Christoph Marischka

KI und der Risiko-Kapital-Staat

Das Ökosystem der V2

Unter dem Titel *Peenemünde – Die Geschichte der V-Waffen* beschreibt Walter Dornberger die Entstehung und den Betrieb jener Heeresversuchsanstalt, welche er als Generalmajor der deutschen Wehrmacht kommandiert hat. Wenn der Ort sich heute als „Wiege der Raumfahrt" darstellt, so blendet dies zwar den primären Zweck und die unmittelbare Wirkung der dortigen Entwicklung – eine Revolutionierung und Entgrenzung der Kriegführung – aus, ist aber sachlich auch richtig. Wie der technische Leiter der Versuchsanstalt, Wernher von Braun und auch dessen Stellvertreter, Eberhard Rees, ging Dornberger nach der bedingungslosen Kapitulation der deutschen Wehrmacht in die USA und war dort weiter in der Raketenentwicklung für die NASA und die Rüstungsindustrie tätig. Rees schreibt in seinem Geleitwort zum oben genannten Buch, dass sowohl „die russischen Sputnik-Satelliten Ende der fünfziger Jahre" als auch „die amerikanische Explorer-Serie […] mit Raketen in eine Umlaufbahn um die Erde gebracht [wurden], die auf der Technologie des A4, also der Rakete V2 basierten."[1]

Dornberger beschreibt in seinem Buch ausführlich, wie über Jahre verschiedene Raketenöfen in verschiedenen Versuchsständen erprobt, unterschiedliche Materialien und Anordnungen, unterschiedliche Treibstoffe, Mischungsverhältnisse, Methoden der Einspritzung, Zerstäubung, Kühlung, Stabilisierung, Steuerung usw. ausprobiert wurden. Technologie-Entwicklung ist eben keine (reine) Wissenschaft, sondern auch ein ständiges Versuchen und Scheitern. Dazu wurde auf der Versuchsanstalt eine umfassende Infrastruktur geschaffen mit eigenen Kraftwerken, Flughäfen, Messständen, Windkanal, Fertigungsstätten, Sauerstoffwerk, KZ-Außenlagern, Fernwärmeleitungen und der dritten S-Bahn in Deutschland. Darüber hinaus waren neben der Wehrmacht (Heer und Luftwaffe) sowohl führende Unternehmen wie AEG, Siemens usw. eingebunden, als auch kleine und mittelständische Unternehmen, die einzelne Komponenten (z. B. Raketenöfen, Messgeräte, Stabilisierungskreisel, Brems- und Fallschirme) lieferten, für die es sonst kaum einen oder noch gar keinen Markt gab. Auch an verschiedenen Universitäten wurden Einzelkomponenten entwickelt und Modelle entworfen. Heute würde man dies ein *Ökosystem* nennen. Eher am Rande spricht Dornberger auch von „Angebern, Scharlatanen und Semiwissenschaftlern", welche „mit Übertreibungen und Phantasieangaben operierten", um sich auf dem Feld zu etablieren.

KI-Ökosysteme

In der sogenannten *Künstlichen Intelligenz* werden aktuell auf verschiedensten Feldern massive Fortschritte versprochen und erwartet, unter anderem im Gesundheitswesen, der Landwirtschaft, der Energieversorgung, der *Mobilität der Zukunft* und natürlich und vor allem auch der Konsumgüterindustrie und der Unterhaltungselektronik. Im Bereich der *Inneren Sicherheit* kommen KI-Verfahren bereits unter anderem bei der Visa-Vergabe, der Gesichtserkennung an Grenzübergängen, bei der Überwachung von Sammelunterkünften und im Asylverfahren (z. B. KI-gestützte Dialekterkennung) zur Anwendung.[2] Auch die Streitkräfte weltweit erwarten sich von KI künftig massive Vorteile in unterschiedlichsten Bereichen. Diese reichen von der automatisierten Lagerlogistik und vorausschauenden Wartung, der medizinischen Versorgung und autonomen Transportsystemen über die Entscheidungsunterstützung auf strategischer (z. B. Krisenfrüherkennung durch „Beobachtung" sozialer Netzwerke) und taktischer (sogenannte *combat clouds*) Ebene, die sogenannte Strategische Kommunikation (*Chat-Bots* zur Rekrutierung, Erkennung von *Fake News*), die Erkennung von Cyber-Angriffen bis hin zur Zielerkennung und zu autonomen Waffensystemen und Schwärmen.[3]

Es besteht somit ein breites Interesse in verschiedenen politischen und industriellen Kreisen zur (Weiter-)Entwicklung Künstlicher Intelligenz. Anders als in Peenemünde, wo die konkreten Spezifika (Maße und Transportfähigkeit, Reichweite, *Nutzlast* in Form von Sprengladung usw.) des A4 bzw. der V2 früh definiert waren, ist dieses Interesse bislang relativ unspezifisch. Es soll einfach an KI geforscht und in KI und entsprechendes Humankapital investiert werden. Wo sich dann tatsächlich Vorteile hieraus gewinnen lassen oder tatsächlich *Disruptionen* entstehen werde sich dann zeigen – und zwar in Form marktfähiger Produkte, die auf eine Nachfrage treffen bzw. diese generieren. Hierbei sollen Startups und mit ihnen verbunden Risikokapital eine zentrale Rolle spielen. Das gilt für zivile Märkte ebenso wie den Rüstungsmarkt. Entsprechende Maßnahmen, Institutionen und Strukturen, die zur Schaffung eines entsprechenden Ökosystems beitragen können und sollen, werden im folgenden anhand einiger Beispiele dargestellt.

