> *Der Staat ist heute der massiven Welle von Cyberangriffen, die uns trifft, nicht gewachsen. Ob auf Bundes-, Kantons- oder Gemeindeebene, die Behörden haben offensichtlich noch nicht begriffen, was bei diesen Hackerangriffen auf dem Spiel steht. Dabei stehen unsere persönlichen Daten auf dem Spiel, die wir Behörden, Banken oder Versicherungen anvertrauen.*
> (*Le Temps*, 2022)

Die Versprechungen von 5G

Und die Sicherheitsherausforderungen

DATENSICHERHEIT

Es ist unumgänglich, die Einführung der 5G-Technologie mit der Frage von Cyberangriffen und Computerterrorismus zu verknüpfen, einer sehr stillen und oft unentdeckten Bedrohung.

Mit der Einführung von 5G geht eine Flut von vernetzten Objekten aller Art einher. Diese sind anfällig für Datendiebstahl und jede Form der Übernahme von aussen. Unsere zunehmende Abhängigkeit von modischen Anwendungen, die Virtualisierung unserer Daten und die Datenmengen, die von den gegenwärtigen und zukünftigen vernetzten Objekten (IoT) erzeugt werden, gefährden unsere Unabhängigkeit und unsere Sicherheit. Mit 5G wird letztere um das Zehnfache sinken.

Aber was ist Cybersicherheit?

Cyber-Sicherheit ist ein allgemeiner Begriff, der den Schutz von Computern, Servern, Mobiltelefonen, elektronischen Systemen, Netzwerken und Daten vor bösartigen Angriffen umfasst (Kaspersky).[1]

Die Bedrohung der Cybersicherheit steigt jedes Jahr auf globaler Ebene mit der zunehmenden Komplexität und Konnektivität der Netzwerkinfrastruktur, wodurch die Sicherheit der Öffentlichkeit, der Gesundheit, der Wirtschaft und der Schweiz (National Institute Of Standards And Technology) [2] ernsthaft gefährdet wird.

In den USA berichtete ein auf Cybersicherheit spezialisiertes Unternehmen von einem jährlichen Anstieg der Anzahl von Dateien, die 2019 durch Cyberangriffe gefährdet sind, um 112%, was allein im Oktober 2019 7,9 Milliarden Dokumente ausmachte (Risked Based Security).[3]

Im WEF-Bericht zu den globalen Risiken 2018 steht das Risiko von Cyberangriffen an dritter Stelle, nur übertroffen von Naturkatastrophen und extremen Klimaver-änderungen (World Economic Forum).[4]

Das Risiko steigt mit dem Wachstum der vernetzten Objekte exponentiell an, da jedes Objekt auch eine potenzielle Schwachstelle ist, die ausgenutzt werden kann (World Economic Forum).[5]

Die Zunahme von vernetzten Objekten, kurz IoT, erhöht somit das Risiko von Cyber-angriffen.

Um das Ausmass der Gefahr in der Schweiz zu verstehen, ist ein Rückblick notwendig.

1 https://www.letemps.ch/opinions/face-aux-cyberattaques-letat-nest-hauteur
2 https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
3 https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf
4 https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/
5 http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/

PANORAMA VON CYBERANGRIFFEN

«Das war vorhersehbar. Und es ist bereits Realität geworden. Es ist nicht mehr möglich, die Liste der Schweizer Unternehmen und Behörden, die Opfer von Cyberangriffen geworden sind, auf dem neuesten Stand zu halten. Die Angriffe sind unaufhörlich. Seitdem am Dienstagabend bekannt wurde, dass der Autoimporteur Emil Frey gehackt wurde, werden sich, während Sie diese Zeilen lesen, sicherlich weitere Vorfälle ereignet haben. Und immer häufiger stellt sich eine Frage: Was tun die Behörden und was sollten sie tun, um diese Plage zu bekämpfen?» (*Le Temps*, 2022)

Die Schweiz erlebte im Jahr 2021 einen Anstieg der Cyberangriffe auf Schweizer Unternehmen um 65% gegenüber dem Vorjahr, laut dem kalifornischen IT-Sicherheitsspezialisten Check Point Software. (TDG, 2022) [1].

Hauptziele sind Industrieunternehmen. Check Point Software zählte im Jahr 2022 wöchentlich 738 Angriffe, was einem Anstieg von 20% entspricht. Zu beachten ist, dass die Statistiken von Check Point Software auf Kundenangaben beruhen und somit nur einen Teil der in der Schweiz aufgetretenen Cyberangriffe darstellen.

