erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Hans-Jörg Kreowski, Aaron Lye

Cyberpeace – für Frieden, Freiheit und eine lebenswerte Welt

Willkommen bei dieser neuen Rubrik, die ab jetzt regelmäßig in der FIfF-Kommunikation erscheinen soll, um von aktuellen Entwicklungen rund um das Thema Cyberpeace zu berichten.

Was Fachkreise schon lange vorher wussten, wurde durch die Enthüllungen von Edward Snowden im Jahre 2013 einer breiten Öffentlichkeit bekannt: Die Geheimdienste der Welt betreiben eine umfassende Überwachung aller elektronischen Kommunikationsmedien. Um darüber hinaus darauf aufmerksam zu machen, dass diese Medien und insbesondere das Internet von Anfang an und in wachsendem Maße für militärische Zwecke genutzt wurden und werden, hat das FIfF die Cyberpeace-Kampagne gestartet. Die Hauptforderungen sind: die Ächtung jeglicher Form von Cyberkrieg und ein demokratisch gestaltetes und demokratisch kontrolliertes Internet, das dem Frieden dient, nicht der Ausspähung und Kriegsführung. Nähere Informationen findet man auf der Kampagnen-Webseite *https://cyberpeace.fiff.de/Kampagne/Home/*.

Im Zuge der Kampagne sind Tausende Aufkleber mit der Cyberpeace-Taube verteilt, viele Vorträge gehalten, viele Publikationen entstanden und viele Veranstaltungen durchgeführt worden, von zweistündigen Cyberpeace-Cafés bis zu zweitägigen Cyberpeace-Foren. Sehenswert ist der Kurzfilm *Cyberpeace statt Cyberwar!* von Alexander Lehmann, der mit Hilfe der bridge-Stiftung finanziert werden konnte. Und die Cyberpeace-Taube ist inzwischen zum FIfF-Logo geworden. Die Cyberpeace-Kampagne ist eine Erfolgsgeschichte.

Auf der FIfF-Klausurtagung Ende März diesen Jahres haben die Teilnehmenden verabredet, der Kampagne neuen Schwung und noch mehr Sichtbarkeit zu verleihen. Als ein wesentliches Element ist dabei an eine thematische Ausweitung gedacht: über Cyberpeace als Gegenkonzept zu Cyberkrieg hinaus. In gewisser Weise kann man Cyberpeace auch als Synonym für FIfF verstehen, denn „Cyber" deckt alles ab, was mit Informatik und Information- und Kommunikationstechnik zu tun hat, und „Peace" steht ja ohnehin für Frieden, womit nicht nur Abwesenheit von Krieg gemeint ist, sondern auch Abwesenheit von Unterdrückung und prekären Lebensverhältnissen. Die Cyberpeace-Kampagne richtet sich dementsprechend gegen alle Militär- und Waffensysteme, die auf Informations- und Kommunikationstechnologie basieren, gegen die Einschränkung von Grund- und Menschenrechten durch Überwachungssysteme und gegen die Zerstörung von Natur und Umwelt, an der auch der Einsatz von Technik einen gehörigen Anteil hat. Positiv ausgedrückt: geht es darum, wie die Methoden und Technologien der Informatik genutzt werden können, um friedliche, freiheitliche und faire Lebensbedingungen für alle Menschen auf der Grundlage eines nachhaltigen Wirtschaftssystems zu schaffen – eine lebenswerte Welt.

Die neue Rubrik ist gedacht für Ankündigungen, Berichte, kurze Texte und Stellungnahmen rund um das Thema Cyberpeace. Alle Leser:innen sind aufgerufen, die Rubrik für eigene Beiträge zu nutzen. Sie können jederzeit an uns geschickt werden: kreo@fiff.de und lye@fiff.de.

In dieser ersten Ausgabe folgen drei Mitteilungen: (1) KI zieht in den Krieg, (2) Eurodrohne und FCAS, (3) Kampagne Heimatland Erde sowie (4) The Pegasus Project.

