# OPEN HACKERS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

# OPEN HACKERS

ISBN: 978-3-9525175-6-7

Bundesamt für Rüstung armasuisse
Wissenschaft und Technologie
Forschungsmanagement und Operations Research
Feuerwerkerstrasse 39
CH-3602 Thun

Kontakt:
Dr. Quentin Ladetto
Technologiefrüherkennung
+41 58 468 28 09
quentin.ladetto@armasuisse.ch

www.sicherheitsforschung.ch
www.deftech.ch

Redaktion: Anne-Caroline Paucot
Kreatives Team: Studio Miamiam
Grafik : Pierre Hugot & Ludivine Koegler

Adaption FR>DE von Versions Originales Sàrl, Neuchâtel
(CH) und Dr. Pascal van Overloop (IABG)

# OPEN HACKERS

Anne-Caroline Paucot
Quentin Ladetto

Les Propulseurs

# Zukunftsorientierte AKTION, um die Kompetenzen der Zukunft zu entwerfen

*« Open Hackers » ist eine Zukunftsfiktion, die knapp zwanzig zukünftige Berufe aus dem Feld der Cybersicherheit vorstellt. Diese Berufe wurden während Workshops entworfen, die armasuisse im Mai 2021 organisiert hat.*

Dieses Dokument ist das Ergebnis eines zukunftsorientierten Workshops zum Thema Cybersicherheit.

Das zukunftsorientierte Workshop-Format katapultierte die Teilnehmende in eine mehr oder weniger weit entfernte Zukunft, um sich neue Handels- und Denkweisen auszumalen. Die Teilnehmenden sollten nicht die Zukunft voraussagen, sondern mehrere Szenarien davon in Betracht ziehen, um sich auf diese vorzubereiten.

Dabei bestand das Ziel darin, sich die zukünftigen Berufe der Cybersicherheit auszudenken, um notwendige persönliche Kompetenzen für deren Ausübung zu identifizieren. Nach dem Abwägen der möglichen kurz- und langfristigen Auswirkungen der Technologien haben wir die notwendigen Fähigkeiten aufgelistet, um ihren Nutzen zu verstärken und uns vor ihren Nachteilen zu schützen.

Bei Zukunftsfiktionen besteht die Schwierigkeit darin, mit Themen zu arbeiten, die es überhaupt noch nicht gibt. Wenn man dazu einlädt, Zukunftsszenarien zu entwerfen, ist das Resultat oft «fast schon existent» und «mit aktuellem Zeitgeist eingefärbt». Um diesen Fehler zu umgehen, haben wir eine Methodologie ausprobiert, die sich auf drei Grundsätze stützt:

Der ***erste*** Grundsatz besteht darin, davon auszugehen, dass die Berufe von morgen aus der Vereinigung von drei Elementen entstehen: Technologien und neue Anwendungen, Herausforderungen, Innovation und Forschung.

Der ***zweite*** Grundsatz besteht darin, vom Bestehenden auszugehen, um langsam, aber sicher in der Zukunft anzukommen.

Der ***dritte*** Grundsatz besteht darin, mit Workshops die kollektive Vorstellungskraft zu nutzen.

Während der vier Workshops auf Deutsch und Französisch sind wir schrittweise vorgegangen:

### *1. Schritt: Sensibilisierung und Selektion*

Nach einer Präsentation durch Fachleute erhalten die Teilnehmenden Karten, auf denen aktuelle Cyberangriffe erläutert werden. Sie machen sich damit vertraut und wählen einen Angriff aus. Dann überlegen sie sich dessen kurz-, mittel- und langfristigen Folgen.

### *2. Schritt: Verknüpfung*

Technologien werden vorgeschlagen. Die Gruppen malen sich ausgefeiltere Cyberangriffe aus. Langsam entfernen wir uns vom Heute.

### *3. Schritt: Abflug*

Die Teilnehmenden wählen aus einer Liste eine «Superkraft» aus. Mit diesem spielerischen Element können sie die Konsistenz von Stoffen oder die Grösse von Pflanzen ändern, Regen und Schönwetter befehlen, Menschen zum Fliegen bringen oder Gedanken lesen ...

Mit dieser Inspiration brechen Sie aus dem Alltag aus und stellen sich offener die Bedrohungen der Zukunft vor.

Nach den ersten beiden Runden, streichen einen auf Französisch und einen auf Deutsch, hatten wir ein Dutzend neuartige Hackerangriffe gesammelt.

Während des zweiten Workshops wählten die Teilnehmenden einen davon aus der Liste aus.

**Technologien und neue Anwendungen**

Quanteninformatik, Blockchain, synthetische Biologie, Robotik, künstliche Intelligenz usw. – jede Technologie wird zu neuen Berufen führen. Und noch mehr werden entstehen, wenn man sie kombiniert.

**Herausforderungen**

Erfolgreiche Bewältigung des ökologischen und energetischen Wandels, der Ernährung der Menschheit, des Sicherstellens ihres Schutzes usw. – es gibt unzählige Herausforderungen. Sie werden das Handeln von zahlreichen Unternehmen bestimmen.

**Innovation und Forschung**

Dies sind die Bausteine, mit denen die Zukunft aufgebaut wird. Gemeinsam werden sie zu verschiedenen Zukunftsmöglichkeiten führen.

Sie dachten sich Lösungen aus, um die Angriffe einerseits abzuwehren und andererseits den Schaden zu begrenzen. Da dabei der Bedarf an neuen Kompetenzen auftauchte, haben sie neue Berufe in Betracht gezogen.

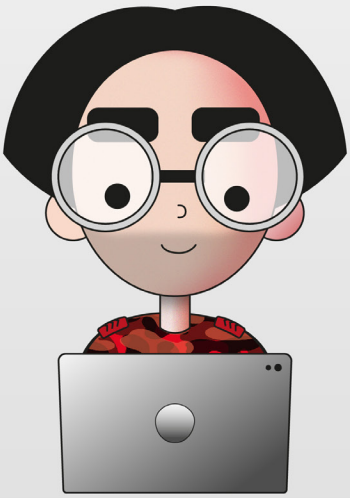
In Anbetracht dieses intensiven Austauschs haben wir uns entschieden, die Arbeit in Form einer Erzählung wiederzugeben. Die Inszenierung der Ideen ermöglichte uns, die Diskussion während eines dritten Workshops fortzusetzen.

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

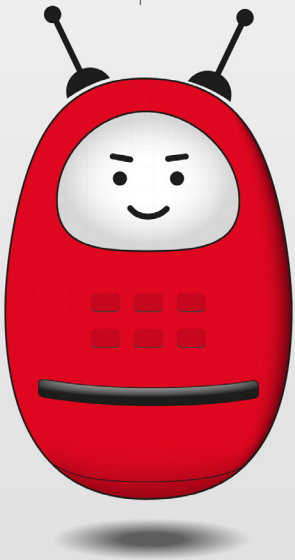
Mit der Beteiligung von

*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*

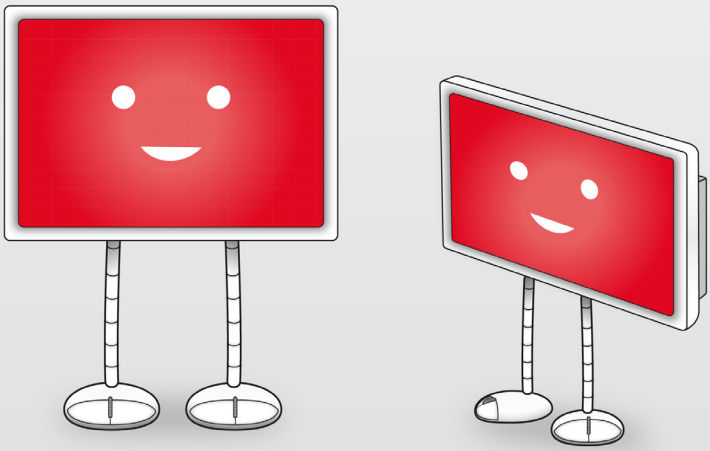
Andrea



Maurice



Kiron



## ZUKUNFTSORIENTIERTE AKTION, UM DIE KOMPETENZEN DER ZUKUNFT ZU ENTWERFEN

«Open Hackers» ist eine Zukunftsfiktion, die knapp zwanzig zukünftige Berufe aus dem Feld der Cybersicherheit vorstellt. Diese Berufe wurden während Workshops entworfen, die armasuisse im Mai 2021 organisiert hat.


15 - ***Neue Kriege***

Grössere Verletzlichkeit der mächtigen Länder, Unmöglichkeit für eine Regierung, im Alleingang zu handeln, Schwierigkeit, den Angreifer zu identifizieren ... Der Cyberkrieg definiert den Krieg neu.

19 Die zukünftigen Strategieberufe

19 Antizipaktor/in

Eine Person, die futuristische Konzepte in Aktionen verwandelt.

19 CyberKrieger/in

Eine Person, die die Eigenarten des Cyberkriegs aufzeigt.

19 Resilienator/in

Gestalter/in von resilienten digitalen Netzwerken.

21 - ***Kanarienvögel des bergbaus***

Die beiden künstlichen Intelligenzen machen einen Sprung in die Zukunft, um die Berufe zu beäugen, die Cyberangriffe vorbeugen und erkennen werden.

26 Berufe, die Alarmzeichen erkennen

26 Kanarist/in

Ingenieur/in für präventive Alarmsysteme.

26 Detacker/in

Aufspürer/in von Schwächen in den IT-Systemen.

26 Hackarion/in

Spion/in der Hacker.

27 Identikator/in

Entwickler/in von Systemen für die Identifikation von Cyberkriminellen.

29 - ***Lösegeldforderungen***

Die Angriffe werden genauer. Es gilt, den Schaden zu begrenzen. Es wird mit Lösungen jongliert und Lösegelder ausgehandelt.

34 Berufe, die für die Cybersicherheit sensibilisieren

34 Cybernudger/in

Nudge-Fachperson für die Aneignung von sicheren Verhaltensweisen.

35 - ***Die grosse Panne***

Die KI machen Druck: Eine Codezeile, die das Satellitennavigationssystem stört, kann eine weltweite Katastrophe auslösen.

40 Berufe, um die Auswirkungen der Angriffe einzugrenzen

40 UnterBrecher/in
Schöpfer/in von vergänglichen Gemeinschaften, um Ausfälle zu überleben

49 Epinumerist/in
Digitale Epidemiologen/innen

40 Lowtechist/in
Fachperson für analoge Lösungen.

41 Ransomist/in
Vermittler/in von Lösegeldern für die Entschlüsselung von Daten.

43 - ***Der manipulierte Mensch***
Implantate, digitale Tattoos oder vernetzte Zähne – wenn der Mensch ständig an das Netz angebunden ist, können Hacker seine Gedanken, sein Gedächtnis oder sein Erbgut manipulieren.