In Kürze:

- Der Gesundheitssektor: +107%.
305 wöchentliche Angriffe pro Unternehmen im Durchschnitt
- Der Finanz- und Bankenplatz: +98%.
durchschnittlich 271 wöchentliche Angriffe pro Unternehmen
- Regierungs- und Militäragenturen: +8,6%.
durchschnittlich 388 wöchentliche Angriffe pro Unternehmen
- Kommunikationssektor: +65 %.
durchschnittlich 107 wöchentliche Angriffe pro Unternehmen
- Versicherungsgesellschaften und Anwaltskanzleien: +1%.
191 Angriffe pro Unternehmen im Durchschnitt [2]

Die erfolgreichen Angriffe allein im Jahr 2021 betrafen die folgenden Einrichtungen:

Der Land- und Kommunalfahrzeughersteller Bucher
Der Messeveranstalter MCH
Der Online-Vergleichsrechner Comparis
Die Schifffahrtsgesellschaft auf dem Genfersee CGN
Die Neuenburger Kantonalbank
Die private Klinikgruppe Pallas
Der Pharmaindustrie-Zulieferer Siegfried
Die Gemeinde Rolle

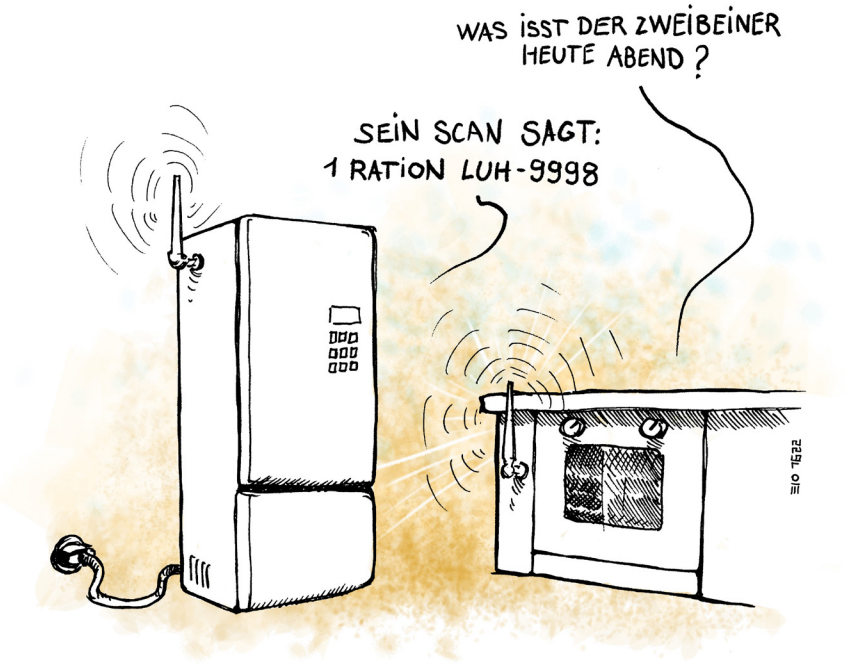
Im Jahr 2022 haben die tatsächlichen Angriffe bereits die folgenden Akteure getroffen:

Das IKRK [3] [4]
Der Automobilkonzern Emil Frey [5]
Der Pharmakonzern Zur Rose [6]
Die Gemeinde Yverdon-les-Bains [7]
Der Luzerner Industriekonzern Chemie + Papier Holding (CPH) [8]

Zum Vergleich: Den grössten Anstieg verzeichnete Europa mit über 600 wöchentlichen Cyberangriffen (+68%), gefolgt von den USA (500, d. h. +61%) und Lateinamerika (+38%).

1 https://www.tdg.ch/le-nombre-de-cyberattaques-a-bondi-de-65-en-suisse-en-2021-283750587480Ibid
2 Ibid.
3 https://www.24heures.ch/les-donnees-de-plus-de-500000-personnes-piratees-au-cicr-566330900259
4 https://www.letemps.ch/economie/contre-cicr-cyberattaque-etait-puissante-ciblee
5 https://www.ictjournal.ch/news/2022-02-03/cyberattaque-contre-emil-frey-des-donnees-publiees-sur-le-darkweb-update
6 https://www.swissinfo.ch/fre/zur-rose-potentiellement-victime-de-cyberpirates/47275872
7 https://www.rts.ch/info/regions/vaud/12785714-la-ville-dyverdonlesbains-a-ete-victime-dune-minicyberattaque.html
8 https://agefi.com/actualites/entreprises/cph-victime-dune-cyberattaque

MIT WELCHEN FOLGEN?



Gesundheit

Diebstahl und Veröffentlichung privater gesundheitsbezogener Daten im Kanton Neuenburg und Lösegeldforderung.[1] [2] Wer wird die Rechnung bezahlen? Wie gefährlich ist es für die Bürgerinnen und Bürger, wenn ihre Gesundheitsdaten landesweit im Darknet veröffentlicht werden?

Depressionen, Krebs, Schwangerschaftsabbrüche usw. - all diese Daten waren vorüber-gehend für alle sichtbar im Internet zu finden. Und dennoch: Die Versicherungsunternehmen drängen darauf, ihre neuen Apps über Smartphones und Smartwatches zu nutzen, insbesondere dank der Einführung von 5G, und erhöhen damit die Verwundbarkeit unserer sensiblen Daten.