(1) Künstliche Intelligenz zieht in den Krieg – Aufruf zur Einreichung von Beiträgen

In ihrer KI-Strategie von 2018 verkündet die Bundesregierung, dass sie Künstliche Intelligenz umfassend fördern will, damit in nahezu allen Bereichen von Staat und Wirtschaft durch KI-Anwendungen große Fortschritte erzielt werden können. Mehrfach wird betont, dass die Nutzung von KI verantwortungsvoll und am Gemeinwohl orientiert erfolgen soll. Anwendungen im militärischen Bereich werden nur am Rande vermischt mit Fragen der inneren Sicherheit erwähnt. KI-basierte Waffentechnik kommt überhaupt nicht vor. Tatsächlich aber wird in Politik, Militär und Wissenschaft weltweit die Entwicklung und die Anwendung von KI-Methoden und KI-Technologien für militärische Zwecke einschließlich Waffensysteme vorangetrieben: KI zieht in den Krieg.

Unter dieser Überschrift soll in zwei geplanten FIfF-Publikationen die Rolle von Künstlicher Intelligenz im militärischen Bereich vorgestellt, diskutiert und hinterfragt werden:

- Ein 16-seitiges Dossier mit sechs bis acht Beiträgen, das dem Heft 4/2021 von Wissenschaft und Frieden beigelegt werden soll.
- Ein 30- bis 40-seitiger Schwerpunkt in der FIfF-Kommunikation 4/2021 mit zehn bis zwölf Beiträgen.

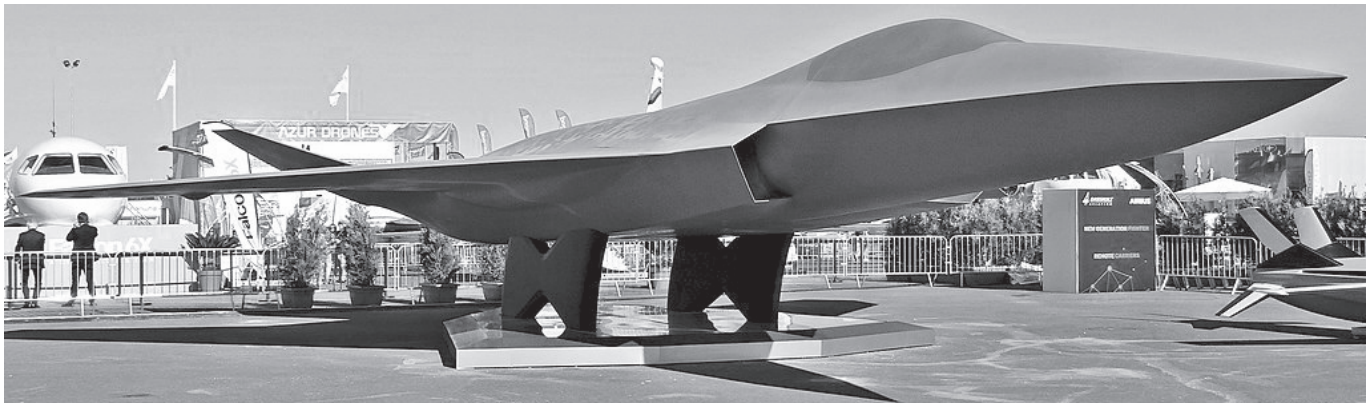
Die Sammlung von Beiträgen für das Dossier ist bereits abgeschlossen. Die Beiträge für den Schwerpunkt mit 15.000 bis 20.000 Zeichen müssen bis Ende Oktober 2021 vorliegen.

Diese Ausschreibung wurde bereits Anfang Mai mit Einreichungsschluss 25. Mai 2021 über Mailinglisten verteilt. Angebote von Kurzentschlossenen können aber immer noch an *kreo@fiff.de* und *lye@fiff.de* geschickt werden, je bitte mit Angabe der Autor:innen, einem Titel und einer kurzen Inhaltsangabe von fünf bis zehn Zeilen. Wir werden versuchen, solche Angebote noch im Schwerpunkt unterzubringen.

