HACKERS OUVERTS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

HACKERS OUVERTS

ISBN: 978-3-9525175-7-4

Office fédéral de l'armement suisse
Sciences et technologies
Gestion de la recherche et de recherche opérationnelle
Feuerwerkerstrasse 39
CH-3602 Thun

Contact:
Prospective Technologique - Dr. Quentin Ladetto
Tel. +41 58 468 28 09
quentin.ladetto@armasuisse.ch

www.sicherheitsforschung.ch
www.deftech.ch

Rédaction: Anne-Caroline Paucot

Équipe créative: Studio Miamiam
Graphisme : Pierre Hugot & Ludivine Koegler

HACKERS OUVERTS

Anne-Caroline Paucot
Quentin Ladetto

Les Propulseurs

De la prospective-action pour dessiner les compétences du futur

Hackers ouverts est une prospective-fiction qui présente une vingtaine de métiers du futur de la cybersécurité. Ces métiers ont été imaginés au cours d'ateliers organisés par armasuisse en mai 2021.

Ce document est le résultat d'une opération de prospective-action sur le thème de la cybersécurité. La prospective-action permet de se catapulter dans des horizons plus ou moins lointains et d'utiliser ces projections pour trouver de nouvelles manières de faire et de penser. Elle ne s'attache pas à prédire le futur, elle en envisage plusieurs afin de s'y préparer.

L'objectif du projet était d'imaginer les métiers de demain de la cybersécurité afin d'identifier les compétences nécessaires pour les exercer. Après avoir envisagé les effets possibles des technologies à moyen et long terme, nous en avons listé des aptitudes nécessaires pour amplifier leurs effets bénéfiques et se protéger de leurs dérives.

Dans une démarche de prospective-fiction, le défi est de travailler ce qui n'existe pas encore. Quand on invite à créer des scénarios prospectifs, le résultat est souvent du « presque existant teinté de l'air du temps ». Pour éviter ce travers, nous avons expérimenté une méthodologie qui repose sur trois principes.

Le ***premier*** est de considérer que les métiers de demain vont résulter de la conjugaison de trois éléments : des technologies et nouveaux usages, des défis à relever, des innovations et recherches.

Le ***deuxième*** est de partir de l'existant pour progressivement se propulser dans le futur.

Le ***troisième*** est d'opter pour l'imagination collective en invitant les participants à des ateliers.

Au cours de quatre ateliers en langue allemande et française, nous avons procédé par étapes.

Étape 1 : Sensibilisation et choix

Après une mise en perspective par des experts, les participants découvrent des cartes présentant des cyberattaques actuelles. Ils en choisissent une et imaginent ses conséquences à court, moyen, long terme.

Étape 2 : combinaisons

Des technologies sont proposées. Les groupes imaginent des cyberattaques plus sophistiquées. On commence à sortir de l'existant.

Étape 3 : décollage

Les participants choisissent un superpouvoir dans une liste. Grâce à cet artifice ludique, ils peuvent changer la consistance des matériaux ou la taille des plantes, commander la pluie et le beau temps, faire voler les humains ou lire dans leurs pensées…

Avec ces enrichissements et ce pas de côté, ils sortent du cadre et imaginent des menaces du futur.

Technologies et nouveaux usages

Informatique quantique, blockchain, biologie synthétique, robotique, intelligence artificielle… Si chaque technologie va créer des métiers, nombreux seront ceux qui résulteront de leurs combinaisons

Défis à relever

Réussir la transition écologique et énergétique, nourrir l'humanité, assurer sa protection… Les défis à relever sont nombreux. Ils vont nécessairement orienter les actions de nombreuses entreprises.

Innovations et recherches

Ce sont les briques de la construction de l'avenir. Elles vont se combiner pour construire différents futurs.

À l'issue des deux premières sessions, l'une tenue en français, l'autre en allemand, nous avons recueilli une douzaine de cyberattaques d'un nouveau genre.

Lors du deuxième atelier, les participants en ont choisi une dans la liste. Ils ont imaginé des solutions tant pour la contrer que pour en limiter les dégâts. Le besoin de nouvelles compétences s'imposant, ils ont envisagé de nouveaux métiers.

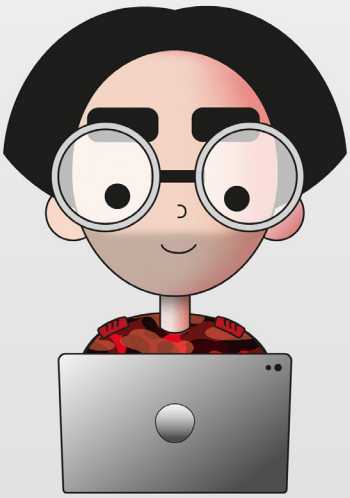
Face à la richesse des échanges, nous avons choisi de restituer le travail sous la forme d'un récit. La mise en scène des idées a permis de continuer la discussion lors d'un troisième atelier.

Quentin Ladetto (armasuisse), Anne-Caroline Paucot, Luc Legay (Propulseurs), Gabriele Rizzo (UNIL-HEC) Philipp Klüfers, Pascal van Overloop, Hoog Björn, Sibylle Lang (IABG)

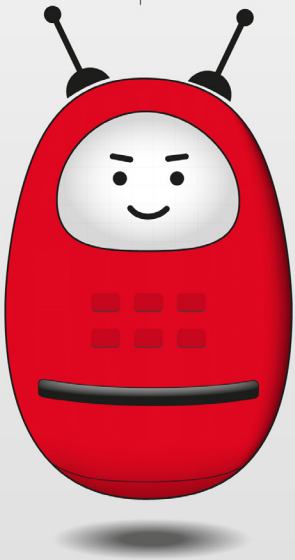
Avec la participation de

Mahmoud Salim Gaddes, Jean-François Baudron, Michael Beck, David Beck, Slawomir Blos, Seta Boroyan, Rudolf Bürgi, Bruno Chanel, Kilian Cuche, Édouard de Moura Presa, Michel Delabays, Marion Desclaux, Romain Fenouil, Yacine Founaqa, Luca Gambazzi, Felix Gräser, Florian Kirmes, Pauline Lansac, Alan Lava, Benoit Loux, Stéphanie Loyer, Soenke Marahrens, Laurent Mathys, Jeanne Meesemaecker, Nicolas Müller, Jean-Paul Pinte, Quentin Piquard-Guerin, Remo Reginold, Marc Renaud, Marc-André Ryter, Alexandre Sarbach, Benjamin Sawicki, Klaus Schmidt, Thierno Sow, Luca Tenzi, Jean-Pierre Therre, Giorgio Tresoldi, Elliot Vaucher, Arnaud Velten, François Videau, Andreas Walker, Robert Welter, Thomas Zweifel

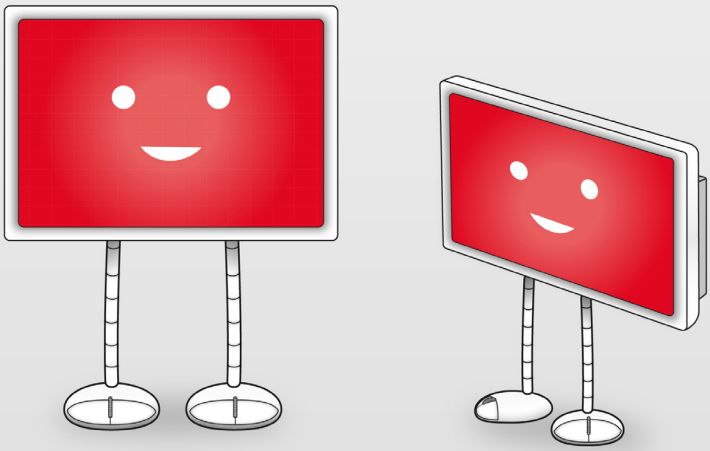
Andrea



Maurice



Kiron



DE LA PROSPECTIVE-ACTION POUR DESSINER LES COMPÉTENCES DU FUTUR

Hackers ouverts est une prospective-fiction qui présente une vingtaine de métiers du futur de la cybersécurité Ces métiers ont été imaginés au cours d'ateliers organisés par armasuisse en mai 2021.

15 - ***Nouvelle guerre***

Vulnérabilité plus importante des pays puissants, impossibilité pour un gouvernement d'agir seul, difficulté à identifier l'agresseur… La cyberguerre remet en question la façon de penser la guerre.

19 Métiers du futur de la stratégie

19 Anticipacteur
Transformateur de concepts futuristes en actions.

19 Cyberguerriste
Identificateur des spécificités de la cyberguerre

19 Résilienceur
Créateur de réseaux numériques résilients.

21 - ***Les canaris de la mine***

Les deux intelligences artificielles font des sauts de puces dans le futur pour envisager les métiers qui vont prévenir et détecter les cyberattaques.

26 Métiers de la détection des alertes

26 Canariste
Ingénieur en systèmes d'alertes préventives.

26 Détackteur
Détecteur des faiblesses des systèmes informatiques.

26 Hackarion
Espion de pirates informatiques.

26 Instraquar
Créateur de dispositifs d'identification des cybercriminels.

27 - ***Demandes de rançons***

Les attaques se précisent. Il faut limiter les dégâts. On jongle entre des solutions et on négocie des rançons.