Finanzen

Laut FINMA ist eine Zunahme von Cyberkriminalität, Spionage und Cyberspionage zu beobachten, obwohl uns die Informationstechnologie immer stärker vernetzt und von-einander abhängig macht. Dies führt zu einer akuten Verwundbarkeit unserer Finanzinstitute, was sich wiederum auf das reibungslose Funktionieren des gesamten nationalen Finanz-platzes auswirkt. Der Reputationsschaden wäre beträchtlich und das Vertrauen in den Finanzplatz würde untergraben (FINMA).[3]

Dennoch kommen die Schweizer Banken ihrer Informationspflicht über Cybervorfälle, die sie ins Visier nehmen, nur unzureichend nach, wie eine Prüfung der Eidgenössischen Finanz-kontrolle (EFK) feststellt.[4] Die Situation wird dadurch verschärft, dass die Banken der FINMA den direkten Zugang zu MELANI (Nationales Zentrum für Cyber-Sicherheit NCSC) verweigern.

«Vom Datenschutz bis zur Abhängigkeit von ausländischen Technologien weist die Schweiz klaffende Lücken auf, zusätzlich zu den Lücken, die im Gesundheitsbereich aufgetreten sind. Der Schaden sitzt tief (...)»

(*Le Temps*, 29 mars 2021)

Nach der Krise von 2008 und angesichts des aktuellen Konflikts im Osten sind unsere Finanzdaten und unsere Unabhängigkeit gefährdet. Die Zunahme von Applikationen, die insbesondere mit E-Banking, Handel, Kryptowährungen, kontaktlosen Zahlungen usw. verbunden sind, schwächt jedoch unsere Fähigkeit, unsere Daten zu sichern, erheblich. Diese werden unter anderem das von den Smartphones genutzte Netz nutzen, insbesondere Antennen aus umstrittener chinesischer Produktion (z. B. Huawei [5]).

Regierung und Militär

Das Seco (Staatssekretariat für Wirtschaft) gibt zu, dass 130'000 Namen von Unternehmen, die im Jahr 2020 auf der EasyGov-Plattform einen Covid-Kredit beantragt haben, gehackt wurden. Auf Bundesebene treten eindeutig Lücken zutage.

Kommunikation, Imageschaden und sensible Staatsdaten werden von ausländischen Hackern als Geiseln genommen.[6] Was ist mit unseren Daten, die mit unserer Sicherheit, dem Terrorismus oder der Privatsphäre in Verbindung stehen? Die Virtualisierung und die digitale Abhängigkeit verschiedener Bereiche der Regierung, der öffentlichen Verwaltung und des Militärs gefährden unsere Institutionen und privaten Daten. Die von einem bestimmten Wirtschaftssektor versprochene IoT-Schwemme wird die Verwundbarkeit des Staates und seiner Mitglieder massiv erhöhen.

Versicherungen und Anwaltskanzleien

«Zurich Insurance scheint Opfer eines Cyberangriffs geworden zu sein. Verschiedene IT-Bereiche des Schweizer Versicherers und seiner Partnerunternehmen waren betroffen. Nachdem die Sicherheitslücke behoben war, informierte das Unternehmen jedoch weder seine Kunden noch die Medien.» Der Hacker war von der mangelnden Transparenz des Riesen enttäuscht und beschloss, die gestohlenen Daten im Darknet zu veröffentlichen, wie unsere Kollegen von *20 Minuten* [7] (*Le Matin*, 2021) am Montag berichteten.

Erpressung, Lösegeld, die Bürger werden durch die Speicherung ihrer Daten im Internet in eine Falle gelockt. Was passiert, wenn die Vielzahl von Anwendungen und vernetzten Objekten diese Daten ebenfalls speichern?

1 https://www.letemps.ch/economie/donnees-medicales-milliers-neuchatelois-ont-mises-ligne
2 https://www.rtn.ch/rtn/Actualite/Region/20220330-Les-donnees-medicales-de-milliers-de-Neuchatelois-sont-en-ligne.html
3 https://www.finma.ch/fr/documentation/dossier/dossier-cyberrisiken/cyberrisiken/
4 https://www.ictjournal.ch/news/2021-02-23/les-banques-suisses-dissimulent-trop-souvent-les-cyberattaques-qui-les-ciblent
5 https://www.euractiv.fr/section/economie/interview/meps-sound-the-alarm-over-chinese-mass-surveillance-project-in-belgrade/
6 https://www.lenouvelliste.ch/suisse/cyberattaque-le-secretariat-detat-a-leconomie-pris-a-son-tour-au-piege-1121460
7 https://www.lematin.ch/story/les-donnees-des-clients-de-la-zurich-insurance-finissent-sur-le-darknet-526688604451

HISTORISCHE VORFÄLLE UND SKANDALE

Im Jahr 2021 beschliesst die Schweiz, ihre nationale Cloud mit Amazon, Alibaba, Oracle, IBM und Microsoft aufzubauen. Das bedeutet, dass alle Daten der Eidgenossenschaft auf den Servern dieser multinationalen Konzerne aus den USA und China gespeichert werden. Aber warum nicht bei Schweizer Firmen? [1]