(2) Eurodrohne und FCAS

Die Bewaffnung der geleasten Bundeswehr-Drohnen vom Typ Heron TP ist im Dezember 2020 am Veto der SPD-Fraktion vorläufig gescheitert. Ein kleiner Sieg der Vernunft. Das heißt aber noch lange nicht, dass es auch zukünftig dabei bleibt. Mehr noch steht die Frage der Bewaffnung dann bald auch für die Eurodrohne an. Ihre Entwicklung läuft seit einiger Zeit unter Leitung von Airbus als europäisches Projekt mit Deutschland, Frankreich, Italien und Spanien. Auch der Kauf von 21 Eurodrohnen für die Bundeswehr ist bereits beschlossene Sache. Das Projekt wird den deutschen Steuerzahler:innen viele Hunderte Millionen Euro kosten. Die Eurodrohne ist als Aufklärungsdrohne konzipiert, die auch bewaffnet werden kann. Mit der Auslieferung der ersten Exemplare an die Bundeswehr wird zum Ende dieses Jahrzehnts gerechnet. Europa soll mit der Eurodrohne unabhängig von nichteuropäischen Systemen werden und so auch militärisch souveräner. Durch europäische Zusammenarbeit sollen auch Kosten gespart werden, die durch den Verzicht auf solche Drohnen gar nicht erst entstünden. Die Bundeswehr wünscht sich bewaffnete Drohnen. CDU und CSU sind auch schon lange dafür. Die SPD macht erklärtermaßen ihre zukünftige Haltung davon abhängig, wie ein umfassender gesellschaftlicher Diskurs zum Für und Wider der Drohnenbewaffnung ausgeht. Eigentlich ist aber längst klar, dass sehr viel gegen solche Waffensysteme spricht. Dabei spielt es keine Rolle, ob sie bewaffnet oder unbewaffnet sind. Denn wenn eine Aufklärungsdrohne ein anzugreifendes Ziel „aufklärt" und andere Waffensysteme es zerstören, ist der Unterschied zu einer Drohne, die selbst schießt, marginal. Sie sind alle Killerdrohnen, die bisher tausendfach völkerrechtswidrig für gezielte Tötungen und mit Tausenden ziviler Opfer eingesetzt wurden. Auch der Einsatz türkischer Killerdrohnen durch Aserbaidschan im Krieg gegen Armenien im Herbst letzten Jahres war völkerrechtswidrig, weil Aserbaidschan angegriffen hat. Die Führung der Bundeswehr behauptet, dass sie Killerdrohnen nie völkerrechtswidrig einsetzen will. Das Gegenteil wäre ja auch hochgradig merkwürdig. Die Bundeswehr bleibt allerdings eine klare und überzeugende Antwort schuldig, wie sie diese Waffen stattdessen einsetzen will.

Noch wahnwitziger ist ein zweites europäisches Rüstungsprojekt, an dem sich vorläufig Deutschland, Frankreich und Spanien beteiligen und das gerade auf den Weg gebracht wird: das *Future Combat Air System* (FCAS). Im Zentrum steht die Entwicklung eines neuen Kampfflugzeugs, das ab 2040 die dann völlig veralteten Eurofighter und Rafale ablösen soll. Das Projekt umfasst aber weit mehr. Es soll ein System von Systemen werden, bei dem Kampfjets zusammen mit Lenkflugkörper- und Drohnenschwärmen in einer Weise eingesetzt werden sollen, die Europa in allen Teilen der Welt die Überlegenheit im Luftkampf sichert. Was sind das für Kriege, die Europa in der zweiten Hälfte des Jahrhunderts führen möchte und gegen welche Kriegsgegner? Aber nicht nur alle friedliebenden Menschen muss dieses gigantomanische Projekt, dessen Kosten im dreistelligen Milliardenbereich liegen wird, zutiefst erschrecken, sondern alle Informatiker:innen haben einen besonderen, fachbezogenen Grund, schockiert zu sein. Als methodisches und technologisches Kernstück von FCAS ist die Künstliche Intelligenz auserkoren. Es ist bisher noch ziemlich unklar, woran dabei im Einzelnen



Model of the Future Air Combat System (FCAS) at the Paris-Le Bourget 2019 Airshow

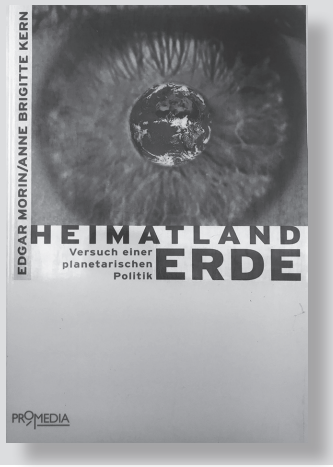
gedacht ist. Aber umso wichtiger ist, die Entwicklung mit großer Aufmerksamkeit zu verfolgen und einen wirkungsvollen Widerstand aufzubauen. FCAS muss verhindert werden.

