Industrie 4.0:
„Zombie-Technologien auf dem Vormarsch“

von Andreas von Rétyi

Quelle: KOPP exklusiv Nr. 08/2017

► **Wie weit soll sie noch gehen, die smarte Technologie, die angeblich alles erleichtern soll? Winkt uns wirklich eine rosige Zukunft des »Alles ist organisiert und arbeitet für dich«, oder blüht uns ein Zombie-Zoo von Geräten, die uns kontrollieren und maßregeln? Und was, wenn die allgemeine Fake-News-Epidemie auf die so »smarte Technik« übergreift?**

Die Revolution ist bereits im Gange, sie scheint nicht mehr aufzuhalten:

→ Immer mehr Geräte kommunizieren miteinander, sind internetfähig, kontrollieren sich, uns und unsere Umgebung. Die verlockende *Tischlein-deck-dich-Mentalität* entpuppt sich zunehmend als gefährliche Falle.

Auf der *CES-Computermesse Las Vegas* war im Januar wieder Erstaunliches aus den »*Zukunftsfabriken*« zu sehen. Ob *AirportGuide-Robots*, *Video-Brillen* oder *Seine-Drohnen fürs Handy*:

❖ Auf den ersten Blick scheint alles ganz pfiffig, harmlos und nützlich, als Erweiterung bestehender Möglichkeiten. Allerorten smarte Helfer, die mit uns kommunizieren. Paradebeispiel: der »*intelligente Kühlschrank*«. **Am Ende wird es einer sein, der uns ständig überwacht, das Konsumentenverhalten registriert oder gar reglementiert.**

Durch das Grassieren internetfähiger Kontrolltechnologie büßen wir Privatsphäre ein und gehen zügig des eigenständigen Denkens verlustig, wenn die Technik uns alles abnimmt. Längst fehlt uns der Überblick darüber, was die »*klugen*« Geräte wirklich können und welche Daten sie sammeln. So sind »smarte Fernseher« schon seit Jahren zur Raumüberwachung einsetzbar, nicht nur durch ihren Besitzer.

→ *Der südkoreanische Forscher Yongdae Kim kritisiert, dass Sicherheitsabteilungen sich bislang kaum um die Schwachstellen von Sensortechnik kümmern, wie sie zunehmend in vernetzten Geräten zum Einsatz kommt. Das biete fatale Angriffsflächen. »Ein Sensor muss legitime physikalische Größen erkennen und andere physikalische Größen ignorieren«, so Kim. Aber genau dies funktioniere leider nicht immer. Sensoren lassen sich von außen gezielt angreifen.*

Gerade die Vernetzung im Internet der Dinge macht es möglich. Wir sehen uns mittlerweile einer Flut von smarten Systemen gegenüber. Was da im Anmarsch ist, hat gerade auch die CES wieder plastisch vorgeführt.

Die smarte Bedrohung

Elektronische Tattoos greifen Körperdaten ab, die Brille Uno blendet E-Mails ein, und geradezu bizarr wird es mit der smarten Haarbürste Hair Coach. Sie soll Haarwuchs und Haareigenschaften analysieren. Kategorie »*braucht kein Mensch*«. Der Blick in den Spiegel sollte genügen. Mit der neuen Technik gehen Kommerz und Verdummung Hand in Hand. Aber, wünschen sich die »*Eliten*« denn nicht genau dies:

- *Eine indifferente Masse, die nichts mehr eigenständig reflektiert?*

Die synthetische Spaßgesellschaft verfällt äußerst willig einer aggressiv offerierten Ablenkung mittels fragwürdiger Unterhaltungstechnik - man denke nur an Poke'rnon Go und seine Folgen, inklusive Überwachungsfaktor und Lebensgefahr.

Von ganz anderer Dimension wiederum sind da Hackerattacken auf moderne Medizintechnik - auf intelligente Insulinpumpen oder smarte Herzschrittmacher, per WLAN ansteuerbar. Nicht umsonst ließ *Dick Cheney* die Fernsteuerung seines Schrittmachers deaktivieren, aus ernster Sorge, einem Hacker-Terrorangriff zum Opfer zu fallen. Im so praktischen, fortschrittlichen »*Internet der Dinge*« ist nichts mehr wirklich sicher. Wir sehen uns mittlerweile einem unheimlichen *Zombie-Zoo* gegenüber, über den sich Dritte un-bemerkt einschleusen können. Wenn es an ausreichenden Sicherheitsfunktionen mangelt, wie das Experten monieren, bleiben unbefugte Zugriffe von außen und gefährliche Datenmanipulationen immer reale Optionen.

Blanker Wahn

Die Gefahren sind omnipräsent, Beispiele gibt es genug.

- Der *Tesla-Autopilot* übersieht einen LKW, es kommt zum tödlichen Unfall. Bemerkenswert: Die Behörden legen den Fall ad acta, vom Fahrzeughersteller erfolgt keine Rückrufaktion. Smartes Versagen total.

Ganze Unternehmen bauen heute auf umfassenden Roboterbetrieb. Im Januar wurde über die erste »*unbemannte Fabrik*« in der chinesischen Stadt *Dongguan* berichtet.

- Von 650 Mitarbeitern wurden 590 ersetzt. Die Produktivität habe sich seitdem um 250 Prozent verbessert, die Fehlerquote sei um 20 Prozent gesunken.
- Heute schon gilt es als schick, sich Chips implantieren zu lassen.
- Da wird sogar mit WLAN-fähigen Biotechnik-Implantaten experimentiert, die Funktionen von Sinnesorganen übernehmen sollen.
- »*Technologie-Künstler*« finden hier neue Performance-Ausdrucksformen.
- Eine eigene Subkultur verherrlicht die Idee, den menschlichen Körper durch invasive Maßnahmen möglichst weitgehend in Cyborgs zu verwandeln.
- Der »*Biohacker*« *Sander Pleji* implantierte sich einen Neurostimulator, um seine Cluster-Kopfschmerzen zu behandeln, wobei er schließlich in Panik-Attacken verfiel und nicht mehr Herr seiner Sinne war.

Die Folgen sind insgesamt unabsehbar. Wir liefern uns fatalen Techniken aus, die sich ganz gezielt in die Irre führen lassen. Schall bringt Drohnen zum Absturz, Infrarotlicht kann Infusionspumpen lebensgefährlich beeinflussen, Laserpulse bringen einen Herzrhythmus-Sensor aus dem Takt. Vor allem aber die Internetfähigkeit smarter Systeme erweist sich als fatal.

Soll das die Technologie unserer Zukunft sein?