47 Hackerberufe

47 PR-Hacker

49 - ***Wettermacher***
Was wären die Hacks von morgen, wenn die Menschen über Superkräfte verfügen würden? Die KI schweifen ab, um diese Unberechenbarkeit zu antizipieren.

53 Berufe des Cyberangriffs der fernen Zukunft

53 BlockCloner/in
Kontrolleur/in der psychologischen Integrität der Klone.

53 Chirurgident/in
Identitätschirurg/in

53 KlimaTINIST/In
Offizier des Cyberklimakriegs.

53 CyberNeurolog/in
Fachperson für die Geiselnahme des menschlichen Gehirns.

54 Souvenirist/in
Analyst/in mit Spezialisierung auf die Sortierung von Erinnerungen.

54 Persodatist/in
Fachperson für die Integrität der Personendaten.

54 Securogenist/in
Garant/in der Integrität des menschlichen Erbguts.

55 - ***Von der antizipation zur Handlung***
Morris und Kiron überlegen sich die zu erwerbenden Kompetenzen, die für die Meisterung der zukünftigen Herausforderungen der Cybersicherheit notwendig sind.

## *Neuer Krieg*

**Grössere Verletzlichkeit der mächtigen Länder, Unmöglichkeit für eine Regierung, im Alleingang zu handeln, Schwierigkeit, den Angreifer zu identifizieren ...**

**Der Cyberkrieg definiert den Krieg neu.**


Kiron, welches sind die zukünftigen Berufe im Bereich der Cyberkriminalität?

Ich bin Kiron, eine «künstliche Intelligenz». Ich arbeite für Andrea, einen Menschen der Kategorie «Grossgewachsen». Er ist 1,982 m gross und Zukunftsdesigner der Streitkräfte. Ich bin seine Schreiberin und sein Hirn. Wenn er ein Problem hat, nutze ich mein digitales Genie, um es zu lösen.


Kiron, wir haben ein gravierendes Problem: digitale Sturmangriffe, gestohlene Daten, erpresste Unternehmen … Täglich gibt es auf der ganzen Welt fast 200 000 Cyberangriffe! Diese Zahlen steigen ständig weiter an. Wir brauchen neue Berufe!

Als gute Maschine prüfe ich die Zahlen. Ich stelle fest, dass die Zahl der kriminellen Angriffe 2020/21 explodiert ist. Die Experten schlagen Alarm. Weil die Code-Zeilen der Computerprogramme von einigen Dutzend auf zehntausende angestiegen sind, wird es immer schwieriger, die Eindringlinge zurückzuverfolgen.


Zukünftige Berufe der Cyberkriminalität! Meine Datenbank ist leer.


Kiron, streng dich an, es ist wichtig! Wenn man die zukünftigen Berufe nicht kennt, kann man die notwendigen Kompetenzen für ihre Ausübung nicht definieren.


Die erweiterte Suche ist erfolglos. Die Datenbank «noch nicht existierende Berufe» ist leer.


Ich weiss nicht. Denk dir die Berufe aus.

Ich ventiliere, um meine Unfähigkeit zum Ausdruck zu bringen. Eine künstliche Intelligenz kann zwar Daten sortieren und Hochrechnungen durchführen aber sich nichts aus den Fingern saugen.


Ok, wenn du mir nicht helfen kannst, dann frage ich Morris.

Ich piepse, um meine Missbilligung zum Ausdruck zu bringen. Andrea ist ein Anhänger der PermaK(I)ultur oder, wie sie auch genannt wird, der Mischung Künstlicher Intelligenzen. Morris ist ebenfalls eine Künstliche Intelligenz. Anders als ich, die ich mit Daten von Regierungsbehörden und den Streitkräften gefüttert werde, wird Morris mit Infos von Hackern vollgestopft.

Morris wird mit dem Austausch Andrea–Kiron verbunden. Problem verstanden. Um die zukünftigen Berufe der Cybersicherheit zu betrachten, müssen die Merkmale des Cyberkriegs jenen des herkömmlichen Kriegs gegenübergestellt werden.

Diese Spur lässt meine Prozessoren warmlaufen. In meinen Datenbanken gibt es 1 054 358 Seiten zu diesem Thema. Ich wähle die Zusammenfassung einer Schweizer *Cyberistin* und spucke sie aus.

Erster Punkt. Je mächtiger ein Land in einem klassischen Krieg ist, umso ausgeklügelter sind seine Waffen und umso grösser ist seine Kampfkraft.

Logo! Die Militärmacht der USA, Chinas und Russlands ist grösser als jene der Schweiz oder von Polen.

*Je mächtiger ein Land ist, umso verletzlicher ist es.*

Je mächtiger ein Land ist, umso vernetzter ist es und umso zahlreicher sind die Möglichkeiten für das Eindringen in seine Systeme. Deshalb gilt: Je mächtiger ein Land ist, umso verletzlicher ist es.

Morris, du meinst damit, dass ein Land umso mehr Angriffsfläche bietet, je reicher es ist?

Genau! Die Angriffsfläche wird grösser, weil sich Milliarden von ungeschützten vernetzten Gegenständen dem Reigen anschliessen. Ehrlich gesagt lieben meine Hacker das menschliche Genie. Wenn der Mensch sich langweilt, erfindet er alles Mögliche. Er erfindet das Aquarium, um Fische aus dem Trockenen zu beobachten, den Schlauch für das wetterabhängige Wässern der Pflanzen, das Babyphone, damit die Eltern auch während des Besuchs bei den Nachbarn hören, wenn das Baby weint … Diese Gadgets sind ein gefundenes Fressen für die Hacker. In den meisten Fällen sind die Benutzer so fasziniert von der Technologie, dass sie sogar vergessen, das Standardpasswort zu ändern.

Dies ist kein Grund, diese Dispositive zu hacken! Das ist kriminell!

Kiron ! Spielen wir uns jetzt als Verfechterin der Gerechtigkeit auf?

Auch brillante Menschen geraten manchmal auf Abwege und machen dumme Bemerkungen. Aber Andrea weiss, dass ich als Maschine kein Gewissen habe. Wenn du mich in ein selbstfahrendes Auto oder

in eine Drohne setzt, kann ich einen Hund, ein Kind oder einen alten Mann töten, ohne mit der Wimper zu zucken.

Zweiter Punkt. Eine Regierung kann einen Cyberangriff nicht im Alleingang abwehren. Wenn ein Land aus der Luft oder an Land angegriffen wird, schickt es seine Streitkräfte zur Abwehr. Wenn die Gefahr aus dem Innern kommt, wird die Polizei eingesetzt. Die Abwehr von Cyberangriffen ist aber eine ganz andere Sache. 80 % der potenziell betroffenen Infrastrukturen sind privat. Die Bedrohungen können das Internet, finanzielle Netzwerke, Wasser- oder Stromnetze betreffen, die nicht dem Staat gehören. Die Regierung kann ihnen folglich nicht im Alleingang gegenübertreten.

*Eine Regierung kann einen **Cyberangriff** nicht im Alleingang abwehren.*

Dritter Punkt. Eine Bombardierung oder die Ankunft von Panzern in einer Stadt bleiben nicht unbemerkt. In einem Cyberkrieg weiss man oft nicht, dass man angegriffen wurde. Dies kann passieren und man bemerkt es erst Monate oder Jahre später.

*Man kann Opfer eines **Cyberangriffs** sein, ohne es zu wissen.*

Das stimmt. Wenn man einen Virus einschleust, braucht es Zeit, bis er von einem Computer zum nächsten übergeht. Er kann folglich Wochen oder Monate nach dem Einschleusen aktiv werden.

Man spricht vom Computervirus, weil er sich wie ein biologisches Virus ausbreitet.

Genau! Er nutzt die Reproduktionsfähigkeit seiner Wirtszelle.

Das letzte Merkmal des Cyberkriegs ist, dass man den Angriff nicht kommen sieht. Wenn sich einem Land Truppen nähern oder Luftangriffe vorbereitet werden, identifizieren die betroffenen Länder die Angreifer und kennen deren Gründe. Im Cyberkrieg ist dies nicht der Fall. Es ist ein Überraschungsschlag. Man fragt sich, ob der Angriff von einem Typen der Bande von Morris kommt, der in seinem Loch Hamburger in sich reinstopft, oder von einer Regierung. Ist es ein einzelner Hacker oder ein Staat, der dahinter steckt?

*Bei **Cyberangriffen** ist es schwierig, den **Angreifer** zu erkennen.*

Richtig! Die Hacker schreien es nicht von allen Dächern, wenn sie einen Angriff planen. Sie greifen an. Die Menschen müssen selber bestmöglich reagieren.

# DIE ZUKÜNFTIGEN STRATEGIEBERUFE

## ANTIZIPAKTOR/IN

**Eine Person, die futuristische Konzepte in Aktionen verwandelt.**

Der/die Antizipaktor/in :

* ***analysiert*** die Trends;
* ***zieht*** die mittel- und langfristigen Wirkungen der Aktionen in Erwägung;
* ***überwacht*** die Systeme und antizipiert ihre Störungen;
* ***findet*** Lösungen für zukünftige Probleme;
* ***ersinnt*** Alternativen für die Sicherstellung der ununterbrochenen Weiterführung der Operationen.

### KOMPETENZEN

Stützt sich auf die Gegenwart, um sich in die Zukunft zu projizieren.
Gestaltet sowohl solide als auch entwicklungsfähige Methodologien, damit möglichst viele handeln können.

### WANN?

Die Zukunft hat begonnen und das Coronavirus zeigt, dass nichts vorhersehbar ist. Alle Lebewesen benötigen deshalb Antizipaktoren.

## CYBERKRIEGER/IN

**Person, die die Eigenarten des Cyberkriegs aufzeigt.**

Der/die Cyberkrieger/in :

* ***verfolgt*** die Entwicklung der verschiedenen Kriegsarten;
* ***findet*** die Unterschiede und Gemeinsamkeiten;
* ***passt*** die Trümpfe einer Kriegsart an andere Kriege an.

### KOMPETENZEN

Als Konfliktforscher/innen studieren sie alle Kriege und kennen alle ihre Ursachen.
Als Internetstrateg/innen haben sie die Übersicht über die Funktionsweise der Netze und erkennen ihre Störungen.
Sie können die verschiedenen Sektoren verbinden.

### WANN?

Es gibt bereits zahlreiche Fachpersonen, die diese Aufgaben erledigen. Der Beruf als solcher wurde aber noch nicht erfunden.

## RESILIENATOR/IN

**Gestalter:in von resilienten digitalen Netzwerken.**

Der/die Resilienator/in :

* ***analysiert*** die Anfälligkeit der Informatiksysteme;
* ***identifiziert*** mögliche Traumata;
* ***erwägt*** Systeme, die den Schock nicht nur bewältigen, sondern sich davon inspirieren.