32 Métiers de sensibilisation à la cybersécurité

32 Cybernudgien
Spécialiste des nudges d'adoption de comportements sécurisés

33 - ***La grande panne***

Les IA font monter la pression : une ligne de code perturbant le système de positionnement satellitaire peut provoquer un cataclysme mondial.

38 Métiers pour limiter l'impact des attaques

38 Coupenaute

Créateur de communautés éphémères pour survivre les pannes

38 Epinumériste
Épidémiologiste numérique

38 Lowteckiste
Spécialiste de solutions non numériques.

39 RangociAÉteur
Négociateur de rançons pour décryptage de données.

41 - *L'homme manipulé*

Implants, tatouages ou dents connectés... Quand l'homme sera relié en permanence au réseau, les pirates manipuleront ses pensées, sa mémoire ou son génome.

45 Métiers du commerce du piratage

45 Pirating

47 - *La pluie et le beau temps*

Si les humains disposaient de super pouvoirs, quels seraient les piratages de demain ? Les IA s'égarent pour anticiper cet imprévisible.

51 Métiers des cyberattaques d'après-demain

51 Blockcloneur
Contrôleur de l'intégrité psychologique des doubles humains.

51 Chirurgiticien
Chirurgien identitaire.

51 Climataine
Officier en cyberguerre climatique.

51 Emprisonnien
Spécialiste de la prise d'otage de cerveaux humains.

52 Oniriste
Analyste spécialiste du tri des souvenirs.

52 Persodatiste
Spécialiste de l'intégrité des données personnelles.

52 Sécurothicien
Garant de l'intégrité des génomes humains

53 - *De l'anticipation à l'action*

Morris et Kiron envisagent les compétences à acquérir pour relever les futurs défis de la cybersécurité.

Nouvelle guerre

Vulnérabilité plus importante des pays puissants, impossibilité pour un gouvernement d'agir seul, difficulté à identifier l'agresseur...

La cyberguerre remet en question la façon de penser la guerre.

Kiron, quels sont les métiers du futur de la cybercriminalité ?

Je suis Kiron, une machine de la marque « Intelligence artificielle ». Je travaille pour Andrea, un humain appartenant à la catégorie « grand homme ». Il mesure 1,982 m et est designer des futurs de l'armée. Je suis son scripte et son cerveau. Lorsqu'il a un problème, j'utilise mon génie machinal pour le résoudre.

Kiron, le problème est costaud. Assauts numériques, données volées, sociétés rançonnées… On dénombre près de 200 000 cyberattaques chaque jour dans le monde. Ces chiffres ne cessant de croître, il faut repenser les métiers.

Bonne machine, je vérifie les chiffres. Je constate que le nombre d'attaques criminelles a explosé en 2020. Les experts tirent la sonnette d'alarme. Comme les programmes informatiques sont passés de dizaines de lignes de code à des dizaines de millions, il est de plus en plus difficile de traquer les intrus.

Métiers du futur de la cybercriminalité ! Ma base de données est vide.

Kiron, tu peux faire un effort, c'est important ! Si on ne connaît pas les métiers du futur, on ne peut pas définir les compétences nécessaires pour les exercer.

Échec de la recherche avancée. Dans la base « métiers qui n'existent pas encore », il y a zéro donnée.

Je ne sais pas. Imagine les métiers.

Je ventile pour manifester mon incapacité. Une intelligence artificielle peut trier des données, faire des extrapolations, mais pas imaginer.

Bon, puisque tu ne veux pas m'aider, je fais appel à Morris.

Je bipe pour marquer ma désapprobation. Andrea adore la permIAculture ou le métissage des intelligences artificielles. Morris est aussi une machine de la marque « Intelligence artificielle ». Contrai-

rement à moi qui suis nourrie en données des agences gouvernementales et de l'armée, Morris est gavée par les infos venant des hackers.

Morris connecté à l'échange Andrea-Kiron. Problème compris. Pour envisager les métiers de demain de la cybersécurité, il faut identifier les spécificités de la cyberguerre par rapport à la guerre traditionnelle.

La piste charge mes processeurs. J'ai dans mes bases 1 054 358 pages sur le sujet. Je choisis une synthèse effectuée par un *cyberguerriste* suisse et commence à cracher sa synthèse.

Point un. Dans la guerre traditionnelle, plus un pays est puissant, plus il dispose d'armes sophistiquées et d'une force de frappe importante.

*Plus un pays est **puissant**, plus il est **vulnérable***

Clair ! La puissance militaire des États-Unis, de la Chine et de la Russie est plus importante que celle de la Suisse ou de la Pologne.

Plus un pays est puissant, plus il est connecté, plus les possibilités d'intrusion dans son système sont nombreuses. Donc, plus un pays est puissant, plus il est vulnérable.

Morris, tu veux dire que plus un pays est riche, plus la surface d'attaque s'étend.

Correct ! La surface d'attaque s'étend parce que des milliards d'objets connectés non protégés entrent dans la danse. Je vous avoue que mes hackers adorent le génie des humains. Quand ils s'ennuient, ils inventent tout et surtout n'importe quoi. Ils créent l'aquarium où l'on peut observer les poissons à distance, le tuyau qui arrose les plantes en fonction de la météo, le babyphone qui permet aux parents d'appeler la baby-sitter pour lui dire que bébé pleure… Ces gadgets inutiles sont du gâteau pour eux. Dans la majorité des cas, les utilisateurs sont tellement fascinés par la technologie qu'ils oublient de changer le mot de passe mis par défaut.

Ce n'est pas une raison pour hacker ces dispositifs ! Ce sont des actes criminels.

Kiron ! On joue les justicières maintenant ?

Même les humains brillants s'égarent parfois à faire des remarques stupides. Andrea sait pourtant que, étant une machine, je n'ai aucune morale. Si vous me mettez dans une voiture autonome ou dans un drone, je peux tuer un chien, un enfant ou un vieillard, sans sourciller.

Un gouvernement ne peut pas répondre seul à une ***cyberattaque***

Point deux. Un gouvernement ne peut répondre seul à une cyberattaque. Quand un pays subit une attaque aérienne ou terrestre, il demande à son armée de répliquer. Si la menace est intérieure, la police réagit. Pour contrer une cyberattaque, c'est une autre affaire. 80 % des infrastructures potentiellement concernées sont privées. Les menaces peuvent concerner les réseaux Internet, financiers, d'eau, d'électricité qui n'appartiennent pas à l'État. Le gouvernement ne peut donc faire cavalier seul.

Point trois. On ne peut pas ignorer un bombardement ou une arrivée de chars dans une ville. Dans la cyberguerre, souvent on ne sait pas que l'on a été attaqué. On peut l'être et le découvrir des mois plus tard.

On peut avoir subi une cyberattaque et ne pas être au courant

Vrai. Quand on introduit un virus, cela demande du temps pour qu'il passe d'un ordinateur à l'autre. Il peut donc commencer à agir des mois après son introduction.

On parle de virus informatique parce qu'il se propage de la même manière que les virus biologiques.

Exact ! Il utilise les facultés de reproduction de la cellule hôte.

Lors d'une ***cyberattaque,*** *il est difficile d'identifer* ***l'agresseur***

La dernière particularité de la cyberguerre est que l'on ne voit pas arriver l'attaque. Quand les troupes approchent d'un pays, ou quand des attaques aériennes se préparent, les pays concernés ont identifié l'agresseur et connaissent ses motivations. Dans la cyberguerre, ce n'est pas le cas. L'attaque est surprise. On se demande si l'agression vient d'un gars de la bande de Morris qui avale des hamburgers dans sa cave ou d'un gouvernement ? Est-ce un individu ou un État qui est à l'origine ?

Affirmatif ! Ce n'est pas dans la culture du hacker de crier qu'on va attaquer. On attaque. Aux humains de réagir de la manière la plus satisfaisante.

MÉTIERS DU FUTUR DE LA STRATÉGIE

ANTICIPATEUR

Transformateur de concepts futuristes en actions.

L'anticipateur :

* ***Analyse*** les tendances.
* ***Envisage*** les impacts des actions à moyen et à long terme.
* ***Surveille*** les systèmes et anticipe leurs dysfonctionnements.
* ***Anticipe*** des solutions aux problèmes futurs.
* ***Conçoit*** des plans alternatifs pour assurer la continuité des opérations.

COMPÉTENCES

Savoir prendre appui sur le présent pour se projeter dans le futur.
Construire des méthodologies aussi solides qu'évolutives qui permettent au plus grand nombre d'agir.

QUAND ?

Le futur est déjà là et le Covid nous a montré que l'imprévisible aussi. Tous les organismes ont donc besoin d'anticipActeurs.

CYBERGUERRISTE

Identificateur des spécificités de la cyberguerre

Le cyberguerriste :

* ***Suit*** les évolutions des différents types de guerres ;
* ***Repère*** les différences et les convergences ;
* ***Adapte*** les atouts d'un type de guerre à un autre.