Eine ausführliche Darstellung von FCAS findet man im Informationsbericht des französischen Senats: *http://www.senat.fr/rap/r19-642-3/r19-642-31.pdf*.

Eine erste kritische Analyse von Jürgen Wagner ist unter dem Titel *Future Combat Air System – Das größte Rüstungsprojekt Europas* als IMI-Studie 2021/4 erschienen: *https://www.imi-online.de/2021/07/13/future-combat-air-system-2/*.

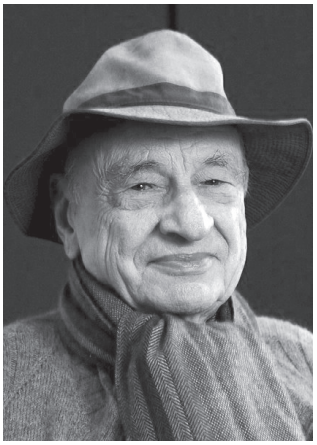
(3) Kampagne *Heimatland Erde*

Das Österreichische Studienzentrum für Frieden und Konfliktforschung (ASPR) hat die Kampagne *Heimatland Erde* zur Förderung des planetaren Bewusstseins gestartet. Das FIfF ist eine von über 50 Kampagnen-Partnerorganisationen aus aller Welt und dort in guter Gesellschaft.



Edgar Morin
Heimatland Erde.
Versuch einer planetarischen Politik
Promedia 1999
240 Seiten
Preis € 17,90 (brosch.)
ISBN: 978-3-85371-139-2

Die Menschheit steht neben der Eindämmung der Covid-19-Pandemie vor vielen weiteren globalen Herausforderungen. Hunger und Armut in der Welt sind gewachsen. Die Zahl der Flüchtlinge ist größer geworden, wobei die meisten von ihnen unter elenden Bedingungen und ohne jede Perspektive in Flüchtlingslagern hausen. Dagegen sind viele Reiche in schamloser Weise noch reicher geworden. Auch die Zahl der Kriege hat zugenommen. Die Bemühungen, den einen oder anderen Krieg zu beenden, sind kläglich. Echte Friedensverhandlungen, die zu einem fairen Interessenausgleich der verfeindeten Parteien und so zu dauerhaftem Frieden führen könnten, stehen nirgendwo auf der Tagesordnung. Die nationalen und internationalen Bemühungen, den menschengemachten Klimawandel und die Zerstörung von Natur und Umwelt zu stoppen, sind weit hinter den Erfordernissen zurückgeblieben. Die Menschheit ist dabei, sich ihrer Lebensgrundlagen zu berauben. Unterdrückung, Ausbeutung, Machtmissbrauch, Menschenrechtsverletzungen, Hass und Gewalt sind in vielen Teilen der Welt Alltag. Keines dieser Probleme lässt sich durch nationale Alleingänge lösen. Das geht nur durch gemeinsames weltweites Handeln auf globaler Ebene beim Überwinden der Ursachen. Das ist mit Heimatland Erde gemeint. Ziel der Kampagne ist, das Bewusstsein zu stärken, dass alle Menschen die Erde als Lebensraum teilen, dass es keine Alternative dazu gibt und dass die Menschheit nur überleben kann, wenn sie ihren Lebensraum nicht zerstört.