Im Jahr 2011 dokumentiert WikiLeaks den Verkauf von Spionagetechnologie an autoritäre Staaten. Diese Waffen werden zur Überwachung der Bevölkerung eingesetzt. Unter den Unternehmen, die sie entwickeln, sind auch einige Schweizer wie Dreamlab. Das Berner Unternehmen verkaufte seine Technologien an den Oman. Dank dieser Technologien konnte das Sultanat seinen Arabischen Frühling unter Kontrolle bringen. [2]

Im Jahr 2015 haben die Computer des britischen Unternehmens Cambridge Analytica die Facebook-Daten von mindestens 87 Millionen Nutzern verwendet, um die Stimmabgabe von Bürgern zu beeinflussen. Mithilfe unserer Daten ist Cambridge Analytica in der Lage, ein sehr genaues Bild der Wähler zu zeichnen. Und die politische Botschaft gezielt zu gestalten. [3] [4]

Im Jahr 2013 beauftragte die Schweiz die israelische Firma Verint, die von einem ehemaligen Mossad-Agenten gegründet worden war, mit der Herstellung des Abhörsystems für ihre Polizei und Gerichte. In Bern beunruhigt diese Wahl. Wird die Schweiz von Israel abgehört? [5]

Im Jahr 1995 schlossen der US-Geheimdienst (ein Spionageorgan, das von der CIA in Zusammen-arbeit mit dem deutschen Geheimdienst gegründet wurde) und die Schweizer Firma Crypto AG ein vertrauliches Abkommen, welches das Ausspionieren der Kommunikation von 130 Ländern ermöglichte. Jahrzehntelang war ein Teil der Schweizer Industrie in diese Aktivitäten verwickelt, trotz der «Neutralität» des Landes und mit dem Segen des Bundesrates. [6] [7] Es dauerte Jahrzehnte, bis die Affäre an die Öffentlichkeit gelangte, was dem Image der Schweiz schweren Schaden zufügte.

Wie viele der 200 Millionen vernetzten Produkte, die es in der Schweiz in den nächsten Jahren geben könnte, werden Ihre Aktivitäten ausspionieren?

1 https://www.rts.ch/docs/13032515--la-suisse-sous-couverture-.html
2 Ibid.
3 Ibid.
4 https://securityaffairs.co/wordpress/72058/social-networks/cambridge-analytica-closes.html
5 https://www.rts.ch/docs/13032515--la-suisse-sous-couverture-.html
6 Ibid.
7 «Opération Rubicon» https://www.bilan.ch/economie/operation-rubicon-la-suisse-dans-le-mal

AKTUELL: KOSTEN DES DIGITALEN VERBRECHENS

Auch die Kosten der digitalen Kriminalität steigen. Eine Studie über 254 Unternehmen in 7 Ländern schätzt die jährlichen Kosten pro Unternehmen auf 27,4% 11.7 Mio. GBP (14,5 Mio. CHF) jährliche Kosten pro Unternehmen im Jahr 2017, was einem jährlichen Anstieg von 27,4% entspricht (World Economic Forum). [1]

Er wird für den Zeitraum 2018-2022 auf 8 Billionen USD geschätzt.

Lösegeldangriffe machten 2017 64% aller Angriffe aus (Proofpoint Quarterly Threat Report). [2].

1 http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/#view/fn-44
2 https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q317-threat-report_1.pdf

IOT: RISIKEN?

Mit dem IoT wird sich die Art der Angriffe verändern. **Bereits heute sind die bekannten und weniger bekannten Risiken:**

- Datendiebstahl (Banknummern, Logins, etc.)
- Manipulation von Jugendlichen
- Spionage
- Deaktivierung von Autos aus der Ferne
- Manipulation von Abstimmungsgeräten
- Mord aus der Ferne durch gehackte Herzschrittmacher

(Proofpoint Quarterly Threat Report) [1].

Dieses neue Gesellschaftsmodell wird uns von stärkeren Akteuren aufgezwungen, d. h. von jenen, die wissen, wie man Daten erfasst und auswertet (GAFAM).

Mit der Möglichkeit, von einigen seiner Anwendungen zu profitieren, bringt dieses neue Gesellschaftsmodell ernsthafte Bedrohungen und Herausforderungen für die persönliche Freiheit mit sich.

Diejenigen, welche die KI steuern, besitzen neue Macht:

- Vorhersagekraft, die suggeriert und vorschlägt (wodurch die Wahrnehmung der Massen beeinflusst werden kann)
- Die Macht, eine bestimmte Wahrheit zu verkünden und sie durchzusetzen (und dabei jede andere Realität, die nicht programmiert ist, auszuschliessen)
- Injunctive Power (indem sie die Handlungen und das Verhalten von Individuen lenkt)
- Zwangsmacht zwingt (indem sie Verhaltensweisen bestraft, die von einer auferlegten Normalität abweichen)

(Solange Ghernaouti, *Swiss Cybersecurity Advisory & Research Group*) [2].