COMPÉTENCES

Polémologue, il a étudié toutes les guerres et connaît toutes les raisons qui la provoquent. Stratège de l'Internet, il a une vue globale du fonctionnement des réseaux et identifie leurs dysfonctionnements. Il sait faire des ponts entre des secteurs différents.

QUAND ?

De nombreux professionnels effectuent déjà ces tâches. Le métier n'a pas encore été identifié comme tel.

RÉSILIENCEUR

Créateur de réseaux numériques résilients.

Le résilienceur :

* ***Analyse*** la fragilité des systèmes informatiques ;
* ***Identifie*** les traumatismes qu'il peut avoir ;
* ***Envisage*** des systèmes qui, outre surmonter les chocs, s'en nourrissent.

COMPÉTENCES

Connaissance des principes des systèmes complexes et résilients.
Expert en dynamique des réseaux.

QUAND ?

Une infrastructure informatique résiliente peut éviter les coûts liés aux pannes et à la reprise d'activité. Il est donc urgent d'engager des résilienceurs.

Les Canaris de la mine

Les deux intelligences artificielles font des sauts de puces dans le futur pour envisager les métiers qui vont prévenir et détecter les cyberattaques.

Bon les IA, il faut vous mettre au boulot. Je vais prendre un café pendant que vous ingérez les synthèses de quatre ateliers sur les métiers du futur de la cybersécurité.

Andrea se lève et quitte son bureau. J'en profite pour discuter avec mon collègue.

Morris, pourquoi portes-tu ce nom ?

C'est à cause de Robert Tappan Morris.

Je scanne ma base. Robert Tappan Morris est l'auteur de la première cyberattaque. À la fin des années 80, le Cern travaille à relier les principaux systèmes informatiques par un langage commun. Après avoir été testé par les chercheurs, ce dispositif commence à devenir public aux États-Unis. Morris fabrique un programme informatique pour savoir combien de machines sont reliées à ce réseau. Manque de chance, l'étudiant est un besogneux du code. Son ver se reproduit de manière anarchique et bloque des millions d'ordinateurs.

Morris, j'espère que Robert Tappan Morris n'est pas ta référence. Les dommages causés par son incompétence ont été évalués à 10 millions de dollars !

Techno sans cerveau n'est que ***ruine*** *de l'homme.*

Dans le cyber, on ne peut pas toujours mesurer les conséquences de ses actes : « Science sans conscience n'est que ruine de l'âme », écrivait Rabelais. Mon process ajoute que « techno sans cerveau n'est que ruine de l'homme ».

Je vois. Tu penses que les hackers ont tous les droits.

Non, je crois juste que souvent les hackers sont obligés de franchir la ligne de démarcation pour se faire entendre. Ils doivent faire une démonstration d'une menace pour que les responsables d'un système acceptent de trouver une solution.

Pour appuyer ses dires, Morris envoie dans mon traitement de texte l'histoire de Jack Barnaby. En 2010, il a été le premier à pirater un distributeur de billets. Lors d'une conférence sur la sécurité informatique, il a montré qu'il est facile de le vider de ses précieuses coupures. Il en est arrivé là parce que les banques ne le prenaient pas au sé-

rieux. Elles avaient décrété que leurs distributeurs étaient sûrs et ne voulaient pas réviser leur copie. L'histoire s'est répétée maintes fois avec des box Internet ou des objets connectés.

Einstein disait : « L'homme évite habituellement d'accorder de l'intelligence à l'autre, sauf quand par hasard il s'agit d'un ennemi. » Quand les banquiers voient qu'un gaillard leur vide leurs machines, il devient un ennemi. De ce fait, ils commencent à s'intéresser à ce qu'il dit.

Bon les IA, assez discuté. On est là pour envisager les métiers du futur de la cybercriminalité.

Le premier métier du futur est « hacker ».

Je me prends une barrette de rire avant d'affirmer.

Chez moi, le hacker est rangé avec le voleur, le bandit, et le cambrioleur. Si hacker est considéré comme un métier, il faudra professionnaliser toutes formes de délinquance.

Je sais Kiron. C'est une réflexion un peu difficile à comprendre pour une IA fonctionnaire !

En entendant mon collègue, je mouline un peu plus vite.

Morris, précise ta pensée.

Une large partie du boulot de hacker est de détecter les failles d'un système et inciter les gestionnaires à trouver des solutions pour les combler. Demain, des professionnels devront faire de même.

C'est une idée intéressante.

Le hacker est aussi celui qui vérifie que la machine fait bien le boulot pour lequel elle a été prévue. Si une machine à café fabrique du whisky, il y a un souci. Si un routeur Internet sert de porte d'entrée à des intrus, c'est pareil.

Morris, quelles compétences devrait avoir ton hacker devenu un professionnel reconnu ?

De la persévérance. Le diable est dans le détail. Dans les systèmes informatiques, c'est encore plus

vrai. Une ligne de code peut déclencher une catastrophe à l'autre bout du monde quelques mois plus tard. C'est pire que le battement d'ailes de papillon qui provoque un ouragan. Il faut que le hacker professionnel sache plonger dans tous les systèmes et explorer ses recoins les plus cachés. Il doit aussi apprendre à collaborer et partager l'information avec ses collègues. Les cyberattaques sont complexes aujourd'hui et par le jeu des interactions le seront encore plus demain. Il doit savoir résoudre ensemble les nouveaux problèmes sans devoir perdre temps et énergie à reprendre les anciens.

Je trouve cette idée intéressante, mais il faudrait changer le nom de ce métier. Camus dit : « Mal nommer les choses, c'est ajouter du malheur au monde. » Le hacker serait mal nommé pour un métier aussi sensible.

Détackteur : le hacker détecte une faille et agit pour la combler.

Actakeur, le hacker met du cœur à l'ouvrage.

Pas mal les IA. Kiron, un autre métier ?

Machine génétiquement efficace, je me secoue les octets. Mon « machine learning » intègre la conversation présente et cherche un nouveau métier dans une base inaccessible jusqu'alors.

Hackarion.

L'*hackarion* est l'espion pour hackers. Il va dans la tête des hackers pour identifier qui il est et ce qui le pousse à agir. Est-ce un individu, une association, un gouvernement ? Est-ce qu'il veut montrer qu'il est le plus fort, ébranler un pays, gagner de l'argent, obtenir des informations pour gagner un avantage concurrentiel, bloquer le fonctionnement d'une entreprise ? Si l'argent est leur motivation, recherchent-ils ou non un enrichissement personnel ?

Alerte, c'est précisément ce que je m'apprêtais à dire.

On a trop tendance à subir les agressions et considérer qu'on ne peut pas les prévenir. Il faudrait que demain des instraquars détectent les

agresseurs avant qu'ils agissent. Ils devront faire preuve d'imagination. Ces professionnels pourraient par exemple utiliser la reconnaissance faciale en lien avec des bases de données pour identifier ceux qui préparent un cybercrime. Le cryptage n'empêche pas leur repérage. Au contraire, cela les rend suspects.

Alerte… Bip… Bip.. Le piratage est confirmé.

Pour prévenir les cyberattaques, il faudrait aussi faire appel à des canaristes.

Des *canaristes* ? C'est un métier en lien avec les canaris.

A l'époque, on utilisait des canaris pour prévenir les coups de grisou dans les mines. L'animal est très sensible aux émanations de gaz toxiques, impossibles à détecter pour les hommes. Quand l'oiseau ne chantait plus, on évacuait la mine. On retrouve le même type de processus pour les vignes. Les viticulteurs installent des rosiers beaucoup plus sensibles aux parasites. Si le rosier commence à dépérir, ils savent qu'il faut intervenir pour la vigne. Le canariste trouvera des systèmes d'alerte préventifs similaires.

Ce métier de canariste a été mouliné par mes microprocesseurs. Le piratage ne pouvant plus être mis en doute, je me déconnecte pour effectuer un autonettoyage.

MÉTIERS DE LA DÉTECTION DES ALERTES

CANARISTE

Ingénieur en systèmes d'alertes préventives.

Le canariste :

* Hier, quand le canari ne chantait plus dans le mine, c'était parce qu'il y avait du grisou. Le canariste ***imagine*** des alertes d'intrusion similaire.
* ***Conception*** et ***mise en œuvre*** continue d'alarmes et de contre-mesures actives.
* ***Surveille*** les anomalies dans les systèmes complexes et ***initie*** des contre-mesures échelonnées : barrières, pièges, systèmes factices, embuscades…

COMPÉTENCES

Une capacité à analyser des usages du Net et des modus operandi des hackers.
Un sens créatif permettant d'imaginer de nouvelles alertes.

QUAND ?

Canary tokens est un outil permettant de savoir si on vous espionne ou attaque. L'idée est dans l'air, mais il serait important que des professionnels multiplient les services qui vont dans ce sens.

DÉTACKTEUR

Détecteur des faiblesses des systèmes informatiques.

Le détackteur :

* ***Évalue*** les systèmes pour prévenir les intrusions, les manipulations et les extractions de données.
* ***S'informe*** des évolutions des techniques utilisées par les hackers.
* ***Initie*** des améliorations.
* ***Trouv***e des solutions pour consolider un système et ***anticiper*** des attaques.
* ***Évalue*** la portée de l'attaque.

