023 il y a eu des tentatives répétées de voler les données privées de patients, en passant par des chatbots compromis par des hackers. Mais les données ainsi obtenues étaient sécurisées par une IA de cybersécurité. Les criminels espèrent qu'un jour ils vont pouvoir décryptées les données par le biais du calcul quantique, mais cela tarde à venir.

SITUATION ACTUELLE EN 2030

Une entreprise pionnière dans les systèmes de santé s'apprête à lancer une OPA. L'entreprise spécialise dans des systèmes d'IA qui interagissent avec les humains de par des chatbots, et même physiquement, étant installés dans des régulateurs cardiaques et des chips implantés dans de plus en plus de personnes (à l'origine uniquement pour des personnes ne pouvons plus communiquer avec le monde externe, désormais il est devenu « cool » de pouvoir gérer son ordinateur ainsi). Mais un médecin inquièt contacte l'entreprise. Son chatbot vient de lui proposer de prendre une dose excessive de médecine. Le chatbot, était-il empoisonné ?

CONCERNANT L'AGRESSEUR

Dans l'absence de la demande d'une rançon, on se demande si c'est une erreur technique – ou si une entreprise rivale, provenant d'ailleurs dans le monde, n'essaye pas de discrédité l'entreprise avant qu'elle ait accès à des fonds importants avec l'OPA.

BODY HACKING

En conséquence....

SCÉNARIO DE BIFURCATION POSITIVE :

ACA

Une IA décentralisée (« Autonomous Cyber-defense Agent ») détecte aussi le mauvais fonctionnement du système IA, et avertisse l'entreprise et l'utilisateur.

UNE DÉFENSE BIGARRÉE

Ayant la possibilité d'acheter un système de défense de plusieurs différentes entreprises locales et étrangères rendent la tâche de l'agresseur davantage difficile puisqu'il faut s'attaquer à plusieurs systèmes différents.

IN CYBER FORUM EUROPE

SCÉNARIO DE BIFURCATION NÉGATIVE :

En cas de succès de l'attaque il risque d'avoir des morts. Les chatbots donneront de mauvais conseils, et certains pourront mourir de surmédication. D'autres auront des problèmes cardiaques, ou ne pourront plus communiquer par les microprocesseurs implantés.

DES DÉGÂTS ÉCONOMIQUES

La réputation de l'entreprise sera ruinée, et ses espoirs d'une OPA aussi.

LA MÉFIANCE DES CITOYENS

Le système de santé basé sur l'IA sera remis en question par le public.

Les pivots

↘ LES EXPERTISES DISPONIBLES

— Des experts en informatique, codage et utilisation de l'IIA

— Des experts qui savent faire une tâche sans IA si nécessaire

— Une population avec un esprit critique

↘ LA GOUVERNANCE

— Le cadre réglementaire

— La cyberdiplomatie

— Le droit de la concurrence

— Les donneurs de confiance (certification etc.)

— Une identité numérique et protection de la vie privée

↘ L'IA POUR LA CYBERDÉFENSE

IN CYBER FORUM EUROPE

26–28 MARS 2024

LILLE GRAND PALAIS

Remerciements

↘ LES SCÉNARIOS ONT ÉTÉ ÉLABORÉS À PARTIR D'INFORMATIONS PROVENANT DE NOMBREUSES SOURCES, NOTAMMENT :

— Entretiens avec Henri d'Agrain, Jacob Galbreath, Piret Pernik, Siraj Shaikh, Thierry Berthier, Yann Bonnet et Urmas Ruuto

— Un atelier à l'IHEDN