1 https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q317-threat-report_1.pdf
2 https://blogs.letemps.ch/solange-ghernaouti/

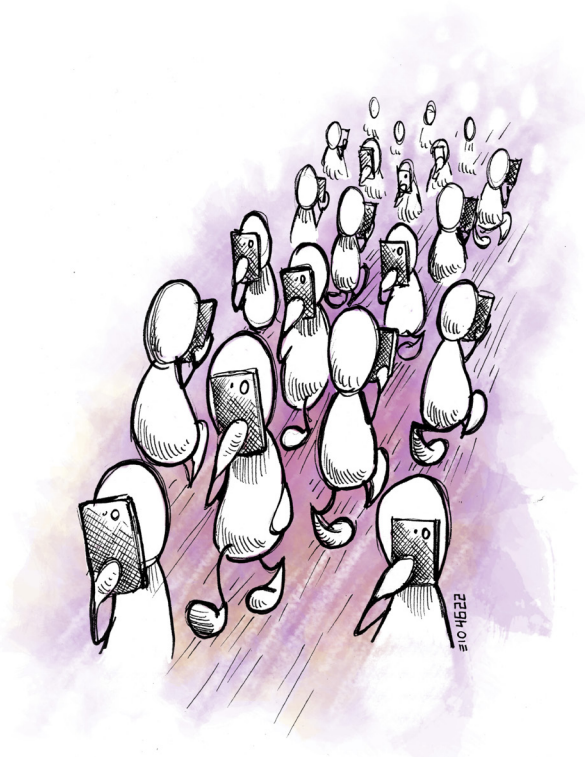
WELCHE UNTERSCHIEDE BESTEHEN FÜR DIE DIGITALE SICHERHEIT ZWISCHEN EINEM 4G- UND EINEM 5G-NETZWERK?

Dies ist nicht unbedeutend. Der Sprung zu 5G wird dazu führen, **dass neue vernetzte Produkte auf den Markt kommen.** Dies wird zu einer Zunahme von Sensoren aller Art in öffentlichen Bereichen (Bewegungssensoren, Lärmsensoren) und Überwachungskameras führen. Alle Gegenstände werden miteinander verbunden sein, insbesondere mit der Cloud, was eine ultraschnelle Kommunikation und einen Datenaustausch zwischen Maschinen (M2M) ermöglicht.

Allgemeine Risiken beim Einsatz von IoT und Werkzeugen, die ihre Nutzung ermöglichen

Im Folgenden finden Sie eine nicht abschliessende Liste potenzieller Gefahren, die mit dem Einsatz von IoT und den Technologien, die deren Nutzung ermöglichen, verbunden sind:

- **Phishing:** Eine Art von "*social engineering*", das dazu dient, Daten wie Bankdaten oder Logins zu stehlen, um Identitätsdiebstahl, nicht autorisierte Einkäufe oder Gelddiebstahl zu begehen. Es gibt verschiedene Arten von Phishing (*spearphishing, whalephishing,..*) (Phoenixnap). [1]
- **Viren:** Codes, die erstellt werden, um ein Computersystem unauffällig zu kompro-mittieren, um Spionage, Lösegeld, Entscheidungen und Kontrollen zu ermöglichen (Phoenixnap) [2]. Viren können unbemerkt ein ganzes Netzwerk von verbundenen Objekten beeinträchtigen, bis sie diese schliesslich unbrauchbar machen.



- **SQL-Injection:** Ein bösartiger Code, der für Unternehmen besonders riskant ist, da er die Datenbanken im Hintergrund, auf die er abzielt, manipulieren und zerstören kann.
- **DoS:** Ein Angriff, der auf die Deaktivierung eines Netzwerks oder Dienstes abzielt, wodurch dieser für diese Nutzer unbrauchbar wird. Typischerweise gegen einen Webserver mit hohem Nutzen gerichtet (Regierungen, multinationale Unternehmen, Banken...), werden diese Angriffe oft als Ablenkung für andere Angriffsformen genutzt (Phoenixnap). [3]
- **Ausspähen:** eine Umleitung des Informationsflusses zwischen unsicheren Objekten, z. B. Smartphones, Computern und anderen. Diese Angriffe sind unbemerkt, da sie die Nutzung des Objekts nicht beeinträchtigen. Jeder vernetzte Gegenstand ist dafür anfällig.
- **KI-Angriffe:** Diese sind bei weitem die gefährlichsten, da sie die Nützlichkeit von Objekten zu zerstörerischen Zwecken umwandeln können (Drohnenangriffe, Auto-unfälle, Entladungen von Herzschrittmachern, Stromausfälle...)

Wie kann die IoT-Technologie das Risiko erhöhen? Es gibt drei Ursachen für ein erhöhtes Risiko (Bruce Schneier, Vorstandsmitglied der EFF, and the *Chief of Security Architecture at Inrupt, Inc.*): [4]

1. Die Steuerung von Systemen durch Computersoftware
2. Konnektivität zwischen Systemen
3. Die Autonomie der Systeme

Das bedeutet:

1 **Kontrolle durch Computerprogramme:** Das IoT ist die Integration von Mikrocomputern in alle Gegenstände des täglichen Lebens. Durch die Fernsteuerung werden Haushalts- und andere Geräte anfällig für die Angriffe, denen Computer heute ausgesetzt sind.

