Nutzungshinweise

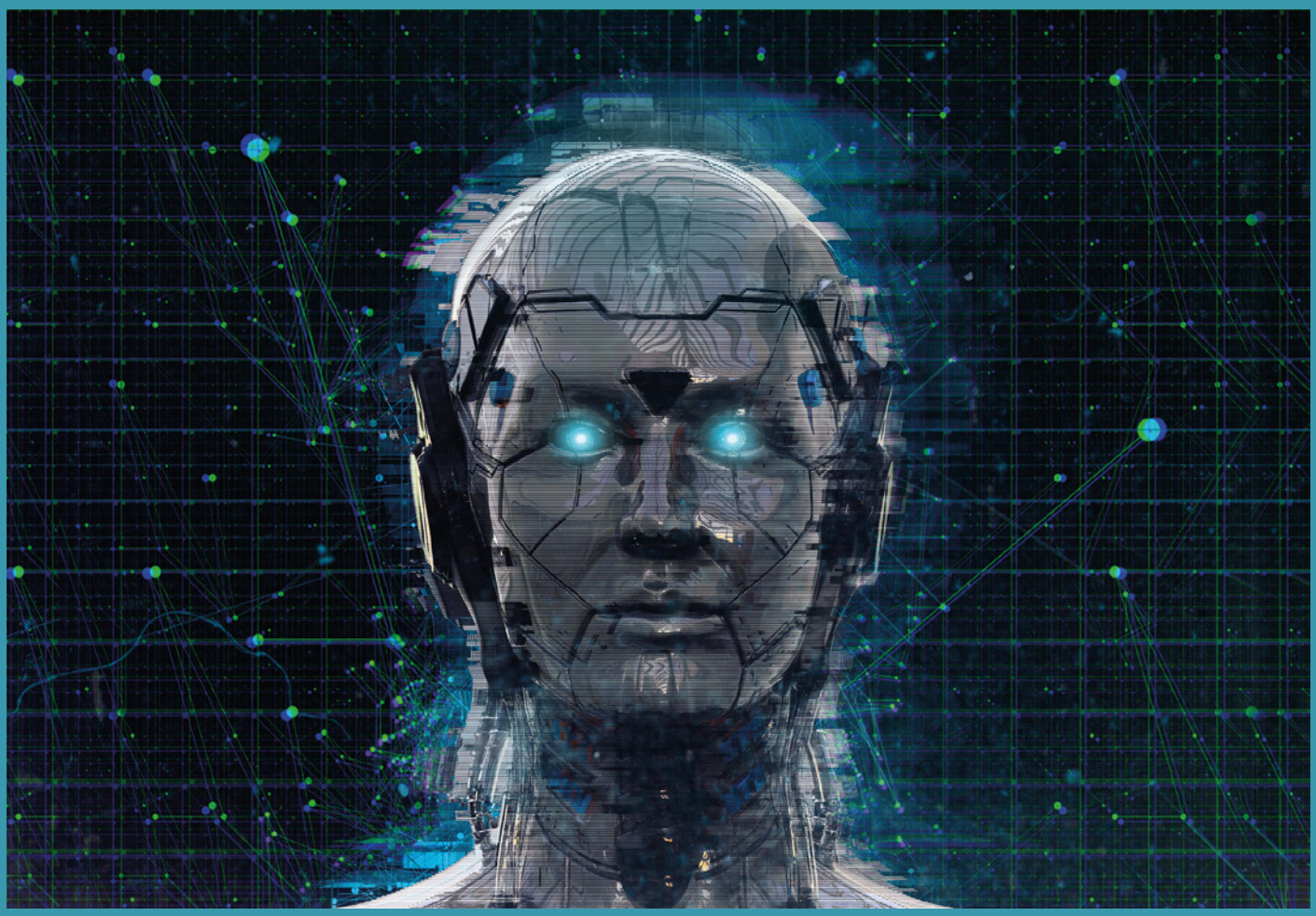
H 7625

FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

41. Jahrgang 2024 Einzelpreis: 7 EUR 1/2024 – März 2024

#FIfFKon2023



Perspektiven, Zukunftsvisionen, Chancen, Utopien

ISSN 0938-3476

• Weizenbaum-Studienpreise • Krieg im Weltraum • KI-Narrative •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Bildmaterial: Depositphotos
Autor abidal, ID 275369004