Edgar Morin 2011
Fronteiras do Pensamento, CC BY-SA 2.0

Mit der Kampagne wird der französische Philosoph Edgar Morin geehrt, der am 8. Juli 2021 seinen 100. Geburtstag feiert, in seinem 1993 erschienenen Buch *Terre Patrie*, das 1999 unter dem Titel *Heimatland Erde – Versuch einer planetarischen Politik* in deutscher Übersetzung publiziert wurde, hat er das Konzept entwickelt, das der Kampagne zugrundeliegt. Mehr Informationen findet man auf der Kampagnen-Webseite unter *https://www.heimatlanderde.com/* mit dem Kampagnenaufruf, dem Kampagnenmanifest, einem Videoaufruf von Edgar Morin und einer kurze Biographie des Philosophen. Auf der Webseite werden auch Mitmachmöglichkeiten aufgezählt. So kann man den Aufruf unterzeichnen, mithelfen, die Kampagne bekanntzumachen, oder sich an der Bastelaktion von Passhüllen für Erdenbürger:innen beteiligen. Insbesondere lud das Studienzentrum ASPR auch zu seiner 37. Sommerakademie zum Thema *Heimatland Erde – Friedenspolitik im Zeitalter des Anthropozäns* ein, die vom 1. bis 5. September 2021 online stattfand.

(4) The Pegasus Project: Ein Kommentar

Pegasus ist eine Schadsoftware/Malware, die vor allem iPhones und Android-Geräte infiziert. Sie ermöglicht es den Betreiber:innen des Tools, Daten wie beispielsweise Nachrichten in diversen Messengern, nachdem sie entschlüsselt wurden, aufgerufene Websites, Fotos und E-Mails oder auch Standort-Metadaten von dem Gerät zu extrahieren. Pegasus vermag Anrufe aufzuzeichnen, heimlich Mikrofon und/oder Kamera zu aktivieren oder auch beliebige Daten nachzuladen. Produziert wird die Software von der israelischen Firma NSO Group. Sie gehört zu den führenden Herstellern kommerzieller Spionagesoftware. Das Unternehmen verkauft weltweit Produkte an Militär, Strafverfolgungsbehörden und Geheimdienste und hat ca. 60 Kunden in 40 ungenannten Ländern.

Viele der Kunden nehmen Journalist:innen, Menschenrechtsverteidiger:innen, politische Gegner, Geschäftsleute und Staatsoberhäupter als Ziele dieser Software. Seit einigen Jahren ist die Software in der Presse. Kürzlich war das erneut der Fall. Mindestens 180 Journalist:innen in 20 Ländern wurden gezielt mit dieser Schadsoftware von mindestens 10 NSO-Kunden angegriffen. Dies geht einer Mitte Juli veröffentlichten Recherche des Pegasus-Projekts hervor, eines globalen Konsortiums von mehr als 80 Journalist:innen aus 17 Medien in zehn Ländern, die von Forbidden Stories mit technischer Unterstützung des Security Lab von Amnesty International koordiniert wurde.

Forbidden Stories und Amnesty International hatten Zugang zu mehr als 50.000 Datensätzen von Telefonnummern, die von NSO-Kunden zur Überwachung ausgewählt wurden. Die Telefonnummern, die möglicherweise im Vorfeld eines Überwachungsangriffs ausgewählt wurden, verteilten sich auf mehr als 45 Länder auf vier Kontinenten. Die Analyse der durchgesickerten Daten durch das Konsortium ergab, dass es sich bei mindestens zehn Regierungen um NSO-Kunden handelt, die Nummern in ein System eingegeben haben: Aserbaidschan, Bahrain, Indien, Kasachstan, Mexiko, Marokko, Ruanda, Saudi-Arabien, Ungarn und die Vereinigten Arabischen Emirate. Aus der Analyse der Daten geht hervor, dass Mexiko die meisten Nummern ausgewählt hat (mehr als 15.000). Von Mexiko ist seit 2017 bekannt, dass verschiedene Regierungsbehörden Pegasus gekauft und gegen Journalist:innen eingesetzt haben. Die Analyse der Daten zeigt, dass sowohl Marokko als auch die Vereinigten Arabischen Emirate mehr als 10.000 Nummern auswählten und mehr als 1.000 Nummern in europäischen Ländern ebenfalls von NSO-Kunden ausgewählt wurden. Neu ist nicht, dass die oben genannten Gruppen systematisch beobachtet werden. Aber es ist zweifelsohne wichtig, die Dimension und Techniken aufzuzeigen.