2 **Interkonnektivität:** Wenn Systeme miteinander verbunden sind, führt die Verwundbarkeit des einen zum Ausfall des anderen. Bereits jetzt wurden Gmail-Konten durch intelligente Samsung-Kühlschränke kompromittiert (Networkworld) [5], Krankenhaus-Computernetzwerke durch Schwachstellen in medizinischen Geräten (Meddeviceonline) [6], und das multinationale Unternehmen Target wurde durch eine Schwachstelle in seinem CVC-System gehackt, die die Informationen von 40 Millionen Bankkarten offenlegte (Krebsonsecurity) [7]. Die Schwach-stellen eines Systems wirken sich auf andere aus und es entsteht eine unvorhersehbare Verwundbarkeit, für die niemand haftet.

3 **Autonomie:** Unsere Computersysteme werden immer autonomer. Sie kaufen und verkaufen Aktien, schalten den Heizkessel ein und aus, regulieren den Stromfluss im Netz und steuern - im Fall von fahrerlosen Autos - tonnenschwere Fahrzeuge automatisch an ihren Bestim-mungsort. Aus Sicht der Sicherheit bedeutet dies, dass die Auswirkungen von Angriffen sofort spürbar werden können. Je mehr wir den Menschen aus der Gleichung herausnehmen, desto mehr können schnelle Angriffe Schaden anrichten und desto mehr verlieren wir an präventive Kontrollmöglichkeiten.

1 https://phoenixnap.com/blog/cyber-security-attack-types
2 Ibid.
3 Ibid.
4 https://www.schneier.com/essays/archives/2016/07/the_internet_of_thin_3.html
5 http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html
6 https://www.meddeviceonline.com/doc/medjacking-how-hackers-use-medical-devices-to-launch-cyber-attacks-0001
7 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

VERWALTUNG VON PERSÖNLICHEN DATEN

Wer verwaltet unsere persönlichen Daten? Als Nutzer werden wir dazu angehalten, den Unternehmen, die unsere Daten verwalten, zu vertrauen und die Verantwortung für die Speicherung unserer Daten abzugeben, insbesondere bei der Cloud.

Aber die Cloud, das sind sehr physische Infrastrukturen, Datenzentren, die in der Regel amerikanisch oder chinesisch sind (Solange Ghernaouti, *Swiss Cybersecurity Advisory & Research Group*) [1].

Wir werden also ohne unsere informierte Zustimmung dazu gedrängt, das Recht auf Speicherung, Verwaltung und Eigentum unserer intimsten Daten an ausländische Unternehmen zu delegieren, die bereits von verschiedenen Skandalen im Zusammenhang mit der Nutzung unserer Daten erschüttert wurden.

Wir akzeptieren also gehorsam einen totalen Kontrollverlust über unsere wertvollste Identität, d. h. unsere Gewohnheiten, unser Verhalten, unsere Gedanken und unsere persönliche Entwicklung.

Mit der Entwicklung von 5G wird sich dieser Trend deutlich beschleunigen, denn je mehr digital genutzt wird, desto mehr Daten werden produziert, desto mehr müssen gespeichert werden und desto mehr ist man gezwungen, den Algorithmen zu vertrauen, die diesen Prozess automatisieren.

[1] *Allez Savoir* n°75, «Un monde virtuel, une pollution bien réelle», Rencontre avec Solange Ghernaouti, Professeure et spécialiste en cybersécurité à l'UNIL», Sept 2020 in https://com-www.unil.ch/allezsavoir/AS075.pdf

ALGORITHMEN UND KI

Wie können KI-Algorithmen von externen und unabhängigen Akteuren auf ihre Qualität und Sicherheit hin überprüft werden, wenn die Entwicklung von KI-Algorithmen unter dem Geschäftsgeheimnis ihrer Eigentümer erfolgt? Wie kann man den Entscheidungen solcher Systeme vertrauen, wenn man nicht in der Lage ist, die interne Logik der KI-Systeme zu verstehen und ihre Funktionsweise zu überprüfen und zu erklären?

Bevor wir in ein KI-gesteuertes System abtauchen, wie es derzeit weltweit geschieht, sollte es auf nationaler und internationaler Ebene Mechanismen geben, die es ermöglichen, den Einsatz von KI-Geräten, die gegen vereinbarte Werte verstossen (UNESCO), abzulehnen, sie anzuzeigen und die verantwortlichen Stellen vor Gericht zu bringen.

Im Jahr 2017 wurden 90% unserer Finanztransaktionen durch Algorithmen abgewickelt (OECD).[1] Nun ist laut Dominique Cardon, einem auf digitale Technologien spezialisierten Soziologen, **die Absicht des Architekten bei der Entwicklung des Algorithmus von zentraler Bedeutung, um die Auswirkungen zu verstehen, die diese Werkzeuge auf die Nutzer haben könnten.** Der Designer muss entsprechend seiner Wahrnehmung der Realität und entsprechend seinen Zielen eine Wahl treffen, welche Komponenten in sein Modell integriert werden, aber auch, wie der Algorithmus Informationen priorisieren und hierarchisieren oder eine Entscheidung treffen wird (Cardon, 2018).[2]

Diese Algorithmen sind also das Ergebnis einer strategischen Entscheidung, die versucht, bestimmte Ziele zu erreichen. Sie sind somit nicht neutral.