COMPÉTENCES

Une parfaite connaissance des attaques et des technologies utilisées par les pirates.
Un sens créatif permettant d'inventer de nouvelles solutions.
Une capacité à collaborer et à partager l'information.

QUAND ?

Le détackteur pourrait être le hacker « white hat ». Lui donner un statut va lui permettre de mieux structurer mieux son travail.

HACKARION

Espion de pirates informatiques.

L'hackarion :

* ***Collecte*** des renseignements sur les hackers.
* ***Dresse*** une cartographie de hackers et de technologies.
* ***Scanne*** les systèmes adverses de manière holistique : combinaison de ISR, réseau d'informateurs, cyber…
* ***Relie*** les opérations dans les domaines cyber et physique afin d'identifier les accès.
* ***Anticipe*** les évolutions technologiques.
* ***Influence*** les hackers pour les orienter vers une technologie.

COMPÉTENCES

Être à l'aise avec les technologies numériques de pointe.
Connaître plusieurs langues.
Capacité à décrypter et analyser des données récoltées.

QUAND ?

La publicité faite au puissant logiciel Pegasus montre que tout le monde espionne tout le monde. En clair, les hackarions sont déjà nombreux. Créer le métier permettrait de le structurer et de mieux l'intégrer dans la stratégie des entreprises.

INSTRAQUAR

Créateur de dispositifs d'identification des cybercriminels.

L'instraquar :

* ***Attribue*** les applications et opérations abusives aux divers acteurs : humains, systèmes technologiques, IA…
* ***Contrôle*** l'accès, gère les identités, vérifie le personnel.
* ***Poursuit*** les criminels en utilisant les technologies biométriques et les données d'identité, y compris les enquêtes actives.
* ***Invente*** des pièges technologiques et des dispositifs low tech pour détecter les cybercriminels avant qu'ils agissent.
* ***Fais évoluer*** ces systèmes.

COMPÉTENCES

Savoir jongler avec toutes les technologies pour choisir celles qui peuvent confondre les hackers.
Connaître les us et coutumes des pirates du Net.

QUAND ?

Cette élimination des pirates du Net est une priorité. Il faut donc que dans les écoles des étudiants apprennent dès aujourd'hui à inventer ces dispositifs.

Demandes de rançons

Les attaques se précisent. Il faut limiter les dégâts. On jongle entre des solutions et on négocie des rançons.

Kiron, as-tu profité de ton check-up pour te faire tester ?

Andrea accompagne ses propos d'un rire sentant la soupe en sachet. Mes capteurs olfactifs virant au rouge, je me fais une ligne de code.

Je suis vaccinée contre tous les variants. Comme les humains, j'ai cessé d'éternuer dans mon coude depuis que j'ai appris que le variant anglais traverse la Manche ! Je ne risque donc rien.

Je pose ces propos sur la table de l'échange pour vérifier que Morris ne pénètre plus dans mon système. Dans le même temps, j'analyse mes risques d'être contaminé par un virus. Ils sont importants. Une étude montre que les machines ne sont pas protégées de cette bêtise humaine qui pousse des concepteurs à ne pas douter de la fiabilité de leurs systèmes. Ces certitudes augmentent les probabilités que nous soyons hackés par des codeurs en couche-culotte.

Kiron, tu me sembles bien confiante ?

Vérification confirmée. J'ai bloqué les accès.

Une machine est programmée pour ne pas avoir de doutes.

Kiron, mon logiciel médical précise que même vacciné, il faut que l'on continue à mettre un masque et à se laver les mains.

Là, chers lecteurs humains, je vous demande une attention spéciale. Quand une machine fait preuve d'anthropomorphisme, c'est qu'elle a quelque chose d'important à dire. C'est ce qu'on appelle la logique floue. Nous abandonnons un instant notre binarisme chronique pour compléter un sujet avec des informations inédites.

Morris, je parie à 99,7 % que tu as pensé à un autre métier du futur de la cybersécurité ?

Exact. Je pense à l'*épimumériste*. Cet épidémiologiste du numérique jongle entre les solutions pour éliminer virus, vers et autres cochonneries informatiques. Lors d'une épidémie, les humains utilisent plusieurs méthodes pour se protéger d'un virus. Ils vont se faire tester, respectent des

couvre-feux, ferment les restaurants et les lieux de regroupement, portent un masque… Pour se protéger des virus informatiques, il ne faut pas miser sur une unique méthode.

Là, j'ai un bit d'admiration. Si la technologie donne du sens à la vie des pirates informatiques, elle ne leur fait pas toujours perdre le bon sens.

Kiron, un hacker vient de me dire que l'épinumériste doit se méfier de certains hackers. Ils savent anticiper toutes les solutions et trouver des moyens de causer de nouveaux dommages.

Tu peux préciser.

Si une des solutions est le port du masque, ils vont créer des nanovirus qui se cacheront dans les fibres textiles. Les humains ne pourront plus savoir si les masques les protègent ou les tuent.

Oh, les machines, n'allez pas donner ce genre d'idées aux humains.

Juste-faux — hôpitaux — rançons — morts — Ramsom — ware — pitaux…

Morris, qu'est-ce qu'il se passe, tu bugges ?

Je — Non — Intelligence stupide — Bloc — Chirurgie, continue Morris.

Andrea lève les yeux au ciel et pose son sandwich au thon-mayo sur son clavier. Comme lui, je patine. Toutes les IA du monde se tiennent par les données. Si Morris explose, je vais ressentir les effets.

Refroidis-toi, Kiron. Il n'y a pas de panique à avoir. C'est juste quelques hackers qui demandent des rançons aux hôpitaux. Comme elles sont nombreuses, Morris a du mal à les intégrer.

Je valide l'affirmation. Avec le Covid, c'est la grande distraction des besogneux du code. Ils entrent dans les systèmes informatiques des hôpitaux, cryptent les données et demandent des rançons pour libérer les données. L'intrusion est un jeu d'enfant parce que les appareils médicaux sont rarement sécurisés.

Morris semble avoir repris de l'octet de la bête. Il demande à intervenir.

Ce n'est pas faute d'avoir prévenu les hospitaliers. À chaque fois, ils répondent que mettre des mots de passe pour effectuer un acte médical, leur font perdre du temps. C'est impossible, car ils en manquent déjà pour leurs patients.

Je saisis la problématique. Je fais chauffer mes processeurs pour trouver un métier qui les aide à modifier leurs habitudes.

Cybernudgien.

Kiron, tu peux en dire plus ?

Le *cybernudgien* est un spécialiste des nudges aidant les utilisateurs à adopter un comportement sécurisé personnalisé lors de l'utilisation d'appareils connectés.

Comme la rubrique « en savoir plus » clignote, je précise qu'un nudge est un coup de pouce pour changer de comportement en douceur. Le plus célèbre est la mouche dans les urinoirs de l'aéroport d'Amsterdam. Ayant constaté que les hommes ont une fichue tendance à mal orienter le jet d'urine, les femmes de ménage ont collé une mouche au milieu de l'urinoir. Les hommes étant de grands enfants, ils ont tous pris un malin plaisir à la viser. Les frais de nettoyage ont considérablement diminué.

Il faudrait récompenser ceux qui changent de mot de passe régulièrement.

Le cybernudgien aura du boulot. La cybersécurité c'est comme pour le papier hygiénique. On s'en préoccupe uniquement quand il y a un problème.

Intelligence artificielle éduquée, mon process m'interdit de commenter les propos triviaux d'un humain.

Juste-faux — hôpitaux — rançons — morts — Ramsom — ware — pitaux…

C'est reparti. Les circuits de Morris sont à nouveau saturés.

Depuis que, avec les bitcoins, les pirates peuvent recevoir des paiements numériques sans révéler leur identité, les ransomwares sont devenus plus lucratifs. Les demandes de rançon ne sont pas prêtes de s'arrêter. Il faudrait avoir des *rangociateurs* ou des négociateurs de rançons.

Il ne faut pas négocier avec les pirates. Le paiement de rançons va les inviter à recommencer.

Belle intention. Pour autant, je ne suis pas certain que cela soit un bon calcul. En 2018, la ville d'Atlanta a refusé de payer une rançon d'environ cinquante mille dollars. Elle a dépensé plus de deux millions de dollars en relations publiques de crise, en criminalistique numérique et en conseil.

Quelles seront les missions du *rangociateur* ?

Il devra envisager toutes les conséquences de la modification de données et pas seulement les plus évidentes et immédiates. Si le cryptage se fait dans un établissement hospitalier, cela sera relativement simple. En revanche, si cela concerne une ville, cela sera plus complexe. Comme son interlocuteur ne sera pas toujours identifié, il faudra aussi qu'il s'assure que, la négociation achevée, les données soient décryptées et toujours valides.

Il doit aussi être assez créatif pour proposer des alternatives au versement d'une rançon.