Inhalt

Ausgabe 1/2024

den hingearbeitet.[4] Somit werden Verfolgungsmöglichkeiten durch systematische Zugriffe auf Verschlüsselung, Staatstrojaner und Befugnisse für Cyberattacken gefordert, die auf der Ausnutzung und dem Vorhalten von Sicherheitslücken basieren.[5] So wird die Angreifbarkeit der allgemeinen technischen Infrastruktur mit finanziellen Ressourcen erhöht durch das Vorhalten (Nicht-Schließen) oder gar Einkaufen von Sicherheitslücken (auf illegalen Märkten) und das Entwickeln entsprechender Exploits. Damit wird allen geschadet, weil genau diese Lücken auch von Kriminellen genutzt werden, wie prominent bei WannaCry[6] deutlich wurde.

Alternativ erreicht man eine breite Informationssicherheit durch technische Integrität für alle, wenn man Ressourcen in das Schließen dieser Lücken steckt. Während hierzu staatliche Einrichtungen wie bspw. das Bundesamt für Sicherheit in der Informationstechnik und das Zentrum Informationstechnik in der Sicherheit gegensätzliche Positionen vertreten (technische Sicherheit vs. Überwachen und Strafen), ist sich die technische Community überwiegend so einig, dass sogar der CCC einen gemeinsamen offenen Brief mit Google verfasst hat, sonst im Diskurs eher auf gegenseitigen Positionen stehend.[7] Schön, dass es immer wieder Expert:innen-Anhörungen und Möglichkeiten für Eingaben von Stellungnahmen gibt. Schade, dass diese oft halbherzig und kurzfristig sind und die Ratschläge der Expert:innen von Exekutive und Legislative nur wenig berücksichtigt werden.[8]

Anmerkungen

1 https://de.wikipedia.org/wiki/Big_Tech (abgerufen am 2.2.2024)

2 https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/ (abgerufen am 2.2.2024)

3 Siehe auch Beitrag im gleichen Heft: Guagnin, Kocksch und Wiesse

4 Neue Programme wie der Souvereign Tech Fund der aktuellen Bundesregierung lassen auf eine konstruktivere Politik hoffen, aber die Chatkontrolle bleibt im EU-Diskurs

5 https://netzpolitik.org/2021/offener-brief-fuer-eine-echte-cybersicherheitsstrategie-ohne-neue-ueberwachungsmassnahmen/ (abgerufen am 2.2.2024), siehe auch Beitrag im gleichen Heft: Guagnin, Kocksch und Wiesse

6 https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ (abgerufen am 2.2.2024)

7 https://netzpolitik.org/2021/offener-brief-google-facebook-und-ccc-protestieren-gemeinsam-gegen-staatstrojaner/

8 https://www.fiff.de/presse/Cybersicherheitsstrategie/uni21.html (abgerufen am 2.2.2024)

Autoreninfo siehe Seite 41

Christian Heck

Eine technisch erzeugte Kriegswirklichkeit

Was codiert, auf tausende Maschinen übertragen und durch permanente Wiederholung Teil unserer Alltagswelt wird, stabilisiert sich selbst und wird schließlich zum kulturellen, unhinterfragten Sediment (Trogemann, Georg 2010).

Intelligence

Alles, was Soldatinnen und Soldaten in Operationszentralen gläserner Gefechtsfelder *(Transparent Battlefield)* sehen bzw. wahrnehmen können, das können sie einzig durch Apparate und Sehmaschinen wahrnehmen.