[1] OCDE (2019), *Artificial Intelligence in Society*, OECD Publishing https://www.oecd-ilibrary.org/docserver/aa565467-fr.pdf

[2] Cardon, Dominique. 2018. «Le pouvoir des algorithmes», Pouvoirs: Revue française d'études constitutionnelles et politiques no. 164: 63-73

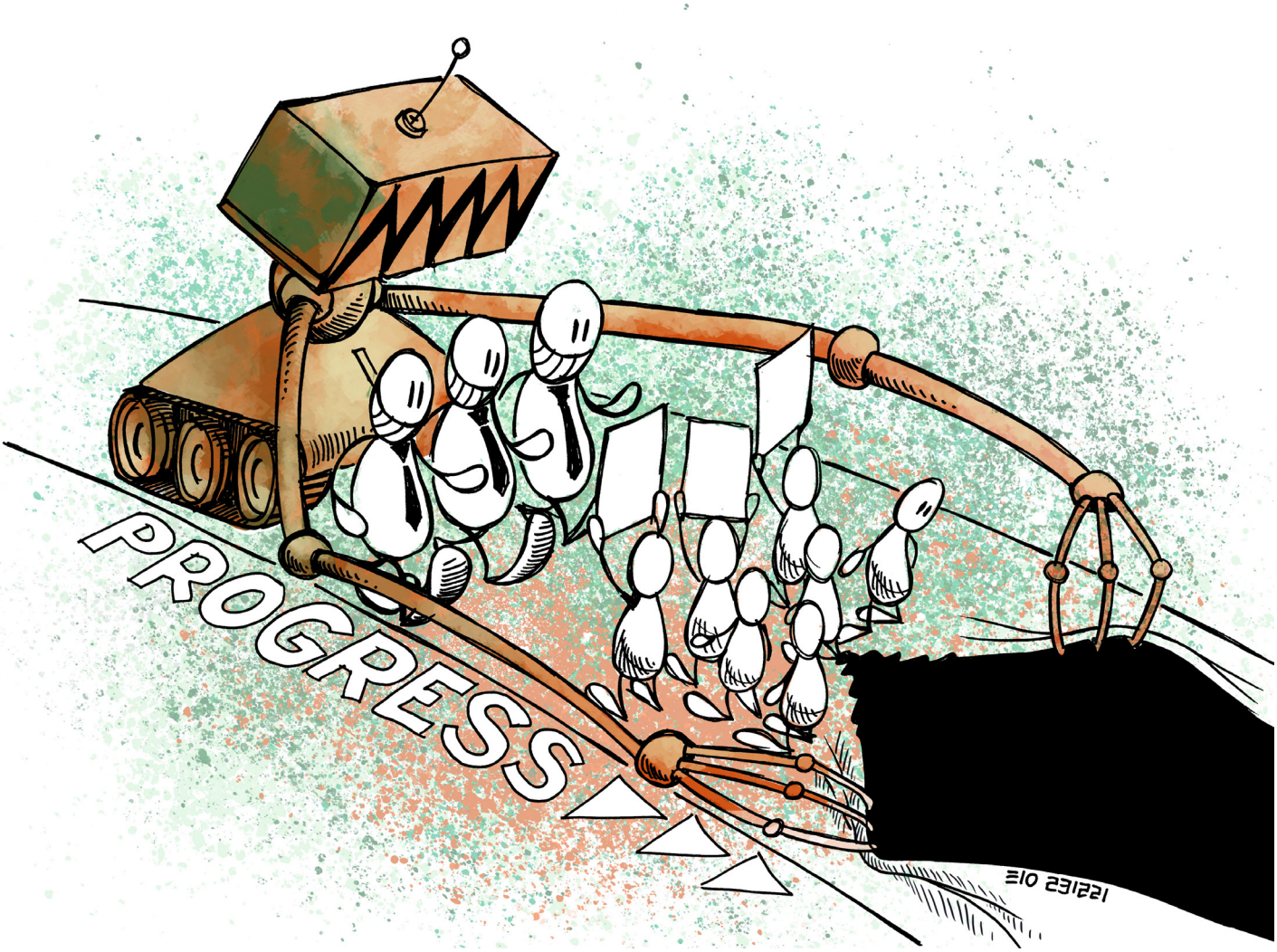
DIGITALISIERUNG, MACHT UND GESETZGEBUNG

Wer neue Befugnisse hat, braucht auch neue Rechte. Welche Rechte haben wir derzeit? Sollten wir nicht die Gesetzgebung für neue digitale Rechte priorisieren, bevor wir in eine Gesellschaft abtauchen, die von privaten Unternehmen aufgezwungen wird, die sich einer unabhängigen Kontrolle entziehen?