Eva Galperin, die Leiterin für Computersicherheit bei der Electronic Frontier Foundation (EFF), war eine der ersten Sicherheitsforscher:innen, die Anfang der 2010er Jahre Angriffe auf Journalist:innen und Menschenrechtsverteidiger:innen in Mexiko, Vietnam und anderswo identifizierte und dokumentierte. Seit diesen Anfängen ist die Installation von Spyware auf Smartphones subtiler geworden. Anstatt dass die Zielperson auf einen Link klicken muss, um die Spyware ungewollt zu installieren, ermöglichen sogenannte Zero-Click-Exploits, die Kontrolle über das Telefon zu übernehmen, ohne dass die Zielperson etwas tun muss. Dazu reicht es, die Telefonnummer zu kennen, um über das Netz anzugreifen. Ein physischer Zugriff vor Ort ist nicht nötig. Dass NSO bei Pegasus Zero-Click-Exploits einsetzt, ist seit spätestens 2015 bekannt. Die WikiLeaks Publikation Spy-Files belegt dieses mit geleakten internen E-Mails.

Bemerkenswert an der aktuellen Recherche ist neben der großen Anzahl auch, dass selbst (relativ) aktuelle iOS- und Android-Versionen betroffen sind. Folglich sind selbst Menschen, die sich der Problematik bewusst sind und Sicherheitsupdates einspielen, trotzdem angreifbar.

Die Konsequenz darf allerdings nicht Resignation sein. Vielmehr müssen wir uns erneut die Frage stellen, wie wir dem Problem individuell, als Informatiker:innen und als Gesellschaft begegnen.

Apple und Google haben kein Interesse daran, sichere Betriebssysteme zu entwickeln. Selbstverständlich haben sie Abteilungen, die sich mit den Angriffen und Gegenmaßnahmen beschäftigen. Allerdings ist der Druck von Regierungen, die immer wieder Hintertüren fordern, groß und es besteht bei den Konzernen ein großes Interesse, daran zu kooperieren.

Außerdem sind die Anreize, Exploits (auf dem Schwarzmarkt) zu verkaufen, größer als sie Software-Produzenten zu melden, damit die Sicherheitslücken geschlossen werden können. Dieses Geschäftsmodell als solches wird von Staaten befürwortet, da diese ja selbst Exploits kaufen (lassen) um Systeme anzugreifen.

Das Framing der Rechercheergebnisse, dass die Überwachungssoftware der israelischen Firma, die vermeintlich ja sonst nur für staatstragende Zwecke von Strafverfolgungsbehörden, Geheimdiensten und Militärs genutzt wird, jetzt von autoritären Staaten zweckentfremdet wird, ist ein Zerrbild der Realität und erweckt den Eindruck, dass es sich nicht um unser Problem handelt.

Auch deutsche Behörden sind Kunden der Überwachungsindustrie. Seit 2007 ist der Einsatz von kommerzieller Spionagesoftware bei Strafverfolgungsbehörden bekannt. Das bekannteste Beispiel ist das Produkt FinSpy von FinFisher, welches seit 2013 vom BKA eingekauft wird. Ständig werden die Befugnisse von Polizei und Geheimdiensten hierzulande ausgeweitet. Erst kürzlich hat eine Gesetzesverschärfung den Trojanereinsatz für allen 19 Geheimdienste legalisiert.

Wir alle wissen, dass Journalist:innen Informationen bekommen, an denen Geheimdienste ebenfalls interessiert sind und auch, woher diese stammen. Insbesondere, wenn es sich um undichte Stellen in der Regierung oder in einem für die Regierung wichtigen Unternehmen handelt. Wir wissen aus der Vergangenheit, dass Überwachung von Journalist:innen auch in der Bundesrepublik kein Tabu ist.

Die Weltöffentlichkeit kennt spätestens seit den Snowden-Enthüllungen das Ausmaß staatlicher Überwachung insbesondere der FiveEyes, aber auch anderswo. Die Repression gegen WikiLeaks und Assange zeigen die Konsequenz von nonkonformem Journalismus auf. Vielerorts werden Journalist:innen verschleppt und umgebracht. Das Bekanntwerden der Dimension der systematischen Überwachung von Journalist:innen ist ein harter Schlag für kritische Journalist:innen weltweit und schafft ein toxisches Klima bezüglich der Sicherheit und Vertraulichkeit von Quellen.