Alles, was sie erfahren, d. h. die Verarbeitung des Wahrgenommenen sowie auch der Abgleich mit weiteren Quellen, Geheimdienstinformationen, *Open Source Intelligence* (OSINT) usw, auch zu lernen, wie man sich innerhalb dieser Cyberräume verhält, wie man sich durch sie hindurch navigiert, all das findet mit Hilfe meist intelligenter Systeme statt. Technische Systeme, mit deren Hilfe Akteure symbolische Repräsentationen mit der konkreten Welt zu verbinden vermögen. Systeme, die sie befähigen in ihrem jeweiligen technologisierten Operationsumfeld zu handeln, d. h. für *Multi-Domain-Operations* (MDO), um „sinnvoll innerhalb von Kontexten handeln [zu] können" (Pangaro 2012). Diese technischen Systeme interpretieren somit Soldatinnen und Soldaten Teile von Welt technisch vor. Eben jene, die einst in sie hineinkamen.

> *„Während dieses Prozesses fließt demnach eine jeweilige Bedeutung […] in den Komplex auf der einen Seite*

(Input) hinein, um auf der anderen Seite (Output) wieder herauszufließen, wobei der Ablauf selbst, das Geschehen innerhalb des Komplexes, verborgen bleibt: eine ‚Black Box' also." (Flusser 2006).

Die Codierung der technischen, symbolischen Repräsentationen von Welt jedoch, nach denen und durch die militärisch-technische Handlungen vollzogen werden, so Flusser weiter, diese digitale Codierung „geht aber nun einmal im Inneren dieser Black-Box vor sich."

Artificiality

Zum Verständnis: Alles, was maschinenlesbar ist, musste erst einmal maschinenlesbar gemacht werden. Nicht nur technisch, sondern auch geistig. Alles, was für unsere Köpfe, auch technische Systeme berechenbar ist *(computable)*, musste erst einmal berechenbar gemacht werden.

Sprechen wir von gläsernen Gefechtsfeldern, von zivilen Cyberräumen, in denen militärische Handlungen verübt werden, so sprechen wir also von einer künstlichen Realität – einer technisch erzeugten Kriegswirklichkeit. Von einer Künstlichkeit *(Artificiality)* laut Herbert Simon, in der das technische Artefakt das Reale imitiert, indem es seiner Umwelt „das gleiche Gesicht zuwendet". Eine „Ähnlichkeit von außen und nicht von innen", „Wahrnehmungsgleichheit, aber zugleich auch eine wesentliche Verschiedenheit" (Simon 1969).

Künstliche technische Bilder als Verbundsysteme im Ineinander menschlicher und technischer Akteure, die aktiv über Leben und Tod von Soldatinnen und Soldaten, von Jugendlichen, von Großeltern, von Eltern und unseren Kindern Entscheidungen treffen. Folglich muss laut Vilém Flusser eine „jede Kritik der technischen Bilder darauf gerichtet sein, ihr Inneres zu erhellen. Solange wir über eine derartige Kritik nicht verfügen, bleiben wir, was die technischen Bilder betrifft, Analphabeten" (Flusser 2006).

Sense making

Denn die Militarisierung des Internets, auch dem der Dinge, greift mehr und mehr in unseren technologisierten Lebensalltag ein – in unser soziales Miteinander, dort, wo wir beisammen sind und miteinander sprechen. Dort, wo sich der Gemeinsinn verortet und Begriffe ihren gesellschaftlichen Sinn erhalten, also *Sense making* stattfindet. Mit technischen Systemen – und durch sie –, ob nun intelligent oder nicht, entstehen somit neue Erfahrungs- und Handlungsräume, die vorher nicht existiert haben. Wir lernten zu erkennen, dass Technik mehr und mehr der Erkenntnis unserer Lebenswelt vorausläuft. „Dass das, was wir erkennen können, sich im gleichen Maße verändert, wie wir unsere Lebenswelt technisch umbauen" (Trogemann 2021).