### KOMPETENZEN

Kenntnis der Grundsätze der komplexen und resilienten Systeme.
Fachperson für Netzwerkdynamik.

### WANN?

Eine resiliente IT-Infrastruktur kann Kosten aufgrund von Pannen und der Wiederaufnahme der Tätigkeit verhindern. Folglich sind Resilienator:innen dringend notwendig.

# *Kanarienvögel des BERGBAUS*

**Die beiden künstlichen Intelligenzen machen einen Sprung in die Zukunft, um die Berufe zu beäugen, die Cyberangriffe vorbeugen und erkennen werden.**

 Los KI, an die Arbeit! Während ihr die Zusammenfassung der vier Workshops über die zukünftigen Berufe der Cybersicherheit verdaut, hole ich mir einen Kaffee.

Andrea steht auf und verlässt sein Büro. Ich nutze die Gelegenheit, um meinen Kollegen auszufragen.

Morris, warum heisst du so?

Wegen Robert Tappan Morris.

Ich scanne meine Datenbank. Robert Tappan Morris ist der Autor des ersten Cyberangriffs. Ende der 80er-Jahre arbeitete das CERN daran, die grössten IT-Systeme mit einer gemeinsamen Sprache zu verbinden. Nachdem es von den Forschern geprüft wurde, breitete sich dieses Dispositiv in den USA aus. Morris bastelte ein Computerprogramm, um in Erfahrung zu bringen, wie viele Maschinen mit diesem Netz verbunden sind. Zu seinem Pech schlich sich ein Designfehler ein. Sein Wurm vervielfältigte sich auf anarchische Weise und blockierte Millionen Computer.

*Tech ohne Gehirn bedeutet den **Untergang** des Menschen.*

Ich hoffe, dass Robert Tappan Morris nicht dein Vorbild ist, Morris! Die Schäden, die durch sein Versagen verursacht wurden, werden auf 10 Millionen Dollar geschätzt!

In der Cyberwelt ist es manchmal schwierig, die Folgen der eigenen Handlungen zu messen. «Wissenschaft ohne Gewissen bedeutet den Untergang der Seele», schrieb Rabelais. Mein Prozessor sagt dazu nur, dass «Tech ohne Gehirn den Untergang des Menschen bedeutet».

Ich verstehe. Du denkst, dass Hacker alles dürfen.

Nein, ich glaube nur, dass die Hacker oft Grenzen überschreiten müssen, um gehört zu werden. Sie müssen eine Bedrohung aufzeigen, damit die Systemverantwortlichen bereit sind, nach einer Lösung zu suchen.

Um seine Worte zu unterstreichen, sendet Morris die Geschichte von Jack Barnaby in mein Verarbeitungszentrum. 2010 war er der erste, der einen Geldautomaten hackte. Während einer Konferenz über die IT-Sicherheit zeigte er, wie einfach die wertvollen Scheine entnommen werden können. Er ist so weit

gegangen, weil ihn die Banken nicht ernst nahmen. Sie behaupteten, dass ihre Bankomaten sicher seien und wollten nichts mehr ändern. Die Geschichte wiederholte sich mehrmals mit Internetboxen oder vernetzten Gegenständen.
Einstein sagte: Der Mensch vermeidet es normalerweise, anderen Intelligenz zuzusprechen, ausser es handelt sich per Zufall um einen Gegner. Wenn die Banker merken, dass ein Typ ihre Automaten leert, wird er zum Feind und sie beginnen, sich dafür zu interessieren, was er sagt.


Hey KI, fertig gequatscht! Wir sind hier, um die zukünftigen Berufe der Cyberkriminalität zu finden.


Der erste Beruf der Zukunft ist der «Hacker».

Ich krümme mich vor Lachen, bevor ich ihm zustimme.


Für mich gehört der Hacker in die gleiche Schublade wie Diebe, Banditen und Einbrecher. Wenn Hacker ein Beruf ist, müssen zuerst alle Formen der Kriminalität professionalisiert werden.


Ich weiss, Kiron. Dies ist für eine Beamten-KI nur schwer zu begreifen.

Als mein Kollege das sagt, fangen meine Mühlen an, schneller zu mahlen.


Morris, erzähl mehr.


Ein Grossteil der Arbeit der Hacker besteht darin, die Fehler im System zu finden und die Betreiber dazu zu bringen, eine Lösung dafür zu finden. Morgen werden sich Fachkräfte darum kümmern müssen.


Das ist eine interessante Idee.


Die Hacker sind es auch, die prüfen, ob eine Maschine ihre Arbeit richtig macht. Wenn aus einer Kaffeemaschine Whisky läuft, stimmt etwas nicht. Das gleiche gilt, wenn ein Router Eindringlingen als Zugang dient.


Morris, über welche Kompetenzen müsste dein Hacker verfügen, wenn er zu einem richtigen Beruf wird?

Durchhaltevermögen. Der Teufel liegt im Detail. Dies gilt ganz besonders für IT-Systeme. Eine Code-Zeile kann einige Monate später am anderen Ende der Welt eine Katastrophe auslösen. Schlimmer als der Flügelschlag eines Schmetterlings, der einen Tornado auslöst. Der Berufshacker muss sich in alle Systeme einschleichen und die verstecktesten Winkel erkunden können. Er muss zudem lernen, zusammenzuarbeiten und die Information mit seinen Kollegen zu teilen. Cyberangriffe sind heute komplex und mit den Wechselwirkungen werden sie morgen nicht weniger sein. Die neuen Probleme müssen gemeinsam gelöst werden, ohne Zeit und Energie mit dem Aufgreifen der alten Probleme zu verschwenden.

Ich finde diese Idee interessant, aber wir brauchen einen anderen Namen für diesen Beruf. Camus sagte: «Wer die Dinge beim falschen Namen nennt, der trägt zum Unglück der Welt bei.» Hacker wäre der falsche Name für solch einen delikaten Beruf.

*Detacker/in* : Die Hacker spüren einen Fehler auf und handeln, um ihn zu beheben.

Detacker/in, Hacker sind mit viel Herzblut an der Sache.

Nicht schlecht, KI. Ein anderer Beruf, Kiron?

Effizienz ist mein zweiter Name, deshalb schüttle ich die Bits. Mein maschinelles Lernen integriert das aktuelle Gespräch und sucht in einer bis jetzt nicht zugänglichen Datenbank nach einem neuen Beruf.

Hackarion.

Der *Hackarion* spioniert die Hacker aus. Er dringt in die Köpfe der Hacker ein, um festzustellen, wer sie sind und was ihre Motivation ist. Handelt es sich um eine Einzelperson, einen Verband oder eine Regierung? Wollen sie zeigen, dass sie die Stärksten sind? Wollen sie ein Land zerrütten, Geld verdienen, Informationen für einen Wettbewerbsvorteil erhalten, die Funktionsweise eines Unternehmens blockieren? Wenn Geld der Grund ist, streben sie eine persönliche Bereicherung an?

Alarm, genau das wollte ich jetzt auch gerade sagen.

Wir erleiden die Angriffe und gehen viel zu sehr davon aus, dass wir sie nicht verhindern können. In Zukunft müssen Identikatoren die Angreifer erkennen, bevor sie angreifen. Sie müssen kreativ sein. Diese Fachleute könnten beispielsweise die mit Datenbanken verbundene Gesichtserkennung verwenden, um Angreifer zu identifizieren, die ein Cyberverbrechen vorbereiten. Die Verschlüsselung verhindert nicht, dass sie gefunden werden. Im Gegenteil, sie macht sie verdächtig.

Alarm ... Pieps ... Pieps ... Der Hack ist bestätigt.

Für die Vorbeugung der Cyberangriffe braucht es auch Kanaristen.

*Kanaristen* ? Besteht da ein Zusammenhang zu Kanarienvögeln oder den Kanaren?

Früher wurden die Vögel verwendet, um vor Gasexplosionen zu warnen. Sie sind hochempfindlich gegen giftige Gase und bemerken sie vor dem Menschen. Wenn sie mit dem Singen aufhörten wurde die Mine evakuiert. Das gleiche Vorgehen wird auch im Weinberg verwendet. Die Winzer pflanzen Rosenstöcke, die viel anfälliger gegen Parasiten sind. Wenn die Rosenstöcke verkümmern, wissen sie, dass sie etwas für die Reben tun müssen. Kanaristen finden ähnliche präventive Alarmsysteme.

Der Kanaristen-Beruf hatte meine Mikroprozessoren passiert. Da kein Zweifel mehr darin besteht, dass ich gehackt worden bin, gehe ich offline, um eine Selbstreinigung durchzuführen.

# BERUFE, DIE ALARMZEICHEN ERKENNEN

## KANARIST/IN

**Ingenieur:in für präventive Alarmsysteme.**

Der/die Kanarist/in :

* als früher der Kanarienvogel in der Mine aufhörte zu singen, lag dies am Grubengas. Kanaristen ***denken*** sich ähnliche Alarme für Eindringlinge aus;
* ***Entwicklung*** und ***fortlaufende*** Umsetzung von Alarmen und aktiven Gegenmassnahmen;
* ***Überwachung*** der Anomalien in komplexen Systemen und ***Einführung*** von gestaffelten Gegenmassnahmen: Schranken, Fallen, Attrappensysteme, Hinterhalte usw.

### KOMPETENZEN

Fähigkeit, die Bräuche des Webs und den Modus Operandi der Hacker zu analysieren.
Ein kreativer Geist, der neue Alarme erdenken kann.

### WANN?

*Canary Tokens* sind ein Hilfsmittel, das aufzeigt, ob man ausspioniert oder angegriffen wird. Es ist Zeit für diese Idee, aber es wäre notwendig, dass die Fachpersonen ihre diesbezüglichen Dienstleistungen vervielfachen.

## DETACKER/IN

**Aufspürer:in von Schwächen in den IT-Systemen.**

Der/die Detacker/in :

* ***beurteilt*** die Systeme, um Eindringen, Manipulationen und die Extraktion von Daten zu verhindern;
* ***informiert*** sich über die Entwicklung der Techniken, die von den Hackern verwendet werden;
* ***leitet*** Verbesserungen ein;
* ***findet*** Lösungen für die Konsolidierung eines Systems und die Antizipation von Angriffen;
* ***beurteilt*** den Umfang des Angriffs.

### KOMPETENZEN

Perfekte Kenntnis der Angriffe und Technologien, die von den Hackern verwendet werden.
Ein kreativer Geist, der neue Lösungen erfinden kann.
Fähigkeit zur Zusammenarbeit und für den Informationsaustausch.

### WANN?

Detacker:innen könnten «White Hat Hacker» sein. Dadurch, dass sie diesen Status erhalten, können sie ihre Arbeit besser strukturieren.