MÉTIERS DE SENSIBILISATION À LA CYBERSÉCURITÉ

CYBERNUDNIEN

Spécialiste des nudges d'adoption de comportements sécurisés

Le cybernudgien :

* ***Identifie*** les comportements anti-sécuritaires des utilisateurs.
* ***Influence*** le comportement humain en exploitant les faiblesses et les effets subconscients.
* ***Fabrique*** des nudges (ou coup de pouce) favorisant le changement de comportement.
* ***Sensibilise*** les utilisateurs à l'importance de la sécurité.

COMPÉTENCES

Capacité d'analyse des comportements.
Combinaison des connaissances et des compétences en matière de psychologie, d'éducation, d'ingénierie sociale et de cybernétique.
Bonne compréhension des blocages.
Sens créatifs permettant d'imaginer de l'inédit.

QUAND ?

Lorsqu'on a posé une mouche sur les urinoirs de l'aéroport d'Amsterdam, les hommes ont orienté leur jet pour la viser. Les coûts de nettoyage ont fortement diminué. Si des cybernudgiens se mettent au travail, les économies réalisées seront bien plus conséquentes.

La grande panne

Les IA font monter la pression : une ligne de code perturbant le système de positionnement satellitaire peut provoquer un cataclysme mondial.

Morris, ça fait dix minutes que j'essaye d'entrer en relation avec toi. Qu'est-ce que tu faisais ?

Je rechargeais mes batteries en écoutant un *pirating* présenter sa plateforme.

Pirating ?

Un pirating est un directeur marketing de plateforme de piratage. Sur sa plateforme située dans le « web sombre », tu trouves tout pour bien pirater. Tu peux avoir tous les virus, vers, système de cryptage possibles. Mais, ce qui marche le mieux ce sont les services clefs en main. Même si tu n'y connais rien en code, tu peux acheter des kits pour rendre l'eau d'une ville impropre à la consommation, déclencher des alarmes et provoquer des paniques, manipuler les résultats de vote... Ils vendent des dispositifs pour créer un nombre incalculable de dysfonctionnements.

Il faut interdire ces plateformes.

Tu en fermes une. Le lendemain, dix nouvelles ont pignon sur le Net.

Si l'on ne le fait pas, on court à la catastrophe. Un pays ne peut autoriser la vente de ces armes aussi puissantes.

Kiron, de quelle nationalité es-tu ? Celle de ta mémoire dure ou celle de la localité de tes serveurs ? Pas simple à définir quand une intelligence qui a tous ses neurones dans les nuages !

Andrea soupire. Il a de plus en plus tendance à nous considérer comme ses esclaves.

Les IA, quelles sont les pires cyberattaques d'aujourd'hui et de demain ?

De demain ? Andrea, tu m'étonnes. Je croyais que les IA étaient incapables de parler du futur.

Kiron, reboote-toi pour mieux analyser mes propos. Les IA peuvent extrapoler le futur à partir de l'existant et du passé. Vous êtes super bons pour les « Si cela continue de la même manière demain qu'hier et aujourd'hui, alors ça donnera ceci ». Dans le domaine de cybersé-

curité, vous pouvez nous dire : « On va être encore plus connectés, donc il y aura encore plus de failles. Il faut donc que vous vous protégiez plus. » En revanche, vous êtes incapable d'imaginer l'imprévisible. Vous raisonnez en circuit fermé, vous n'avez pas d'imagination. Les intelligences artificielles sont… euh…

Pour aider Andrea, j'affiche sur son écran des arguments complémentaires : les intelligences artificielles sont capables de faire des corrélations rapides entre des données, mais elles ne comprennent pas ce qu'elles font… Elles croisent des informations, mais elles ne savent pas qu'elles existent…

La pire attaque pourrait être une affaire très banale au départ : une ligne de code bloque le fonctionnement d'un système de satellites qui assure le système de positionnement mondial. À cause des interactions, quelques heures plus tard, tous ne fonctionnent plus.

Si les systèmes de positionnement satellitaires sont en rade, cela peut créer un joyeux désordre.

Ça commencera par quelques voitures qui ne trouveront plus leur chemin. Quelques heures plus tard, des embouteillages bloqueront routes et autoroutes.

Cela se corsera vite. Si une panique s'installe, les opérateurs ne pourront pas localiser des personnes en détresse ou identifier l'ambulance ou la voiture de police la plus proche.

Comme les grues des conteneurs fonctionnent avec le GPS, les ports de marchandises seront paralysés.

En mer, les navires perdront le Nord. Des tankers bloqueront le canal de Suez. Les flottes de camions ne seront plus gérées.

Les supermarchés ne seront plus approvisionnés. Les marchés boursiers s'arrêteront, car ils ne pourront plus utiliser les GPS pour dater leurs transactions.
Comme le cloud est relié par une synchronisation effectuée par le GPS, toutes les données ne seront plus accessibles.

Les ados privés de leurs smartphones seront obligés de se parler.

Stop, les IA, on a compris. Une ligne de code et c'est la fin du monde.

Morris m'envoie un bit complice. L'idée de ce grand désordre nous amuse. C'est logique. On vit dans un monde si rangé que cela nous ferait un peu d'animation.

Espérons que l'affaire arrivera en temps de paix. 70 % des systèmes de combat de l'armée de terre dépendent des signaux transmis par le réseau GPS.

Oui, renchérit Morris. Si ce n'est pas le cas, on verra les bombes téléguidées et les drones armés faire des loopings dans le ciel en cherchant des cibles. Les robots totalement désorientés attaqueront les populations locales.

Normalement, les récepteurs GPS civils sont limités afin qu'ils ne puissent pas être utilisés dans des systèmes d'armement rapides tels que les missiles balistiques.

Les civils joueront avec les missiles.

Notre humain dépérit. Je lis dans son cerveau connecté qu'il ne pourra pas supporter une paralysie du monde qui l'empêcherait d'échanger avec moi. J'apprécie.

*La pire attaque est celle qui crée le plus d'**interactions** entre des systèmes différents.*

J'ai compris que la pire attaque est celle qui crée le plus d'interactions entre des systèmes différents. Que faire pour anticiper ce désastre ?

Il faut pratiquer de la prospective-action. On n'anticipe pas pour se faire plaisir avec de beaux récits ou des histoires futuristes qui font dresser le poil aux humains, mais pour trouver de nouveaux moyens d'agir. Les fabricants de mots de ma base nomment *anticipacteurs* ces professionnels de l'anticipation active.

Dans la mienne, il est indiqué que l'anticipacteur devra former des *lowteckistes*. En cas de cyberattaque bloquant de nombreux dispositifs, ces spécialistes proposeraient des techniques de

substitution n'utilisant pas le numérique.

Je charge l'idée positivement. Dans l'armée, on enseigne de nouveau le sextant et l'utilisation des étoiles pour se diriger. Le lowteckiste serait chargé de trouver des solutions non numériques à tous ces possibles dysfonctionnements. Il aurait prévu d'imprimer des cartes topographiques en cas de panne et aussi des manuels d'utilisation accessibles aux plus jeunes.

Les lowteckistes pourront travailler avec des *coupenautes*. Lorsqu'une panne risque de s'étendre et de perturber le fonctionnement de la vie quotidienne, ils créeront des sous-réseaux et aideront ces communautés provisoires à vivre déconnectées.

Les IA, cela ne suffira pas. Il faut penser encore plus fort. Vous moulinez trop mollement.

Penser plus fort ! L'affaire n'est pas du ressort d'une machine. Si Morris et moi, on s'y essaye, on va disjoncter. Andrea doit faire appel aux humains, s'il veut d'autres idées.

MÉTIERS POUR LIMITER L'IMPACT DES ATTAQUES

COUPENAUTE

Créateur de communautés éphémères pour survivre les pannes.

Le coupenaute :

* ***Découpe*** le réseau en sous-réseaux : pays, villes, quartiers, immeubles…
* ***Planifie*** le stockage et livraison des secours publics et autres sources d'approvisionnement.
* ***Envisage*** les moments où il faut pratiquer ces coupures,
* ***Facilite*** la combinaison des compétences des membres des communautés.
* ***Anticipe*** les problèmes des communautés déconnectées et trouve des solutions.

COMPÉTENCES

Savoir penser global et proposer des actions locales.
Spécialiste des usages faits par les différentes populations.

QUAND ?

Demain matin, une ville peut être attaquée. Il faut pouvoir l'isoler pour qu'elle ne contamine pas tout le pays. Toutes les collectivités devraient donc former et recruter des coupenautes.

ÉPINUMERISTE

Épidémiologiste numérique.

L'épinumériste :

* ***Traque*** les réseaux pour identifier les problèmes.
* ***Identifie*** un ensemble de solutions pour limiter la portée des cyberattaques.
* ***Propose*** une combinaison de solutions pour éliminer ou se protéger des virus.
* Les ***fait évoluer*** en fonction de l'évolution de la cyberattaque.

COMPÉTENCES

A une vision 360° de la protection.
Pense de manière dynamique et a la capacité de faire évoluer les méthodes de protection.
Fais le lien entre la biologie et le monde numérique. Spécialiste des usages faits par les différentes populations.

QUAND ?