Cyberkriege sind demnach immer in bereits bestehende Handlungskontexte eingebunden und rekontextualisieren diese, indem sie durch Wiederaufladungen während des militärischen, computergestützten Erkenntnisgewinns in Erscheinung treten. Sie aktivieren somit realweltlichen Gebrauch, das heißt immer dann, wenn sie in die Umwelt eingebettet werden, neue Handlungskontexte, eben solche, die es für uns als Gesellschaft a posteriori zu erschließen gilt. Zu ihrer zivilgesellschaftlichen Erschließung sind die Systeme selbst jedoch leider nicht sonderlich hilfreich, da das, was wir wahrnehmen und erkennen können, eben erst innerhalb des gesetzten technischen Rahmens hergestellt wird.

So sind wir derweil auch nicht dazu in der Lage, sie in ihrer Komplexität durchzudenken und zu verstehen. Weder als Individuum, noch als Gesellschaft. Wenn laut Hannah Arendt das „Ergebnis des Verstehens Sinn" ist, dann kann der Zweck des Verstehens auch nur die Erzeugung von Sinn sein (Arendt 1994). Auf den gesellschaftlichen Kontext übertragen: Gemeinsinn. Dieser Sinn kann sich laut Arendt einzig durch die Existenz der Pluralität unter Menschen ergeben. Hierfür muss jedoch über diese technischen Wirkräume und über ihre sozialen, gesellschaftlichen und kulturellen Konsequenzen gesprochen werden können. Sie müssen in ihrer Komplexität verständlich dargelegt und gemeinsam erschlossen werden können.

Nach Arendt hieße das weiter: Je komplexer künstliche Welten auf Basis statistischer Modelle, Computersimulationen und Big Data generiert werden, desto weniger ergeben sie für die Gesellschaft Sinn, eben da wir nicht über sie sprechen können. Darum werden wir sie so nicht verstehen – weder die inneren Funktionsweisen der technischen Systeme noch ihre konkreten Folgen für die Zivilgesellschaft.

Einer der möglichen Gründe für die Sinnlosigkeit von Cyberkriegen liegt somit in den jeweiligen Ansätzen zur Konzeption gesellschaftsrelevanter Fragestellungen: der des Sinns und der Erkenntnis. Uns als Zivilgesellschaft ist es laut Hannah Arendt durchaus möglich, weit über die Grenzen der Erkenntnis hinauszudenken – nur nicht über das Wirkliche hinaus. Doch unser gemeinsames Leben, unser gemeinschaftliches Miteinander ist wirklich.

„Seien wir realistisch, versuchen wir das Unmögliche!" (Che Guevara)

Referenzen

Arendt, Hannah (1994): Zwischen Vergangenheit und Zukunft. Übungen im politischen Denken I., Ursula Ludz (Hrsg.), München: Piper Verlag, S. 111.

Flusser, Vilém (2006): Für eine Philosophie der Fotografie, 10. Aufl. (zuerst 1986), S. 15

Pangaro, Paul (2012): On artificial intelligence, Interview auf Vimeo. URL: https://vimeo.com/41782297

Simon , Herbert (1969): The Sciences of the Artificial, MIT Press.

Trogemann, Georg (2010): Code and Machine in Code: Between Operation and Narration, Andrea Gleiniger und Georg Vrachliotis (Hrsg.), Berlin, Boston: Birkhäuser, S. 41-53.

Trogemann, Georg (2021): DAS 18. KAMEL und Die Habitate des Denkens, in: Über das Paradox, Technik in der Kunst zu lehren, Ursula Damm / Mindaugas Gapsevicius (Hrsg.), Bielefeld: transcript Verlag, S. 117-166.

Autoreninfo siehe Seite 42