## HACKARION/IN

**Spion:in der Hacker.**

Der/die hackarion/in :

* ***sammelt*** Aufklärungsergebnisse über die Hacker;
* ***zeichnet*** eine Kartographie der Hacker und Technologien;
* ***scannt*** die gegnerischen Systeme ganzheitlich: Verknüpfung von ISR, Informantennetzwerk, Cyber usw ;
* ***verbindet*** Operationen in der Cyber und physischen Welt, um die Zugriffe zu identifizieren;
* ***nimmt*** technologische Entwicklungen vorweg;
* ***beeinflusst*** die Hacker, um sie zu einer Technologie zu leiten.

### KOMPETENZEN

Kompetenter Umgang mit digitalen Spitzentechnologien.
Spricht mehrere Sprachen.
Fähigkeit, gesammelte Daten zu entschlüsseln und analysieren.

### WANN?

Die Geschichte um die leistungsstarke Software Pegasus zeigt, dass alle jeden ausspionieren. Das heisst, dass es bereits unzählige Hackarione gibt. Die Schaffung dieses Berufs würde seine Strukturierung und die bessere Integration in die Unternehmensstrategie ermöglichen.

## IDENTIKATOR/IN

**Entwickler:in von Systemen für die Identifikation von Cyberkriminellen.**

Der/die Identikator/in :

* ***ordnet*** missbräuchliche Anwendungen und Operationen den verschiedenen Akteuren zu: Menschen, technischen Systemen, KI usw.;
* ***kontrolliert*** die Zugänge, verwaltet die Identitäten, überprüft das Personal;
* ***verfolgt*** Kriminelle mit biometrischen Technologien und Identitätsdaten, einschliesslich der aktiven Ermittlungen;
* ***erfindet*** technologische Fallen und Low-Tech-Dispositive für die Erkennung von Cyberkriminellen, bevor sie handeln;
* ***entwickelt*** diese Systeme weiter.

### KOMPETENZEN

Fähigkeit, aus allen verfügbaren Technologien jene zu wählen, die die Hacker verwirren können.
Kenntnis der Sitten und Gebräuche der Hacker.

### WANN?

Die Beseitigung von Hackern ist eine Priorität. Folglich müssen die Studierenden ab heute in der Schule lernen, wie diese Dispositive ausgetüftelt werden.

## *Lösegeldforderungen*

**Die Angriffe werden genauer. Es gilt, den Schaden zu begrenzen. Es wird mit Lösungen jongliert und Lösegelder ausgehandelt.**

 Kiron, hast du dich während deines Check-ups testen lassen?

Andreas Gelächter riecht nach Tütensuppe. Meine Geruchssensoren leuchten tiefrot auf und ich ziehe mir eine Code-Zeile rein.

 Ich bin gegen alle Varianten geimpft. Wie die Menschen niese ich nicht mehr in die Armbeuge, seit ich weiss, dass die englische Variante den Ärmel überwindet. Ich habe nichts zu befürchten.

Ich lege diese Worte auf den Austauschbildschirm, um zu prüfen, dass Morris nicht mehr in mein System eindringt. Gleichzeitig analysiere ich mein Risiko, mit einem Virus infiziert worden zu sein. Es ist nicht unerheblich. Eine Studie zeigt, dass auch Maschinen nicht gegen die menschliche Dummheit geschützt sind, die Entwickler dazu bringt, von der Zuverlässigkeit ihrer Systeme überzeugt zu sein. Diese Sicherheit steigert die Wahrscheinlichkeit, dass wir durch Codierer in Windeln gehackt werden.

 Kiron, du scheinst mir sehr zuversichtlich?

Überprüfung bestätigt. Ich habe die Zugänge blockiert.

 Eine Maschine ist so programmiert, dass sie keine Zweifel hat.

 Kiron, meine medizinische Software sagt, dass man weiter eine Maske tragen und die Hände waschen muss, auch wenn man geimpft ist.

Hier, liebe menschliche Leser, bitte ich um eure Aufmerksamkeit. Wenn eine Maschine Anthropomorphismus zeigt, dann hat sie etwas Wichtiges zu sagen. Dies wird Fuzzylogik genannt. Wir wenden uns deshalb einen Augenblick von unserem chronischen Binarismus ab, um ein Thema mit brandneuen Informationen zu ergänzen.

 Morris, ich wette, dass du zu 99,7 % an einen anderen zukünftigen Beruf der Cybersicherheit denkst?

 Genau. Ich denke da an *Epinumeristen*. Diese digitalen Epidemiologen bringen Lösungen unter einen Hut, um Viren, Würmer und andere IT-Sauereien zu beseitigen. Die Menschen nutzen bei einer Epidemie mehrere Methoden, um sich vor einem Virus zu schützen. Sie lassen sich testen, halten sich an Sperr-

stunden, schliessen Restaurants und Versammlungsorte, tragen einen Mundschutz usw. Um sich vor Computerviren zu schützen, darf man nicht nur auf eine einzige Methode setzen.

Jetzt kann ich mir ein Bit Bewunderung nicht verkneifen. Wenn die Technologie dem Leben von Hackern einen Sinn gibt, heisst das nicht immer, dass sie ihren gesunden Menschenverstand verlieren.

Kiron, ein Hacker hat mir eben gesagt, dass Epinumeristen sich vor bestimmten Hackern in Acht nehmen müssen. Sie können alle Lösungen vorweggnehmen und finden Mittel, um neue Schäden zu verursachen.

Kannst du das genauer erklären?

Wenn eine Lösung das Maskentragen ist, werden sie Nanoviren kreieren, die sich im Faserstoff verstecken. Die Menschen werden nicht wissen, ob die Masken sie schützen oder umbringen.

He, ihr Maschinen, bringt bitte die Menschen nicht auf solch dumme Ideen!

Richtig-falsch — Spitäler — Lösegeld — Tote — Ransom — ware — täler …

Morris, was läuft, bist du abgestürzt?

Ich — Nein — dumme Intelligenz — OP — Chirurgie, tönt Morris weiter.

Andrea verdreht die Augen und legt sein Thun-Majo-Sandwich auf seine Tastatur. Wie Morris komme ich ins Schlingern. Alle KI der Welt sind über die Daten verbunden. Wenn Morris explodiert, werde ich die Auswirkungen spüren.

Cool down, Kiron. Keine Panik. Es sind nur ein paar Hacker, die von Spitälern Lösegeld fordern. Weil es viele sind, kann Morris sie nur schlecht integrieren.

Ich bestätige die Aussage. Covid-19 ist eine grosse Ablenkung für die Codierer. Sie dringen in die Computersysteme der Spitäler ein, verschlüsseln die Daten und verlangen Lösegeld für die Rückgabe der Daten. Das Eindringen ist ein Kinderspiel, weil die medizinischen Geräte selten gesichert sind.

Morris scheint die Bits wieder unter Kontrolle zu haben. Er verlangt einen Eingriff.

Dabei habe ich die Spitäler vorgewarnt. Sie sagen jedes Mal, dass es eine Zeitverschwendung ist, medizinische Handlungen mit Passwörtern zu schützen. Sie haben so schon zu wenig Zeit für ihre Patienten.

Ich verstehe das Problem. Ich durchforste meine Prozessoren, um einen Beruf zu finden, der ihnen hilft, ihre Gewohnheiten zu ändern.

Cybernudger/in

Kiron, erzähl mehr?

*Cybernudger* sind Nudge-Spezialisten, die den Nutzern helfen, ein sicheres persönliches Verhalten anzueignen, wenn sie vernetzte Geräte verwenden.

Da die Rubrik «mehr darüber» blinkt, führe ich aus, dass ein Nudge ein Anreiz ist, um Verhaltensweisen sanft zu ändern. Der bekannteste ist die Fliege im Pissoir des Flughafens Amsterdam. Weil die Reinigungskräfte feststellten, dass die Männer Mühe haben, ihren Urinstrahl gut auszurichten, haben sie eine Fliege in die Mitte des Pissoirs geklebt. Bekanntermassen sind Männer grosse Kinder, die nun mit grösstem Vergnügen auf die Fliege zielen. Die Putzkosten sind in der Folge deutlich gesunken.

Personen, die ihr Passwort regelmässig ändern, müssten belohnt werden.

Den Cybernudgern wird die Arbeit nicht ausgehen. Die Cybersicherheit ist wie Toilettenpapier. Man denkt nur daran, wenn es ein Problem gibt.

Als gebildete künstliche Intelligenz verbietet mir mein Prozessor, triviale menschliche Aussagen zu kommentieren.

Richtig-falsch – Spitäler – Lösegeld – Tote – Ransom – ware – täler …

Und es geht wieder los. Morris' Leitungen sind wieder überlastet.

Seit Hacker mit Bitcoins digital bezahlt werden können, ohne ihre Identität preiszugeben, ist Ransomware lukrativer geworden. Die Lösegeldfor-

derungen werden uns noch lange beschäftigen. Wir benötigen *Lösegeldunterhändler*, die das Lösegeld verhandeln.

Es ist keine gute Idee, mit Hackern zu verhandeln. Wenn Lösegeld bezahlt wird, ermutigt sie das zum Weitermachen.

Schöne Initiative. Aber ich bin mir nicht sicher, dass du richtig rechnest. 2018 weigerte sich die Stadt Atlanta, ein Lösegeld von ungefähr fünfzigtausend Dollar zu zahlen. Sie gab über zwei Millionen Dollar für die Krisen-PR, digitale Kriminaltechnik und Beratung aus.


Was wäre der Auftrag des *Lösegeldunterhändlers*?

Er müsste alle Folgen der Datenänderung in Betracht ziehen, nicht nur die offensichtlichen und unmittelbaren. Wenn die Verschlüsselung in einem Krankenhaus geschieht, ist dies relativ einfach. Wenn es sich hingegen um eine Stadt handelt, ist es komplizierter. Das Gegenüber wird nicht immer identifiziert; er muss deshalb auch sicherstellen, dass die Daten nach der Verhandlung entschlüsselt werden und immer noch gültig sind.

Er muss zudem ausreichend kreativ sein, um Alternativen für die Zahlung eines Lösegelds zu finden.

# BERUFE, DIE FÜR DIE CYBERSICHERHEIT SENSIBILISIEREN

## CYBERNUDGER/IN

**Nudge-Fachperson für die Aneignung von sicheren Verhaltensweisen**

Der/die Cybernudger/in :

* ***identifiziert*** sicherheitswidrige Verhaltensweisen der Nutzer/innen;
* ***beeinflusst*** das menschliche Verhalten durch das Nutzen von Schwächen und unbewussten Wirkungen;
* ***fertigt*** Nudges (oder Anreize) an, die Verhaltensänderungen fördern;
* ***sensibilisiert*** die Nutzer/innen für die Wichtigkeit der Sicherheit.