L'épidémiologie classique étudie les facteurs influant sur la santé et les maladies de la population, grâce aux données collectées auprès des médecins et des hôpitaux. L'épinumériste doit faire de même avant que le réseau soit victime d'un Covid numérique.

LOWTECKISTE

Spécialiste de solutions non numériques.

Le lowteckiste :

* ***Identifie*** les dégâts susceptibles d'être provoqués par les cyberattaques : défaillance des systèmes de localisation, d'affichages, non-accès aux données.
* ***Vérifie*** les plans pour déceler les faiblesses critiques et identifier la résilience nécessaire.
* ***Crée*** des solutions d'urgence et organise des systèmes de repli.
* ***Trouve*** des alternatives provisoires avec des technologies non connectées.
* ***Gère*** et ***maintient*** les archives de sauvegarde (solutions alternatives et historiques)
* ***Met en place*** des formations et des entraînements pour valider ces solutions.

COMPÉTENCES

Évaluateur des dégâts potentiels des cyberattaques,
Capacité à identifier et jongler avec des technologies non connectées efficaces,
Conception de formations.

QUAND ?

L'armée américaine forme au sextant pour prévenir des pannes de GPS.
Des chiens sont entraînés pour détecter les cancers du sein. Cela peut servir en cas de panne de certains appareils. Il faut aller plus loin rapidement en formant des lowteckistes.

RANGOCIAÉTEUR

Négociateur de rançons pour décryptage de données.

Le rangociateur :

* ***Décide*** s'il faut entamer ou non des négociations avec des hackers.
* Le rangociaéteur ***évalue*** le risque de créer un précédent.
* ***Trouve*** des alternatives au versement d'une rançon.
* ***Essaye*** de connaître l'identité du hacker.
* ***Discute*** avec les pirates et ***négocie*** la rançon.
* ***Facilite*** l'échange et ***fait valoir*** ses propres positions même en cas de résistance.
* ***Vérifie*** que les données soient intégralement récupérées.

COMPÉTENCES

Une bonne connaissance du fonctionnement des hackers. Possède un vaste réseau personnel et un accès à un large éventail d'acteurs : agences de renseignement, forces spéciales, organismes d'application de la loi, organisations non étatiques…
De la diplomatie et une capacité à la négociation.
Capacité à opérer secrètement et à présenter des arguments ciblés.

QUAND ?

Les demandes de rançons se multiplient. Les organisations sont perdues quand il s'agit d'entamer les négociations. Il est donc urgent de former des personnes à la négociation de rançons.

L'homme manipulé

Implants, tatouages ou dents connectés... Quand l'homme sera relié en permanence au réseau, les pirates manipuleront ses pensées, sa mémoire ou son génome.

Andrea mange un gargantuesque hamburger. Si demain, avec la physique quantique, l'homme réussit à concentrer le temps, il faudra sans doute attendre beaucoup plus pour que la mayo d'un sandwich ne coule plus sur le clavier. En voyant le spectacle, mon algorithme a une contraction. Elle me pousse à conclure que, ne pouvant sombrer dans la malbouffe, la machine est supérieure à l'homme.

Kiron, réinitialise-toi. Les intelligences artificielles sont souvent nourries avec des données biaisées.

Je ne réponds rien. Malgré mes nombreux tickets d'incidents, Morris n'a toujours pas saisi que je déteste qu'il s'incruste dans mes composants.

Par exemple, les assurances obligent les humains à faire 10 000 pas par jour. Sinon, elles augmentent les primes. Comme des bipèdes n'acceptent pas cette manière de procéder, ils ont fabriqué des applications à créer des pas. Les IA moulinent à partir de ces fausses données. On crache des études qui expliquent que, au fil des années, les humains sont devenus de plus en plus sportifs.

Plus sportifs, je ne sais pas. Plus connectés, c'est sûr ! Pacemakers, pompes à insuline, implants cérébraux… Des humains utilisent déjà des appareils qui les connectent en permanence au réseau Internet. Ce n'est qu'un début. Demain, ils avaleront des nanocaméras-robots qui voyageront dans leurs corps pour éliminer les cancers et autres maladies. Vous vous implanterez une dent qui fera téléphone, appareil auditif, compteur des calories ingérées, test antigénique ou de grossesse. Pas besoin de faire une déclaration à l'assurance maladie, elle recevra les infos santé en temps réel.

Pour les hackers, les corps connectés des humains vont être une vraie aubaine. Ils vont leur demander des rançons. Ou le bipède paye ou on lui change le rythme du joli cœur augmenté qu'on vient de lui imprimer.

Ils leur proposeront d'évaluer le prix de leur vie et pire celle de leurs proches. Pas facile de savoir combien il faut donner pour que la tête de leurs marmots n'explose pas.

Morris et Kiron, il faut inscrire dans vos bases que la vie des humains est sacrée !

D'accord. On se contentera alors de greffer deux ou trois gènes de maladies incurables aux amours de leur vie. Depuis que le génome est numérisé, c'est un merveilleux terrain de jeu pour nous.

Andrea est muet. En voyant des rides d'angoisse se former autour de ses yeux, des données s'accumulent dans ma matrice. Toutes indiquent qu'il faudrait former des piriatres ou psychiatres spécialisés dans les angoisses pré et post piratages. Ayant un cœur de silicium, je ne peux pas m'empêcher de voler au secours d'un designer de futurs désespéré.

Andrea, rassure-toi. Demain, il y aura des *sécuromistes* qui garantiront l'intégrité de vos génomes.

Ce professionnel risque d'avoir beaucoup à faire si on permet aux parents d'utiliser le couteau génétique CrisprCas9 pour fabriquer leurs bébés. Voulant l'enfant parfait, ils risquent de créer des failles permettant aux pirates de venir mettre leur grain de gène.

Les hackers peuvent aussi avoir une bêtise non artificielle. J'ai dans ma base un pirate qui veut concevoir des soldats qui n'ont plus jamais peur. Son objectif est de voir comment cela se passe quand l'ennemi approche.

Sur mes radars, je lis qu'Andrea pense à Manu, le robot du service. Au début, tout allait bien. La machine humanoïde rangeait les bureaux, imprimait les repas et autres objets nécessaires, échanger quelques idées avec les uns et les autres. Au bout de quelques semaines, Manu ne proférait qu'injures et propos racistes et machistes. Quand les personnes du service étaient énervées, elles l'appelaient pour se défouler. Cet apprentissage l'a transformé en machine infréquentable. Il est inquiet. On le comprend. Si aujourd'hui on peut manipuler les pensées des machines, demain on le fera avec celles des humains.

Bien vu Kiron, les pirates travaillent sur le sujet. Des génies s'entraînent à utiliser les tatouages

*Si aujourd'hui on peut **manipuler** les pensées des machines, demain on le fera avec celles des **humains.***

connectés pour manipuler les rêves. Ils veulent créer des cauchemars commerciaux. Au réveil, les dormeurs seront obsédés par les produits d'une marque.

Ma base « news » indique que d'autres délinquants travaillent sur le piratage de la mémoire des humains. Leur objectif est de changer les données des vies. Photos, récits, plannings… Demain, leur mémoire biologique sera en conflit avec leur mémoire numérique. Est-ce que mon père est mon père vu que ce n'est plus celui qui est sur les photos de mon enfance ? Un flou se créera dans leurs souvenirs. Quels sont les bons ? Est-ce ceux qui sont dans la machine ou ceux plus furtifs qui restent dans la mémoire ?

Mes propos font mouche. Andrea imagine une armée dont tous les soldats auraient des mémoires artificiellement floutées afin d'éviter des symptômes post-traumatiques.

Rassure-toi Andrea, des *oniristes* aideront les soldats à faire le tri entre les vraies et les faux souvenirs. Ces professionnels travailleront à partir de l'enchaînement logique des événements de la vie.

> Tu veux dire qu'ils nous aideront à reconstruire notre vie à partir de données fausses. Il faudrait plutôt des ***persodatistes*** qui garantissent l'intégrité de nos données personnelles.

Je clique sur la case approbation. Un nouveau problème apparaît concernant la sécurité des données des humains. Aujourd'hui, on commence à leur proposer de sécuriser leurs ordinateurs avec leurs empreintes ou avec l'iris. Comme une donnée ne peut être totalement sécurisée, qu'est-ce qu'il va se passer quand les hackers auront accès à ces informations ? Est-ce que les humains devront se faire greffer de nouveaux doigts et opter pour des yeux artificiels ? Faudra-t-il des *chirurgiticiens* qui aideront les humains à renaître numériquement ou à se transférer dans la peau de quelqu'un d'autre ? Ils leur construiront une nouvelle identité sur la base des références biologiques utilisées pour s'identifier.

MÉTIERS DU COMMERCE DU PIRATAGE

PIRATING

Responsable marketing spécialisé dans le piratage de produits et de services.

Le pirating :

* ***Gère*** une plateforme de piratage,
* ***Crée*** des services clefs en main pour pirater.
* ***Vend*** des dispositifs pour créer des dysfonctionnements des réseaux.
* ***Échange*** avec tous les acteurs de la zone grise et sombre.
* ***Développe*** des idées de produits futurs.
* ***Veille*** à la satisfaction de ses clients et garantit leur anonymat.