Hier ist eine Liste neuer Rechte, die gesichert werden sollten, bevor das IoT der Gesellschaft aufgezwungen wird:

- Das Recht des Einzelnen, andere Meinungen und Verhaltensweisen als die von einer KI geäusserten zu haben
- Die Toleranz von KI-Geräten gegenüber Menschen, deren Besonderheiten am Rande dessen liegen, was von den KI-Designern als normal definiert wird.
- Das Recht der Freiheit des Menschen, sich der Einfluss-, Lenkungs- und Zwangs-gewalt von KI entziehen zu können.
- Das Recht auf Abschaltung
- Das Recht, vergessen zu werden (endgültige Löschung der Daten)
- Das Recht, nicht unter computergestützter Überwachung zu leben
- Das Recht der Person zu wissen, ob sie mit künstlicher Intelligenz interagiert
- Das Recht auf Transparenz der Entscheidungsfindung durch künstliche Intelligenz
- Das Recht, gegen eine Entscheidung, die von einer künstlichen Intelligenz getroffen wurde, Beschwerde einlegen zu können
- Das Recht auf die Sicherheit seiner Daten
- Das Recht auf Privatheit der eigenen Daten

Mangels dieser Rechte, einer zumindest europäischen, wenn nicht gar nationalen Cloud, angesichts der Gefahren für die Demokratie, die Funktionsweise des Staates, unsere persönlichen Daten und unsere Privatsphäre, angesichts der realen Gefahren im Zusammenhang mit KI, der Definition von Algorithmen, den Risiken von Cyberangriffen und Lösegeldzahlungen sind wir der Ansicht, dass die Einführung der 5G-Technologie die bereits heute zu beobachtenden Risse noch verstärken wird und unsere Unabhängigkeit und Freiheit als demokratischer Staat ernsthaft gefährden wird.



Bibliographie

https://www.lete mps.ch/opinions/face-aux-cyberattaques-letat-nest-hauteur

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/

https://www.tdg.ch/le-nombre-de-cyberattaques-a-bondi-de-65-en-suisse-en-2021-283750587480

https://www.24heures.ch/les-donnees-de-plus-de-500000-personnes-piratees-au-cicr-566330900259

https://www.ictjournal.ch/news/2022-02-03/cyberattaque-contre-emil-frey-des-donnees-publiees-sur-le-darkweb-update

https://www.swissinfo.ch/fre/zur-rose-potentiellement-victime-de-cyberpirates/47275872

https://www.rts.ch/info/regions/vaud/12785714-la-ville-dyverdonlesbains-a-ete-victime-dune-minicyberattaque.html

https://agefi.com/actualites/entreprises/cph-victime-dune-cyberattaque

https://www.letemps.ch/economie/devraient-faire-autorites-suisses-face-fleau-cyberattaques

https://www.letemps.ch/economie/donnees-medicales-milliers-neuchatelois-ont-mises-ligne

https://www.rtn.ch/rtn/Actualite/Region/20220330-Les-donnees-medicales-de-milliers-de-Neuchatelois-sont-en-ligne.html

Bibliographie

https://www.finma.ch/fr/documentation/dossier/dossier-cyberrisiken/cyberrisiken/

https://www.ictjournal.ch/news/2021-02-23/les-banques-suisses-dissimulent-trop-souvent-les-cyberattaques-qui-les-ciblent

https://www.euractiv.fr/section/economie/interview/meps-sound-the-alarm-over-chinese-mass-surveillance-project-in-belgrade/

https://www.lenouvelliste.ch/suisse/cyberattaque-le-secretariat-detat-a-leconomie-pris-a-son-tour-au-piege-1121460

https://www.lematin.ch/story/les-donnees-des-clients-de-la-zurich-insurance-finissent-sur-le-darknet-526688604451

https://www.rts.ch/docs/13032515--la-suisse-sous-couverture-.html

https://securityaffairs.co/wordpress/72058/social-networks/cambridge-analytica-closes.html

https://www.bilan.ch/economie/operation-rubicon-la-suisse-dans-le-mal

http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/#view/fn-44

https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q317-threat-report_1.pdf

https://blogs.letemps.ch/solange-ghernaouti/

https://phoenixnap.com/blog/cyber-security-attack-types

https://www.schneier.com/essays/archives/2016/07/the_internet_of_thin_3.html

http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html

https://www.meddeviceonline.com/doc/medjacking-how-hackers-use-medical-devices-to-launch-cyber-attacks-0001

https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Allez Savoir n°75, «Un monde virtuel, une pollution bien réelle, Rencontre avec Solange Ghernaouti, Professeure et spécialiste en cybersécurité à l'UNIL», (sept. 2020)
https://com-www.unil.ch/allezsavoir/AS075.pdf

OCDE (2019), «Artificial Intelligence in Society», OECD Publishing
https://www.oecd-ilibrary.org/docserver/aa565467-fr.pdf

Cardon, Dominique. 2018. «Le pouvoir des algorithmes», Pouvoirs: Revue française d'études constitutionnelles et politiques no. 164: 63-73

Dessins et typographie: Eddy Juillerat – www.310.ch