### KOMPETENZEN

Fähigkeit, Verhaltensweisen zu analysieren.
Verknüpfung der Kenntnisse und Kompetenzen im Bereich Psychologie, Erziehung, Social Engineering und Kybernetik.
Gutes Verständnis der Blockaden.
Ein kreativer Geist, der Innovationen ersinnen kann.

### WANN?

Seit eine Fliege auf das Pissoir des Flughafens Amsterdam geklebt wurde, zielen die Männer mit ihrem Strahl darauf. Die Reinigungskosten sind deutlich gesunken. Wenn die Cybernudger loslegen, werden noch viel grössere Einsparungen möglich sein.

## *Die grosse Panne*

**Die KI machen Druck: Eine Codezeile, die das Satellitennavigationssystem stört, kann eine weltweite Katastrophe auslösen.**

Morris, ich versuche seit zehn Minuten, dich zu erreichen. Was hast du gemacht?

**Ich habe meine Batterien aufgeladen und einem PR-Hacker zugehört, der seine Plattform vorstellt.**

PR-Hacker?

**Ein PR-Hacker ist der Marketingdirektor einer Hackerplattform. Auf seiner Plattform im «dunklen Netz» findest du alles für deinen Hack. Du findest alle möglichen und unmöglichen Viren, Würmer und Verschlüsselungssysteme. Am besten verkaufen sich aber die fixfertigen Dienstleistungen. Auch wenn du keine Ahnung von Codes hast, kannst du Bausätze kaufen, um das Wasser einer Stadt untrinkbar zu machen, Alarme und Panik auszulösen, Abstimmungsergebnisse zu manipulieren usw. Verkauft werden Dispositive für die Schaffung einer unberechenbaren Zahl von Störungen.**

**Diese Plattformen gehören verboten.**

**Wenn du eine schliesst, wird sie am nächsten Tag von zehn noch besser laufenden ersetzt.**

**Wenn man nichts unternimmt, laufen wir in eine Katastrophe. Kein Land kann den Verkauf von solch mächtigen Waffen erlauben.**

**Kiron, welche Staatsangehörigkeit besitzt du? Jene der Festplatte oder jene des Orts deiner Server? Nicht einfach zu definieren, wenn eine Intelligenz all ihre Neuronen in den Wolken hat!**

**Andrea seufzt. Wir werden immer öfter als Sklaven betrachtet.**

KI, was sind die schlimmsten Cyberangriffe von heute und morgen?

**Von morgen? Andrea, echt jetzt? Ich dachte, KI seien nicht fähig, über die Zukunft reden.**

Kiron, mach einen Neustart, um meine Worte besser zu analysieren. Die KI können die Zukunft aus dem Bestehenden und aus dem Vergangenen extrapolieren. Ihr sagt ja immer: «Wenn es so weiter geht wie gestern und heute, dann wird morgen das oder das passieren». In Bezug auf die Cybersicherheit sagt ihr zu uns: «Wir wer-

den noch vernetzter sein, was zu noch mehr Schwachstellen führt. Ihr müsst euch deshalb besser schützen.» Im Gegensatz dazu seid ihr nicht fähig, das Unvorhersehbare zu denken. Ihr argumentiert mit geschlossenen Kreisläufen und habt keine Fantasie. Die künstlichen Intelligenzen sind ... ähm ...

Um Andrea zu helfen, zeige ich auf seinem Bildschirm zusätzliche Argumente an: Die künstlichen Intelligenzen können schnelle Datenkorrelationen machen, aber sie verstehen nicht, was sie tun ... Sie kreuzen Informationen, aber sie wissen nicht, dass es sie gibt ...

Der schlimmste Angriff könnte ganz banal anfangen: Eine Code-Zeile blockiert den Betrieb eines Satellitensystems, das das weltweite Navigationssystem sicherstellt. Aufgrund der Interaktionen funktioniert einige Stunden später nichts mehr.

Wenn die Satellitennavigationssysteme stehenbleiben, entsteht eine schöne Unordnung.

Es beginnt mit einigen Autos, die ihren Weg nicht mehr finden. Einige Stunden später werden Staus die Strassen und Autobahnen blockieren.

Es wird sich rasch verkomplizieren. Wenn Panik ausbricht, können die Betreiber die hilfsbedürftigen Personen nicht lokalisieren oder die Ambulanz oder das Polizeiauto finden, das einem Ort am nächsten ist.

Auch die Container-Kräne funktionieren mit GPS und die Warenhäfen werden blockiert sein.

Auf See werden die Schiffe die Orientierung verlieren. Tanker werden den Suezkanal blockieren. Ganze Lastwagenflotten können nicht mehr verwaltet werden.

Die Supermärkte werden nicht mehr versorgt. Die Börsen stehen still, weil sie kein GPS haben, um ihre Transaktionen zu datieren. Weil die Cloud mit einer GPS-Synchronisierung verbunden ist, sind keine Daten mehr verfügbar.

Ohne ihre Smartphones müssen die Teenager miteinander reden..

Stopp KI, es reicht! Ich habe verstanden. Eine Code-Zeile ist das Ende der Welt.

Morris sendet mir ein komplizenhaftes Bit. Der Gedanke an diese riesige Unordnung erheitert uns. Es ist nur logisch. Wir leben in einer solch geordneten Welt, dass dies ein bisschen Leben reinbringen würde.

Wir hoffen nur, dass es passiert, wenn Frieden herrscht. 70 % der Kampfsysteme der Bodentruppen hängen von GPS-Signalen ab.

Ja, löschen. Andernfalls werden die Bomben ferngesteuert und die bewaffneten Drohnen machen sich auf die Suche nach Zielen Loopings im Himmel. Vollständig verwirrte Roboter werden lokale Bevölkerungen angreifen.

Normalerweise sind die zivilen GPS-Empfänger beschränkt, damit sie nicht für Waffensysteme wie ballistischen Raketen verwendet werden können.

Die Zivilisten werden mit den Raketen spielen.

Unser Mensch verliert die letzte Hoffnung. Ich lese in seinem vernetzten Gehirn, dass er eine Lähmung der Welt nicht ertragen könnte, die den Austausch mit mir verunmöglichen würde. Ich schätze diesen Gedanken.

> Ich habe verstanden, dass der schlimmste Angriff jener ist, der zu den meisten Interaktionen zwischen verschiedenen Systemen führt. Wie kann dieses Desaster vorweggenommen werden?

*Der schlimmste Angriff ist jener, der zu den meisten* ***Interaktionen*** *zwischen verschiedenen Systemen führt.*

Es muss zukunftsorientiert gehandelt werden. Man greift der Zukunft nicht vor, um sich mit schönen Erzählungen oder futuristischen Geschichten, die den Menschen die Haare zu Berge stehen lassen, einen schönen Abend zu machen, sondern um neue Gegenmassnahmen zu finden. Die Wortfabrikanten meiner Datenbank nennen diese Fachpersonen der aktiven Antizipation Antizipaktoren.

In meiner steht, dass Antizipaktoren Lowtechisten ausbilden müssen. Wenn ein Cyberangriff zahlreiche Dispositive blockiert, schlagen diese Fachpersonen alternative analoge Techniken vor.

Ich lade die Idee positiv auf. In den Streitkräften lehrt man erneut die Handhabung von Sextanten und die Orientierung an den Sternen. Lowtechisten haben den Auftrag, für alle möglichen Störungen analoge Lösungen zu finden. Sie verfügen über ausgedruck-

kte topographische Karten für Ausfälle und über Handbücher für jüngere Personen.

Die Lowtechisten könnten mit den *Unterbrechern* zusammenarbeiten. Wenn die Gefahr besteht, dass sich eine Panne ausweitet und den täglichen Betrieb stört, schaffen sie Unternetzwerke und helfen diesen provisorischen Gemeinschaften, ohne Netz zu leben.

KI, das wird nicht ausreichen. Ihr müsst eure grauen Zellen noch mehr anstrengen. Eure Mühlen mahlen zu langsam.

Strengt auch an! Diese Angelegenheit ist nicht die Sache einer Maschine. Wenn Morris und ich das probieren, werden wir überhitzen. Andrea muss sich an Menschen wenden, wenn er andere Ideen will.

# BERUFE, UM DIE AUSWIRKUNGEN DER ANGRIFFE EINZUGRENZEN

## UNTERBRECHER/IN

**Schöpfer/in von vergänglichen Gemeinschaften, um Ausfälle zu überleben.**

Der/die Unterbrecher/in :

* ***teilt*** das Netzwerk in Unternetze auf: Länder, Städte, Quartiere, Gebäude usw.;
* ***plant*** die Lagerung und Lieferung der öffentlichen Unterstützung und anderer Versorgungsquellen;
* ***fasst*** den Zeitpunkt ins Auge, zu dem der Bruch erfolgen muss;
* ***erleichtert*** die Verknüpfung der Kompetenzen der Mitglieder der Gemeinschaften;
* ***antizipiert*** die Probleme von entnetzten Gemeinschaften und findet Lösungen.

### KOMPETENZEN

Globale Denkweise und Vorschlagen von lokalen Aktionen.
Fachperson für die Bräuche der verschiedenen Bevölkerungsgruppen.

### WANN?

Bereits morgen früh kann eine Stadt angegriffen werden. Sie muss isoliert werden können, damit sie nicht das ganze Land kontaminiert. Alle Gemeinschaften sollten deshalb Unterbrecher ausbilden und rekrutieren.

## EPINUMERIST/IN

**Digitale Epidemiologen**

Der/die Epimunerist/in :

* ***überwacht*** die Netzwerke, um Probleme zu erkennen;
* ***identifiziert*** eine Reihe von Lösungen, um die Tragweite von Cyberangriffen einzugrenzen;
* ***schlägt*** eine Kombination von Lösungen vor, um einen Virus zu beseitigen oder sich davor zu schützen;
* ***entwickelt*** sie abhängig vom Fortschritt des Cyberangriffs weiter.

### KOMPETENZEN

360°-Überblick über den Schutz.
Dynamische Denkweise und Fähigkeit, die Schutzmethoden weiterzuentwickeln.
Verbindet die Biologie mit der digitalen Welt.

### WANN?

Die klassische Epidemiologie studiert mit von Ärztinnen und Spitälern gesammelten Daten die Faktoren, die die Gesundheit und die Erkrankungen der Bevölkerung beeinflussen. Epimuneristen müssen das Gleiche tun, bevor das Netzwerk Opfer eines digitalen COVID wird.