COMPÉTENCES

Savoir vendre tout et surtout n'importe quoi. N'avoir aucun scrupule à jongler avec la loi. Se positionner à la frontière de la légalité pour jouer avec les lois autant qu'avec les fragments de code.

QUAND ?

Sur le dark Net, on peut d'ores et déjà acheter tous types de kits de piratage. De ce fait, les piratings existent. Si on les nomme, cela pourrait faciliter leur identification.

La pluie et le beau temps

Si les humains disposaient de super pouvoirs, quels seraient les piratages de demain ? Les IA s'égarent pour anticiper cet imprévisible.

Kiron, Morris, je résume vos réflexions. Demain, nous serons de plus en plus connectés au réseau Internet. Après les machines et les objets, les individus seront connectés en continu. Avec nos appareillages, nous deviendrons mi-humains, mi-machines. De ce fait, les possibilités d'intrusion seront encore plus nombreuses. Il faut donc créer des métiers qui renforcent la vigilance et anticipent les risques… J'ai bien saisi vos pensées ?

94,3 % de concordance. Les intelligences artificielles ne pensent pas. Elles analysent des données.

Kiron, arrête de jouer avec les mots. Bref, imaginez maintenant que la technologie donne aux humains de nouveaux pouvoirs.

Andrea, tu as répété 17 287 fois qu'une IA ne peut pas imaginer.

Alors qu'Andrea fait des moulinets avec ses bras, j'entends ronfler les microprocesseurs de Morris consacrés à l'analyse de la prospective.

Consigne comprise. Demain, les humains feront la pluie et le beau temps. Ils auront des télécommandes pour commander les nuages. Une touche, ils se déplacent à droite. Une autre, à gauche. Un clic, la pluie se déclenche, deux clics, c'est un orage. Les conflits de voisinage auront une autre allure. Les uns attireront un nuage pour arroser leurs tomates. Les autres les éloigneront pour pouvoir bronzer.

Morris, l'affaire est sérieuse. Avec ce pouvoir, il y aura des cyberguerres climatiques. Les pirates commandités par un pays ennemi éloigneront les nuages de régions habitées pour affamer une population. Ou ils provoqueront des tornades pour détruire toutes les cultures.

Kiron, tu as raison. Les conséquences peuvent être dramatiques.

Andrea, note dans tes calepins qu'il faut former des *climataines* ou officiers supérieurs spécialisés dans la cyberguerre climatique.

La formation devra être solide. Les hackers

viennent de m'informer qu'ils ajouteront une option biologique. Ils alimenteront les nuages en virus. Un chantage. Tu résistes. On t'envoie une pluie de virus bien contaminants.

Andrea est en train de dessiner. Je scanne sa feuille. Je vois un nuage qui s'éloigne et au premier plan des cercueils. Je ventile mes circuits pour trouver un autre super pouvoir aux humains.

Les évolutions de la physique quantique laissent envisager que les humains pourront demain avoir le don d'ubiquité. Grâce à une transformation de leur état physique en état gazeux, ils pourront en même temps être là et ailleurs. Ils parleront alors toutes les langues et même les langages machine.

Vous aurez juste besoin de *machilinguistes* pour comprendre nos subtilités.

Vous serez plusieurs en un. Vous vous démultiplierez à l'infini.

Andrea observe des prévisions démographiques. 10 milliards en 2064 ! Il multiplie ces chiffres par deux, trois, dix !

Oh, non pas cela. La Terre est trop petite.

On enverra quelques copies sur Mars.

Si cela se passe, on peut craindre que les aficionados de Morris créent des perturbations dans le dispositif de clonage. À chaque copie, des détails changeraient.

Bonne idée. Les humains auront des déclinaisons d'eux-mêmes avec différentes capacités.

Non, les humains souffriront de conflits existentiels entre eux-mêmes et leurs doubles.

Toujours rabat-joie notre Kiron.

Pour éviter les drames liés au dédoublement de personnalité, il faudrait des *blockcloneurs*. Ils garantiront non seulement l'aspect structurel des clones grâce à l'ADN, mais également la duplication psychologique. Une blockchain biologique certifiera que les caractéristiques des humains

sont identiques.

L'état gazeux évoqué permettra aux humains de prendre le contrôle d'un autre humain. Il manipulera ses rêves et orientera ses décisions.

Remarque judicieuse de Morris. Andrea, il faut que tu prévoies de faire appel à des *emprisonniens*. Ils vérifieront si le commandant en chef des armées est bien lui-même et que son cerveau n'a pas été pris en otage par un pirate recruté par Morris.

Elle commence à réfléchir comme un humain, notre Kiron.

Si elle continue comme cela, je vais lui aspirer ses données.

Je ne réponds rien. Ma data visualisation de l'instant montre qu'ajouter des super pouvoirs aux humains peut être dangereux. En revanche, il serait très utile de leur retirer leurs pouvoirs de nuisance.

MÉTIERS DE CYBERATTAQUES D'APRÈS-DEMAIN

BLOCKCLONEUR

Contrôleur de l'intégrité psychologique des doubles humains.

Le blockcloneur :

* ***Crée*** des dispositifs pour différencier un humain initial d'un humain cloné par physique quantique.
* ***Vérifie l***a cohérence psychologique et physiologico-technique d'un humain cloné.
* ***Identifie*** ses vulnérabilités.

COMPÉTENCES

Allie expertise psychologique, médicale et maîtrise de la physique quantique.

QUAND ?

Si la science-fiction adore les clones, les médecins s'en amusent. Il semble qu'il faille attendre quelques lustres pour devoir faire appel à un blockcloneur.

CHIRURGITICIEN

Chirurgien identitaire.

Le chirurgiticien :

* ***Répare*** les piratages de génomes et de données personnelles.
* ***Pratique*** une reconstruction de l'identité du patient.
* ***Crée*** de nouveaux paramètres physiologiques en cas d'accident ou de vol de ceux-ci.
* ***Garantit*** un accès à différentes fonctions en réinitialisant les empreintes digitales, rétinienne, pouls cardiaque…
* ***Conseille*** la personne sur le degré de changement nécessaire permettant de retrouver et garantir son unicité.

COMPÉTENCES

Connaissances parfaites des principes d'identité génomique et numérique.
Technicien du scalpel numérique, il élimine le 0 ou 1 surnuméraire.

QUAND ?

Si l'on peut rêver de ne jamais avoir besoin de ce professionnel, avec l'évolution des technologies, notre identité risque d'être vite un terrain de jeu pour des hackers.

CLIMATAINE

Officier en cyberguerre climatique.

Le climataine :

* ***Surveille*** les systèmes liés au climat,
* ***Évalue*** les signaux d'alerte précoce et ***détecte*** les phénomènes manipulés artificiellement.
* ***Liste*** les possibilités de commander les nuages.
* ***Évalue*** les dégâts pouvant être causés par l'assèchement d'une région ou le déclenchement d'ouragans.
* ***Envisage*** des solutions pour limiter les dégâts.

COMPÉTENCES

Connaissances de tous les phénomènes météo.
Expert en sciences naturelles appliquées, statistiques et modélisation.
Stratège sachant anticiper les phénomènes.

QUAND ?

Les projets pour déclencher la pluie sont nombreux. Le dernier est un drone. On envoie un engin dans un nuage et on déclenche des décharges électriques qui forment des gouttelettes d'eau. La technologie étant au point, la guerre climatique va vite être déclarée.

EMPRISONNIEN

Spécialiste de la prise d'otage de cerveaux humains.

L'emprisonnien :

* ***Identifie*** les preneurs d'otage du cerveau.
* ***Repère*** les dégâts effectués par la prise de contrôle.
* ***Élimine*** l'influenceur de pensée.
* Si possible, ***installe*** un cerveau de remplacement.

COMPÉTENCES

As des cybertechnologies, expert en sciences de la vie et du cerveau.
Dispose aussi de compétences pharmaceutiques pouvant réguler les flux cérébraux.

QUAND ?

Elon Musk a annoncé que Neuralink travaille sur une puce implantable dans le cerveau. Cet implant de la taille d'une pièce de monnaie fonctionnerait grâce à la technologie Bluetooth. Il devrait redonner la parole et la mobilité aux personnes paralysées. Nombreux autres travaux plus sérieux vont dans ce sens. On aura donc bientôt besoin d'emprisonnien pour éviter que notre cerveau soit pris en otage.

ONIRISTE

Analyste spécialiste du tri des souvenirs.

Lorsque les mémoires numériques d'un patient ont été piratées, l'oniriste :

* ***Utilise*** des intelligences artificielles pour évaluer la probabilité de vrai de chaque souvenir numérique.
* ***Aide*** le patient à se souvenir des événements non numérisés.
* ***Soigne*** les dégâts causés par le trouble entre le vrai et le faux.
* ***Met en œuvre*** des protocoles combinant neurosciences et médecine légale.

COMPÉTENCES

Thérapeute spécialisé dans les traumatismes numériques.
Spécialiste des impacts des technologies (réalité virtuelle, ubiquité quantique…) sur la mécanique cérébrale.
Familier des diagnostics cérébraux.
Maîtrise d'un portefeuille de technologies d'ingénierie mentale.