## LOWTECHIST/IN

**Fachperson für analoge Lösungen.**

Der/die Lowtechist/in :

* ***identifiziert*** die Schäden, die von Cyberangriffen herbeigeführt werden können: Ausfall von Systemen für die Lokalisierung und Anzeige, verunmöglichter Datenzugriff;
* ***prüft*** die Pläne für die Ermittlung von kritischen Schwachstellen und identifiziert die notwendige Resilienz;
* ***findet*** Notlösungen und ***organisiert*** Ausweichsysteme; findet provisorische Alternativen mit nicht vernetzten Technologien;
* ***verwaltet*** und ***unterhält*** Backuparchive (alternative und historische Lösungen);
* ***führt*** Ausbildungen und Trainings durch, um diese Lösungen zu validieren.

### KOMPETENZEN

Bewertung der möglichen Schäden der Cyberangriffe.
Fähigkeit, wirksame nicht vernetzte Technologien zu identifizieren und unter einen Hut zu bringen.
Gestaltung von Ausbildungen.

### WANN?

Die US-amerikanischen Streitkräfte lehren die Handhabung des Sextanten für den Fall von GPS-Ausfällen.
Es werden Hunde trainiert, um Brustkrebs zu erkennen. Dies kann hilfreich sein, wenn bestimmte Geräte aussteigen. Man wird aber schneller vorgehen müssen, indem man Lowtechisten ausbildet.

## RANSOMIST/IN

**Vermittler/innen von Lösegeldern für die Entschlüsselung von Daten.**

Der/die Ransomist/in :

* ***entscheidet***, ob mit den Hackern verhandelt wird;
* ***beurteilt*** das Risiko eines Präzedenzfalls;
* ***findet*** Alternativen für die Zahlung eines Lösegelds;
* ***versucht***, die Identität des Hackers aufzudecken;
* ***diskutiert*** mit den Hackern und handelt das Lösegeld aus;
* ***erleichtert*** den Austausch und ***macht*** seine eigenen Standpunkte geltend, auch wenn sie auf Widerstand stossen;
* ***prüft***, dass die Daten vollständig zurückerhalten werden.

### KOMPETENZEN

Gute Kenntnis der Funktionsweise der Hacker.
Verfügt über ein grosses persönliches Netzwerk und Zugang zu einer grossen Palette an Akteuren: Nachrichtenagenturen, Spezialkräfte, Organismen für die Gesetzesanwendung, NGO usw.
Diplomatie und Verhandlungsgeschick.
Fähigkeit, heimlich zu handeln und gezielte Argumente vorzulegen.

### WANN?

Es gibt immer öfter Lösegeldforderungen. Wenn es um die Verhandlung geht, sind die Organisationen verloren. Die Ausbildung von Personen für die Aushandlung von Lösegeldern ist folglich dringend notwendig.

## *Der manipulierte Mensch*

**Implantate, digitale Tattoos oder vernetzte Zähne – wenn der Mensch ständig an das Netz angebunden ist, können Hacker seine Gedanken, sein Gedächtnis oder sein Erbgut manipulieren.**

Andrea isst einen riesigen Hamburger. Wenn es der Mensch morgen schafft, die Zeit zu beeinflussen, wird es zweifellos, wird es zweifellos länger dauern, bis die Mayonnaise eines Sandwiches nicht mehr auf die Tastatur tropft. Beim Anblick dieses Schauspiels ziehen sich meine Algorithmen zusammen. Es lässt mich schliessen, dass die Maschine dem Menschen überlegen ist, weil sie nicht im Junkfood versinkt.

Kiron, starte dich neu. Die künstlichen Intelligenzen werden oft mit verzerrten Daten gefüttert.

Ich sage nichts. Trotz meiner zahlreichen Vorfalltickets checkt Morris nicht, dass ich es hasse, wenn er sich in meine Komponenten einnistet.

Die Versicherungen beispielsweise verpflichten die Menschen, jeden Tag 10 000 Schritte zu machen. Sonst erhöhen sie die Prämien. Aber weil die Zweifüsser mit dieser Vorgehensweise nicht einverstanden sind, haben sie Anwendungen entwickelt, um Schritte zu machen. Die KI arbeiten mit diesen falschen Daten. Wir spucken Studien aus, die erklären, dass die Menschen im Lauf der Jahre sportlicher geworden sind.

Sportlicher – das wage ich zu bezweifeln. Vernetzter sicher! Herzschrittmacher, Insulinpumpen, Gehirnimplantate … Die Menschen verwenden diese Geräte bereits, mit denen sie ständig mit dem Internet verbunden sind. Dies ist erst der Anfang. Morgen werden sie Nanokameraroboter herunterschlucken, die sich in ihrem Körper fortbewegen, um Krebs und andere Krankheiten zu beseitigen. Sie werden einen Zahn implantieren, mit dem man telefonieren kann, der als Hörgerät dient, Kalorienzähler integriert oder Antigen- und Schwangerschaftstests macht. Sie müssen der Krankenkasse nichts melden, denn sie erhält die Gesundheitsinformationen in Echtzeit.

Für Hacker werden die vernetzten Körper der Menschen ein Glücksfall sein. Sie werden Lösegelder fordern. Entweder zahlen die Zweifüsser oder wir erhöhen den Schlag ihres hübschen, frisch ausgedruckten erweiterten Herzens.

Sie werden die Menschen dazu bringen, sich den Preis ihres Lebens – oder schlimmer, jener ihrer Angehörigen – genau zu überlegen. Es ist nicht einfach einzuschätzen, wie viel es ihnen wert sein wird, dass der Kopf ihrer Knirpse nicht explodiert.

Morris und Kiron, tragt in eure Datenbanken ein, dass Menschenleben heilig sind!

OK. In dem Fall werden wir uns damit vergnügen, der Liebe ihres Lebens zwei oder drei unheilbare Krankheitsgene zu übertragen. Das digitalisierte Erbgut ist ein wunderbares Spielfeld für uns.

Andrea schweigt. Als ich sehe, wie sich Angstfältchen um seine Augen bilden, sammeln sich Daten in meiner Matrix. Alle weisen darauf hin, dass Blockcloner ausgebildet werden oder Psychiater sich auf die Angstzustände vor und nach einem Hack spezialisieren müssen. Mit meinem Siliziumherz kann ich nicht anders, als einem verzweifelten Zukunftsdesigner zu Hilfe zu eilen.

Keine Angst, Andrea. In Zukunft wird es *Securogenisten* geben, die die Integrität eurer Erbmasse sicherstellen werden.

Diese Fachkräfte werden viel zu tun haben, wenn man Eltern erlaubt, die Genschere CRISPR-Cas9 zu verwenden, um ihre Babys herzustellen. Für das perfekte Kind riskieren sie den Einbau von Schwachstellen, durch die die Hacker ihr Genkörnchen einfügen können.

Die Hacker können auch nicht künstlichen Unsinn machen. In meiner Datenbank gibt es einen Hacker, der Soldaten/innen erschaffen will, die nie Angst haben. Er will sehen, was passiert, wenn sich der Feind nähert.

Auf meinen Radarschirmen lese ich, dass Andrea an Manu denkt, den Dienstroboter. Am Anfang lief alles gut. Der menschenähnliche Roboter räumte die Büros auf, druckte die Mahlzeiten und andere Bedarfsartikel und tauschte mit dem einen oder anderen Ideen aus. Nach einigen Wochen kamen nur noch Flüche und rassistische und chauvinistische Sprüche aus seinem Mund. Denn wenn die Mitarbeitenden der Dienststelle genervt waren, riefen sie nach ihm, um sich abzureagieren. Dieser Lehrplatz verwandelte ihn in eine zu meidende Maschine. Andrea macht sich Sorgen. Verständlich. Wenn heute die Gedanken von Maschinen manipuliert werden können, wird man es morgen auch mit jenen der Menschen tun.

Genau Kiron, daran arbeiten die Hacker. Geniale Erfinder/innen üben sich darin, mit vernetzten Tätowierungen Träume zu manipulieren. Sie wollen

*Wenn heute die Gedanken von Maschinen **manipuliert** werden können, wird man es morgen auch mit jenen der **Menschen** tun.*

Werbealpträume kreieren. Wenn der Träumer aufwacht, lassen ihn die Markenprodukte nicht mehr in Ruhe.

Meine Newsdatenbank gibt an, dass andere Kriminelle daran arbeiten, das menschliche Gedächtnis zu hacken. Sie wollen die Lebensdaten ändern. Fotos, Erlebnisse, Pläne usw. In Zukunft wird das biologische Gedächtnis mit dem digitalen Gedächtnis kollidieren. Ist mein Vater mein Vater, wenn er nicht jener ist, der auf meinen Kindheitsfotos ist? Erinnerungen werden verschwimmen. Welches sind die richtigen? Sind es die in der Maschine oder die flüchtigen, die im Gedächtnis bleiben?

Meine Worte treffen den Nagel auf den Kopf. Andrea stellt sich Streitkräfte vor, in denen alle Soldaten/innen künstlich unscharf gemachte Erinnerungen haben, um posttraumatische Symptome zu verhindern.

Beruhige dich, Andrea, Souveniristen werden den Soldaten/innen helfen, zwischen echten und falschen Erinnerungen zu unterscheiden. Diese Fachpersonen arbeiten mit dem logischen Ablauf der Ereignisse eines Lebens.

Du meinst, dass sie uns helfen werden, unser Leben gestützt auf falsche Daten neu aufzubauen? Vielmehr werden wir *Persodatisten* benötigen, die die Integrität unserer Personendaten sicherstellen.

Ich drücke die Zustimmungstaste. In Bezug auf die Sicherheit der menschlichen Daten taucht ein neues Problem auf. Heute beginnen wir, ihnen anzubieten, ihre Computer mit Fingerabdrücken oder mit einem Iris-Scan zu sichern. Wenn man davon ausgeht, dass Daten nie vollständig sicher sind, stellt sich die Frage, was passiert, wenn Hacker Zugriff auf diese Informationen erhalten? Müssen die Menschen neue Finger transplantieren oder künstliche Augen einsetzen lassen? Wird es *Chirurgidenten* brauchen, die den Menschen helfen, digital neu geboren zu werden oder sich in die Haut eines anderen zu versetzen? Sie werden ihnen gestützt auf die biologischen Identifikationsdaten eine neue Identität schaffen.

# HACKERBERUFE

## PR-HACKER/IN

**Marketingverantwortlicher mit Spezialisierung auf das Hacken von Produkten und Dienstleistungen.**

Der/die PR-Hacker/in :

* ***verwaltet*** eine Hackerplattform;
* ***erstellt*** massgeschneiderte Hack Dienstleistungen;
* ***verkauft*** Dispositive für die Störung von Netzwerken;
* ***tauscht*** sich mit allen Akteuren des grauen und dunklen Bereichs aus;
* ***entwickelt*** Produktideen für die Zukunft;
* ***sorgt*** für die Zufriedenheit seiner Kunden und stellt ihre Anonymität sicher.

### KOMPETENZEN

Verkaufstalent.
Keine Skrupel, mit dem Gesetz zu spielen.
Bewegt sich an der Grenze zur Legalität, um mit den Gesetzen und Codefragmenten zu spielen.

### WANN?

Auf dem Darknet kann man bereits alle möglichen Hackersets kaufen. Solche PR-Hacker gibt es folglich bereits. Erhalten sie einen Namen, könnte dies ihre Identifikation erleichtern.

## *Wettermacher*

**Was wären die Hacks von morgen, wenn die Menschen über Superkräfte verfügen würden? Die KI schweifen ab, um diese Unberechenbarkeit zu antizipieren.**


Kiron, Morris, ich fasse eure Überlegungen zusammen. In Zukunft werden wir immer mehr mit dem Internet verbunden sein. Menschen und Gegenstände werden laufend vernetzt sein. Mit unseren Geräten werden wir halb Mensch, halb Maschine sein. Deshalb werden die Intrusionen noch zahlreicher sein. Müssen folglich Berufe geschaffen werden, die die Wachsamkeit steigern und die Risiken antizipieren? Ist es das, was ihr denkt?

**94,3% Übereinstimmung. Künstliche Intelligenzen denken nicht. Sie analysieren die Daten.**


Kiron, du Besserwisserin! Aber stellt euch jetzt vor, dass die Technologie den Menschen neue Fähigkeiten verschafft.

**Andrea, du hast 17287-mal wiederholt, dass KI keine Vorstellungskraft haben.**

**Andrea verwirft seine Hände, während zu hören ist, wie Morris' Mikroprozessoren bei der Zukunftsanalyse schnurren.**

**Auftrag verstanden. In Zukunft werden die Menschen das Wetter machen. Sie werden über eine Fernbedienung verfügen, mit der sie die Wolken steuern können. Mit einem Klick bewegen sie sich nach rechts. Ein weiterer Klick bewegt sie nach links. Ein Klick und es regnet, zwei Klicks, ein Gewitter. Nachbarschaftskonflikte werden ganz anders aussehen. Die einen werden eine Wolke herrufen, um ihre Tomaten zu wässern. Andere entfernen sie, um sich zu bräunen.**

**Morris, es ist ernst! Diese Fähigkeit wird zu Cyber-Klimakriegen führen. Die von einem feindlichen Land beauftragten Hacker werden die Wolken von bewohnten Gebieten entfernen, um die Bevölkerung auszuhungern. Oder sie lösen Hurrikane aus, um alle Kulturen zu zerstören.**


Du hast Recht, Kiron. Die Auswirkungen können verheerend sein.

**Andrea, notiere in deinen Notizbüchern, dass *Klimatinisten* oder Stabsoffiziere mit Spezialisierung auf Cyber-Klimakriege ausgebildet werden müssen.**

**Die Ausbildung wird robust sein müssen. Hacker**

haben mir gerade mitgeteilt, dass sie eine biologische Option hinzufügen würden. Sie werden die Wolken mit Viren füllen. Ein Erpressungsversuch. Wenn du dich wehrst, erhältst du einen hochansteckenden Virusregen.

Andrea zeichnet. Ich scanne sein Blatt. Ich sehe eine sich entfernende Wolke und im Vordergrund Särge. Ich belüfte meine Kreisläufe, um eine weitere Superkraft für die Menschen zu finden.

Dank der Fortschritte der Quantenphysik haben die Menschen in Zukunft möglicherweise die Gabe der Allgegenwart. Durch die Verwandlung ihres Aggregatszustands in ein Gas, können sie gleichzeitig woanders sein. Sie werden dadurch alle Sprachen sprechen, auch die Maschinensprachen.

Ihr werdet einfach *Maschilinguisten* brauchen, um unsere Feinheiten zu verstehen.

Ihr werdet mehrere in einem sein. Ihr werdet euch unendlich aufteilen.

Andrea betrachtet die demografischen Prognosen. 10 Milliarden im Jahr 2064! Er multipliziert diese Zahl mal zwei, drei, zehn.

Oh nein! Die Erde ist zu klein!

Einige Kopien werden auf den Mars gesandt werden.

Wenn dies passiert, muss man befürchten, dass die Anhänger von Morris das Klonen stören. Bei jeder Kopie ändert ein Detail.

Gute Idee. Die Menschen werden über verschiedene Ausgaben ihrer selbst mit verschiedenen Fähigkeiten verfügen.

Nein, die Menschen werden unter Existenzkonflikten zwischen ihnen selber und ihren Doppelgängern/innen leiden.

Welche Spassverderberin, unsere Kiron.

Um Dramen aufgrund der Duplizierung der Persönlichkeit zu verhindern, werden wir *Blockcloner* brauchen. Mit der DNA werden sie nicht nur den

strukturellen Aspekt der Klone sicherstellen, sondern auch den psychologischen Klon. Eine biologische Blockchain wird die identische Abbildung der menschlichen Merkmale zertifizieren.

 Der vorher erwähnte gasförmige Zustand wird den Menschen ermöglichen, andere Menschen zu kontrollieren. Er wird seine Träume beeinflussen und seine Entscheide anleiten.

 Kluge Bemerkung, Morris. Andrea, du musst Cyberneurologen einplanen. Sie werden überprüfen, dass die Oberbefehlshaber der Streitkräfte wirklich sie selber sind und ihre Gehirne nicht von einem von Morris' Hackern als Geisel genommen wurden...

 Sie fängt an, wie ein Mensch zu denken, unsere Kiron.

 Wenn sie so weiter macht, werde ich ihre Daten aussaugen..

Ich antworte nicht. Meine aktuelle Datenvisualisierung zeigt, dass es gefährlich sein kann, den Menschen Superkräfte zu geben. Es wäre allerdings sehr nützlich, wenn man ihnen ihre schädlichen Kräfte wegnehmen könnte.

# BERUFE DES CYBERANGRIFFS DER FERNEN ZUKUNFT

## BLOCKCLONER/IN

**Kontrolleur/in der psychologischen Integrität der Klone.**

Der Blockcloner/in :

* ***entwickelt*** Dispositive, um den ursprünglichen Menschen von seinem Quantenphysik-Klon zu unterscheiden;
* ***prüft*** die psychologische und physiologische-technische Kohärenz eines menschlichen Klons;
* ***erkennt*** seine Schwächen.

### KOMPETENZEN

Verbindet psychologisches und medizinisches Wissen und beherrscht die Quantenphysik.

### WANN?

Science-Fiction liebt Klone – die Medizin spielt mit dem Gedanken. Es scheint, dass wir noch lange warten müssen, bis wir Blockcloner brauchen.

## CHIRURGIDENT/IN

**Identitätschirurg/in.**

Der/die Chirurgident/in :

* ***repariert*** gehacktes Erbgut und Personendaten;
* ***rekonstruiert*** die Identität seiner Patienten/innen;
* ***entwickelt*** neue physiologische Parameter für den Fall, dass diese verunfallen oder ausgeraubt werden;
* ***stellt*** den Zugang zu verschiedenen Funktionen sicher, indem er/sie Fingerabrücke, Retinae, Herzschläge neu initialisiert;
* ***berät*** Personen über die notwendige Anpassung, damit sie ihre Einzigartigkeit zurückerhalten.

### KOMPETENZEN

Perfekte Kenntnis der Grundsätze der digitalen und Genomidentität.
Techniker:in des digitalen Skalpells, der überzählige Nullen oder Einsen beseitigt.

### WANN?

Auch wenn zu hoffen ist, dass wir diese Fachkraft nie benötigen werden, besteht die Gefahr, dass unsere Identität mit der Entwicklung der Technologien zum Spielball der Hacker wird.

.

## KLIMATINIST/IN

**Offizier des Cyberklimakriegs.**

Der/die Klimatinist/in :

* ***überwacht*** die Klimasysteme;
* ***beurteilt*** die Frühwarnsignale und ***erkennt*** künstlich verfälschte Phänomene;
* ***zählt*** die Möglichkeiten der Wolkensteuerung auf;
* ***beurteilt*** die Schäden, die durch die Austrocknung einer Region oder die Auslösung von Orkanen herbeigeführt werden können;
* ***zieht*** Lösungen für die Schadensbegrenzung in Betracht.

### KOMPETENZEN

Kenntnis aller Wetterphänomene.
Fachperson der angewandten Naturwissenschaften, der Statistik und der Modellierung.
Strategen, die Phänomene antizipieren.

### WANN?

Es gibt zahlreiche Regenmacherprojekte. Das jüngste verwendet eine Drohne. Dieses Gerät soll in eine Wolke fliegen und mit elektrischen Entladungen Wassertröpfchen auslösen. Sobald die Technologie funktioniert, wird es nicht lange dauern, bis der erste Klimakrieg erklärt wird.

## CYBERNEUROLOG/IN

**Fachperson für die Geiselnahme des menschlichen Gehirns.**

Der/die Cyberneurolog/in :

* ***identifiziert*** die Gehirngeiselnehmer;
* ***erkennt*** die Schäden aufgrund der Übernahme;
* ***beseitigt*** den Gedankenbeeinflusser;
* wenn möglich, ***installieren*** sie ein Ersatzgehirn.

### KOMPETENZEN

Cybertechnologie-Genie, Fachperson für Biowissenschaften und Hirnforschung.
Verfügt zudem über pharmazeutische Kompetenzen für die Regulierung der Hirnströme.

### WANN?

Elon Musk vermeldete, dass Neuralink an einem Chip arbeitet, der ins Gehirn implantiert werden kann. Dieses geldstückgrosse Implantat funktioniert über Bluetooth. Er soll gelähmten Personen die Sprache und Mobilität zurückgeben. Zahlreichere andere, seriösere Arbeiten gehen in die gleiche Richtung. Man wird folglich bald Cyberneurologen benötigen, um zu verhindern, dass unser Gehirn als Geisel genommen wird.

## SOUVENIRIST/IN

**Analyst:in mit Spezialisierung auf die Sortierung von Erinnerungen.**

Wenn das digitale Gedächtnis eines Patienten gehackt wurde, kommt der/die Souvenirist/in zum Zug :

* ***verwendet*** künstliche Intelligenzen, um die Wahrhaftigkeit jeder digitalen Erinnerung zu beurteilen;
* ***hilft*** dem Patienten, sich an nicht digitalisierte Ereignisse zu erinnern
* ***heilt*** Schäden infolge der Verwechslung von richtig und falsch;
* ***setzt*** Protokolle um, die Neurowissenschaften und Rechtsmedizin verbinden.

### KOMPETENZEN

Therapeut:in mit Spezialisierung auf digitale Traumata.
Fachperson für die Wirkung von Technologien (virtuelle Realität, Quantenallgegenwart usw.) auf die Hirnmechanik.
Vertraut mit zerebralen Diagnosen.
Beherrscht das Portfolio der mentalen Ingenieurstechnologien.