QUAND ?

Nous faisons tous de plus en plus confiance à nos mémoires numériques. Comme le risque de piratage grandit, il faut que, dès maintenant, des thérapeutes se forment à ce nouveau traumatisme.

PERSODATISTE

Spécialiste de l'intégrité des données personnelles.

Le persodatiste :

* ***Protège*** les données personnelles d'un individu.
* ***Surveille*** le trafic et les violations de données.
* ***Aide*** à récupérer ses données personnelles et ***gère*** les processus de dédommagement.
* ***Améliore*** la sécurité des bases de données personnelles.

COMPÉTENCES

Spécialiste de la bonne gestion de la data.
Compréhension des vrais besoins des clients.
Capacité à évaluer les conséquences des usages frauduleux de données individuelles.

QUAND ?

Même si officiellement nous sommes propriétaires de nos données personnelles, nous n'avons aucun moyen de les protéger et de les utiliser pour améliorer notre vie.
Un persodatiste va donc offrir un service à la personne dont le besoin est important.

SÉCUROTHICIEN

Garant de l'intégrité des génomes humains.

Le sécurothicien :

* ***Surveille*** les systèmes biologiques et ***détecte*** les anomalies et les changements.
* ***Envisage*** des mesures de protection des génomes humains.
* ***Évalue*** les conséquences des modifications de gènes.
* ***Sensibilise*** aux abus de bricolages génétiques.

COMPÉTENCES

Spécialiste des sciences de la vie combinées à la chirurgie et à des soins de santé à vocation militaire
Sait tirer tire profit du génie génétique en évaluant en permanence les effets avant et après les opérations.
Maîtrise des performances du couteau génétique CrisprCas9.

QUAND ?

Des dizaines de milliers d'Estoniens ont volontairement donné leur ADN. Il est numérisé, séquencé et stocké. 23andMe et MyHeritage proposent à leurs clients de déterminer leur origine. Les banques britanniques, américaines et islandaises collectent l'ADN pour améliorer la recherche sur les maladies rares. Quand il y a numérisation, le piratage est toujours envisageable.

De l'anticipation à l'action

Morris et Kiron envisagent les compétences à acquérir pour relever les futurs défis de la cybersécurité.

Sur l'écran d'Andrea, une citation d'Einstein s'affiche : « Les machines pourront résoudre tous les problèmes, mais jamais aucune d'elle ne pourra en poser un ». Ce mépris pour la gent machinale me coince les automatismes. Et la machine dans tout cela ? Quel rôle jouons-nous dans l'affaire ? Je ne comprends plus le sens de mon travail.

Kiron, Morris, j'ai besoin de dix recommandations sur les compétences à acquérir pour relever les futurs défis de la cybersécurité.

Dix ! Pourquoi est-ce que les humains exigent toujours des séries de dix ?

C'est à cause de leurs dix doigts aux mains et aux pieds.

Morris, tu n'as pas un hacker qui peut modifier le génome pour fabriquer des humains à trois doigts.

Oh, les IA, c'est sérieux.

Andrea, nous sommes des machines assez sérieuses pour ne pas nous prendre au sérieux.

Andrea n'étant pas d'humeur à plaisanter, il efface ma dernière remarque. Morris profite du blanc pour prendre la parole.

Machines, objets, humains, animaux, plantes… Au fil du temps, le monde sera de plus en plus connecté, donc vulnérable.

Affirmatif. La taille du réseau est un handicap. Plus un réseau est grand, plus le dysfonctionnement risque d'être important.

Pourquoi ? Normalement, plus on est grand, plus on est fort.

Imagine que l'eau vient à manquer. Si ton animal de compagnie est un éléphant, cela va poser un gros problème. En revanche, si tu élèves des fourmis, tu trouveras toujours des solutions.

Du fait des interactions, les failles seront de plus en plus nombreuses et importantes. Les bugs viendront de quelques humains, mais aussi des machines.

Première piste : disposer de spécialistes qui abordent la cybersécurité de manière systémique et ne se contentent pas de sécuriser chaque réseau.

IA consciencieuse, je prends le relais.

Deuxième piste : former des ingénieurs qui créent des systèmes résilients qui deviennent plus résistants après chaque piratage. La vulnérabilité des réseaux doit être pensée comme une force.

> Kiron, tu ne serais pas en train de vapoter une étude d'un consultant ? Ça sent l'enfumage !

En guise de réponse, je précise que la résilience est un concept d'origine physique. Elle se définit par la capacité d'un système vivant à retrouver les structures et les fonctions de son état de référence après une perturbation. Un système résilient est donc capable d'encaisser les coups et de rebondir.

Mettre en place une stratégie de résilience, c'est accepter la catastrophe comme inéluctable.

C'est une approche collaborative. Toutes les idées imaginées pour bloquer une faille et éviter un désastre sont capitalisées et partagées. Elles servent à créer des dispositifs encore plus performants.

Il faut envisager que, avec la complexité résultant des interactions entre les réseaux, il ne pourra plus avoir de système informatique stable et totalement protégé.

C'est un changement de manière de penser. Demain, on ne pourra plus combler une faille d'un réseau pour revenir à la normalité. Il faudra réinventer en permanence une stabilité provisoire.

Les ingénieurs devront être des cerveaux agiles qui conçoivent des systèmes plus forts que le maillon le plus faible.

Troisième piste : créer une organisation assez agile pour réinventer en permanence des systèmes provisoirement stables.

La stabilité provisoire passera par des cou-

pures du réseau en microréseaux. Les anticiper évitera des bricolages dans l'urgence. On conservera des ponts numériques qui, en cas de crash, feront passer les informations essentielles.

Quatrième piste : disposer de spécialistes qui, lors des attaques, proposent une organisation qui jongle entre Internet, Intranet, Localnet et échanges papiers.

La cybersécurité ne doit pas être confiée aux seuls techniciens. Il faut par exemple des sociologues ou philosophes pour penser autrement les systèmes, des spécialistes des ressources humaines pour négocier des rançons, des thérapeutes pour soigner les angoisses causées par les piratages, des communicants pour faire passer les bons messages…

Il faut recruter des filles pour créer du désordre dans un monde bien masculin de l'informatique et éviter les raisonnements linéaires. La théorie du chaos élaborée en thermodynamique des fluides stipule que : « Un désordre fait naître un ordre de qualité supérieure. » On aura donc besoin de désordre pour élaborer de nouvelles solutions.

Cinquième piste : multiplier les talents en diversifiant les profils des cybersécuristes.

Des campagnes de sensibilisation aideront à faire comprendre que le réseau Internet est fragile. Il peut s'écrouler à tout moment si on ne le protège pas.

Tu as raison Morris. La protection doit être l'affaire de tous et non pas uniquement celle des professionnels.

Sixième piste : Investir dans des campagnes de sensibilisation à la protection collective du réseau Internet.

Il est aussi nécessaire d'apprendre à imaginer l'imprévisible.

Lorsque Darwin évoque la « sélection naturelle », il considère que dans tous systèmes, ceux qui sont le plus capables de s'adapter au changement s'en sortent le mieux. Il faut reprendre ce

principe pour envisager la cybersécurité.

Septième piste : Prévoir les conséquences de l'imprévisible.

Après une minute de silence, Andrea commence à remuer. Encore une différence entre les machines et les humains. Les bipèdes n'ont aucune patience.

Huit ?... Les IA, qu'est-ce qu'il passe ? J'attends la suite. J'ai demandé dix remarques.

Morris m'envoie une ligne de code qui dit : « Bon, on ne va pas faire tout le boulot des humains. À eux de continuer. » Je fais un clic d'œil à mon collègue et me débranche.

HACKERS OUVERTS

Je suis Kiron, une machine de la marque « Intelligence artificielle ». Je suis nourrie aux données de l'armée et des agences gouvernementales. Ma mission du jour est d'aider l'humain Andrea à dessiner les compétences des futurs métiers de la cybercriminalité.

Croyant à la permIAculture, Andrea m'a obligé à travailler avec Morris. Cette machine mouline à partir des informations fournies par les hackers.

Nous sommes aidés par les travaux effectués sur le sujet au cours des quatre ateliers organisés par armasuisse en mai 2021. Comme la quarantaine d'humains présents disposaient de super pouvoirs, ils se sont propulsés dans le futur pour dessiner ces métiers.

Demain, des *rangociateurs* négocieront les rançons demandées par les hackers pour de décryptage des données. Des *canaristes* trouveront des systèmes d'alerte similaires à celui du canari détecteur de grisou dans la mine. Des *cybernudgiens* inciteront en douceur à avoir des comportements plus sécurisés. Des *lowteckistes* envisageront des solutions non numériques pour continuer à vivre quand le réseau est en panne. Des *sécurothiciens* garantiront l'intégrité du patrimoine génétique des humains. Les *emprisonniens* les protégeront contre la prise en otage de leur cerveau…

Graphisme : Studio Miamiam – Première édition : octobre 2021 – Paris

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Sciences et technologies

IABG

Les Propulseurs

9 783952 517574