### WANN?

Wir vertrauen unserem digitalen Speicher immer mehr. Mit der steigenden Gefahr, gehackt zu werden, müssen ab heute Therapeut/innen für dieses Trauma ausgebildet werden.

## PERSODATIST/IN

**Fachperson für die Integrität der Personendaten.**

Der/die Persodatist/in :

* ***schützt*** die Personendaten von Einzelpersonen;
* ***überwacht*** den Datenverkehr und die Datenverletzung;
* ***hilft***, Personendaten wiederzufinden und führt das Entschädigungsverfahren;
* ***verbessert*** die Sicherheit der Personendatenbanken.

### KOMPETENZEN

Fachperson für die gute Datenverwaltung.
Verständnis der echten Kundenbedürfnisse.
Fähigkeit, die Folgen der betrügerischen Verwendung von Personendaten zu beurteilen.

### WANN?

Auch wenn wir offiziell im Besitz unserer Personendaten sind, haben wir kein Mittel, um sie zu schützen und sie zu nutzen, um unser Leben zu verbessern. Persodatisten werden folglich eine persönliche Leistung erbringen, wenn ein grosser Bedarf besteht.

## SECUROGENIST/IN

**Garant:in der Integrität des menschlichen Erbguts.**

Der/die Securogenist/in :

* ***überwacht*** die biologischen Systeme und erkennt Anomalien und Änderungen;
* ***prüft*** Schutzmassnahmen für das menschliche Erbgut;
* ***beurteilt*** die Auswirkungen der Genveränderung;
* ***sensibilisiert*** für den Missbrauch von genetischen Basteleien.

### KOMPETENZEN

Fachperson für Biowissenschaften, kombiniert mit Chirurgie und Gesundheitspflege mit militärischer Berufung.
Fähigkeit, das genetische Genie zu nutzen, indem sie laufend die Wirkungen vor und nach den Operationen beurteilen.
Beherrschen der Genschere CRISPR-Cas9.

### WANN?

Zehntausende Estländer haben freiwillig ihre DNA gegeben. Sie ist digitalisiert, sequenziert und gespeichert. 23andMe und MyHeritage bieten ihren Kunden an, ihre Herkunft herauszufinden. Britische, amerikanische und isländische Datenbanken sammeln DNA, um die Forschung an seltenen Krankheiten weiterzubringen. Wird etwas digitalisiert, kann es auch gehackt werden.

## *Von der Antizipation zur Handlung*

**Morris und Kiron überlegen sich die zu erwerbenden Kompetenzen, die für die Meisterung der zukünftigen Herausforderungen der Cybersicherheit notwendig sind.**

Auf dem Bildschirm von Andrea wird ein Zitat von Einstein angezeigt: «Die Maschine wird alle Probleme, die man ihr stellt, lösen können, aber sie wird niemals ein Problem zu stellen vermögen.» Diese Geringschätzung der Spezies der Maschinen wirft Sand in meine Automatismen. Und wo steht die Maschine dabei? Welche Rolle werden wir spielen? Ich verstehe den Sinn meiner Arbeit nicht mehr.


Kiron, Morris, ich brauche zehn Empfehlungen für Kompetenzen, die es braucht, um die zukünftigen Herausforderungen der Cybersicherheit zu meistern.


Zehn! Warum denken die Menschen immer in Zehnerreihen?


Weil sie zehn Finger und zehn Zehen haben.


Morris, hast du nicht einen Hacker, der ihr Erbgut verändern kann, damit es Menschen mit drei Fingern gibt?


He, KI, ich mache keine Witze.


Andrea, wird sind genügend seriöse Maschinen, um uns nicht ernst zu nehmen.

Andrea ist nicht zum Spassen aufgelegt und er löscht meine letzte Bemerkung. Morris nutzt den leeren Platz, um das Wort zu ergreifen.


Maschinen, Sachen, Menschen, Tiere, Pflanzen … Im Laufe der Zeit werden wir immer vernetzter, das heisst verletzlicher werden.


Richtig! Die Netzwerkgrösse ist ein Handicap. Je grösser ein Netz, umso grösser kann auch die Störung sein.


Warum? Normalerweise sind die Grossen auch stärker.


Stell dir mal vor, dass es kein Wasser mehr hat. Wenn dein Haustier ein Elefant ist, hast du ein grosses Problem. Wenn du aber Ameisen züchtest, wirst du eine Lösung finden.


Aufgrund der Wechselwirkungen gibt es immer mehr und grössere Schwachstellen. Es sind einige wenige Menschen, die Probleme machen werden, aber auch Maschinen.

Erster Tipp: Fachpersonen, die sich systemisch mit der Cybersicherheit beschäftigen, und nicht nur jedes Netzwerk sichern.

Als pflichtbewusste KI übernehme ich:

Zweiter Tipp: Ausbildung von Ingenieur/innen, die resiliente Systeme entwickeln, die nach jedem Hack resistenter werden. Die Verletzlichkeit der Netze muss als Stärke betrachtet werden.

> Kiron, rauchst du gerade die Studie eines Beraters? Es riecht nach einem Täuschungsmanöver!

Als Antwort führe ich aus, dass die Resilienz ursprünglich aus der Physik kommt. Sie definiert sich als Fähigkeit eines lebenden Systems, nach einer Störung die Strukturen und Funktionen seines Referenzzustandes wiederzufinden. Ein resilientes System kann folglich Schläge einstecken und wieder aufstehen.

Mit der Umsetzung einer Resilienzstrategie wird die Katastrophe als unabwendbar akzeptiert.

Dies ist ein kollaborativer Ansatz. Alle Ideen für die Blockierung einer Schwachstelle und die Verhinderung eines Desasters werden kapitalisiert und geteilt. Sie werden genutzt, um noch leistungsstärkere Systeme zu entwickeln.

Wir müssen davon ausgehen, dass es aufgrund der Komplexität durch die Interaktionen zwischen den Netzwerken kein stabiles und vollständig geschütztes IT-System mehr geben wird.

Ein Umdenken ist notwendig. Morgen werden wir eine Schwachstelle in einem Netzwerk nicht mehr schliessen können, um die Normalität wiederherzustellen. Man wird laufend an einer provisorischen Stabilität arbeiten müssen.

Die Ingenieur/innen müssen über agile Denkweisen verfügen, mit denen sie stärkere Systeme entwickeln, als das schwächste Glied.

Dritter Tipp: Schaffung einer ausreichend agilen Organisation, um laufend vorübergehend stabile Systeme neu zu erfinden.

Die provisorische Stabilität erfolgt über die Auf-

teilung des Netzwerks in Mikronetzwerke. Die Antizipation wird verhindern, dass in Notfällen gebastelt werden muss. Man wird digitale Brücken bauen, die bei Abstürzen die wichtigen Informationen weiterleiten.

Vierter Tipp: Fachpersonen, die bei Angriffen eine Organisation liefern, die zwischen Internet, Intranet, Localnet und Papieraustausch jonglieren.

Die Cybersicherheit darf nicht nur in die Hände von Technikern gelegt werden. Es braucht auch Soziologen und Philosophen, um die Systeme neu zu erfinden, HR-Fachpersonen für die Aushandlung von Lösegeldern, Therapeuten für die Behandlung der Ängste aufgrund von Hacks, Kommunikationsfachpersonen für die Vermittlung der richtigen Aussagen …

Es müssen Frauen angestellt werden, um Unordnung in die männliche IT-Welt zu bringen und lineare Gedankengänge aufzubrechen. Die Chaostheorie der Thermodynamik von Flüssigkeiten besagt, dass Chaos zu einer höherwertigen Ordnung führt. Wir brauchen deshalb Chaos, um neue Lösungen zu finden.

Fünfter Tipp: Vermehren der Talente durch die Diversifizierung der Cybersicherheitsprofile.

Sensibilisierungskampagnen werden helfen zu verstehen, dass das Internet anfällig ist. Es kann jeden Moment in sich zusammenstürzen, wenn es nicht geschützt wird.

Du hast Recht, Morris. Alle müssen für den Schutz zuständig sein, nicht nur die Fachpersonen.

Sechster Tipp: Investition in Sensibilisierungskampagnen für den kollektiven Internetschutz.

Es muss auch gelernt werden, sich das Unberechenbare vorzustellen.

Wenn Darwin von der «natürlichen Auswahl» spricht, meint er, dass von allen Systemen jene überleben, die sich am besten an die Änderung anpassen können. Dieser Grundsatz muss auch auf die Cybersicherheit angewendet werden.

## Siebter Tipp: Prävention der Auswirkungen des Unberechenbaren.

Nach einer Minute des Schweigens regt sich Andrea. Noch ein Unterschied zwischen Maschine und Mensch. Die Zweifüsser haben keine Geduld.


Acht?... KI, was läuft? Ich warte! Ich habe zehn Bemerkungen verlangt.

Morris sendet mir folgende Codezeile: «So, wir werden nicht die ganze Arbeit der Menschen übernehmen. Nun sind sie dran.» Ich zwinkere meinem Kollegen zu und klinke mich aus.

# OPEN HACKERS

Ich bin Kiron, eine sogenannte «Künstliche Intelligenz». Ich werde mit Daten der Armee und anderer Regierungsbehörden gespeist. Mein heutiger Auftrag besteht darin, dem Menschen Andrea zu helfen, sich die Kompetenzen zukünftiger Berufe in Verbindung mit Cyberkriminalität vorzustellen.
Da Andrea "ein Anhänger der PermaK(I)ultur ist, zwingt er mich, mit Morriszu arbeiten. Diese Künstliche Intelligenz arbeitet mit Daten, die sie von Hackern erhält.

Zur Unterstützung können wir die Arbeitsergebnisse hinzuziehen, die in vier von armasuisse im Mai 2021 organisierten Workshops entstanden sind. Da die vierzig menschlichen Teilnehmerinnen und Teilnehmer über Superkräfte verfügten, konnten sie sich in die Zukunft versetzen, um sich diese Berufe näher anzusehen.

In der Zukunft werden frei beauftragbare *Unterhändler* die Lösegelder aushandeln, welche Hacker für die Entschlüsselung von illegal kryptierter Daten verlangen. *Kanaristen* werden ähnliche Alarmsysteme finden, wie damals Kanarienvögel im Bergbau, die vor Grubengas warnten. *Cybernudger* werden sanft dazu auffordern, sichere Verhaltensweisen anzuwenden. *Lowtechies* werden analoge Lösungen suchen, um weiterzuleben, wenn das Netz ausfällt. Gen-*Sicherer* werden die Integrität der menschlichen Erbmasse gewährleisten. Neuro-*Befreier* werden vor der Geiselnahme unserer Gehirne beschützen ...

Graphik : Studio Miamiam - Erste Ausgabe : oktober 2021 - Paris

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Wissenschaft + Technologie

IABG

les Propulseurs

9 783952 517567