Das Programm der letzten Bundesregierung

Bereits das Programm der letzten (schwarz-roten) Bundesregierung war vor allem auch ein technologiepolitisches Programm, welches unter der Chiffre der *Digitalisierung* und *Künstliche Intelligenz* für verschiedene gesellschaftliche Probleme (wie das Gesundheitssystem, Pflegenotstand, Klimawandel) technologische Lösungen in Aussicht stellte. Um schnell zu marktfertigen Produkten zu kommen, waren quer durch verschiedene Politikbereiche verschiedene Maßnahmen vorgesehen. Bereits in der einleitenden Zusammenfassung unter dem Titel *Eine neue Dynamik für Deutschland* werden unter anderem *„[s]teuerliche Forschungsförderung"* und „eine Allianz für schnelleren Transfer von Forschungsergebnissen in marktfähige Produkte" angekündigt. Hierfür war unter anderem vorgesehen, „Forschungscampi aus[zu]bauen", in „ausgewählten Forschungsfeldern […] starke Anreize für die Zusammenarbeit der Forschungs- und Wissenschaftseinrichtungen [zu] setzen", „Konzepte für Zukunftscluster [zu] entwickeln und um[zu]setzen sowie rechtliche Barrieren für Wissenschaftskooperationen ab[zu]bauen". Auch sollte „die direkte Forschungsförderung des Bundes stärker auf den Wissens- und Technologietransfer in die Wirtschaft [ausgerichtet]" werden. Außerdem wurden „neue

Instrumente zur Förderung von Sprunginnovationen“ sowie – unter der Überschrift *Für eine modern ausgerüstete Bundeswehr* – die Gründung einer *Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien* angekündigt.

Als zentrale Elemente der angestrebten Anwendung von Forschung in Produkten werden auch hier Startups hervorgehoben, zu deren Förderung ebenfalls ein breites Maßnahmenbündel vorgesehen war, unter anderem, indem man „den Zugang zu der Forschungsförderung für Startups deutlich erleichter[t]“, „Startups und Gründungen aus der Forschung“ fördert und sich auf europäischer Ebene für „eine einheitliche Europäische Startup Definition einsetz[t], um spezielle zielgenaue Fördermaßnahmen zu ermöglichen“ und „Rahmenbedingungen [schafft], die Unternehmen und Startups eine unbürokratische Skalierung von digitalen Geschäftsmodellen ermöglich[en]“. Zu Startups im High-Tech-Bereich gehört jedoch auch viel Risikokapital. Das wusste auch die Bundesregierung und hielt im Koalitionsvertrag fest: „Wir brauchen in Deutschland eine deutliche Ausweitung des Volumens des Wagniskapitalmarktes, um insbesondere Unternehmen in der Wachstumsphase zu unterstützen“. Hierzu kündigte man an, „die Bedingungen für Wagniskapital weiter [zu] verbessern“, unter anderem durch eine Vereinfachung von „Besteuerungsverfahren“ und die „Einführung steuerlicher Anreize zur Mobilisierung von privatem Wagniskapital über die bisherigen Maßnahmen hinaus“. Darüber hinaus wollte man auch mehr „institutionelle Anleger für Investitionen in Startups“ mobilisieren und hielt fest: „An diesen Wagniskapitalfinanzierungen sollen sich Privatwirtschaft, öffentliche Hand, KfW [Kreditanstalt für Wiederaufbau] und europäische Finanzpartner beteiligen.“

Damit hat der Koalitionsvertrag wesentliche Forderungen übernommen, welche während der Koalitionsverhandlungen im Oktober 2017 in einer gemeinsamen Stellungnahme von Spitzenverbänden der Industrie und Forschung unter dem Titel *Wissenschaft und Forschung als Fundament unserer Zukunft weiter stärken* veröffentlicht wurde.[4] Kurz nach der Veröffentlichung dieser Stellungnahme wendete sich Max-Planck-Präsident Martin Stratmann unter dem Titel *Der Staat muss auch riskante Projekte fördern* über den Tagesspiegel an die Öffentlichkeit. Darin warb er für die Einrichtung einer Agentur nach dem Vorbild der Forschungsförderung des Pentagon: „Es lohnt ein Blick in die USA: Dort werden solche Innovationsprojekte über die Defense Advanced Research Projects Agency (DARPA) sehr wirkungsvoll umgesetzt. So hat DARPA maßgeblich das Internet entwickelt und die Kommerzialisierung des Positionsbestimmungssystems GPS ermöglicht. Voraussetzung für den Erfolg: Autonomie, Verzicht auf politische Steuerung, Rekrutierung herausragender Projektmanager, und: eine Kultur, die Scheitern gestattet und damit die Voraussetzung schafft für den eigentlichen Erfolg. Auch wir sollten mehr die Chancen im Risiko sehen!“[5]

Sowohl die gemeinsame Stellungnahme als auch Stratmann im Tagesspiegel betonen zwar die Bedeutung von Startups bzw. „hoch risikoreiche[r] Projekte und Geschäftsmodelle“, schweigen aber weitgehend zur impliziten Rolle von Risikokapital und den hierfür zu schaffenden Rahmenbedingungen. Umso mehr hervorgehoben wird diese hingegen in einer Publikation unter dem Titel *Artificial Intelligence – A strategy for European startups*, welche die „Unternehmensberatung“ Roland Berger gemeinsam mit dem Risikokapitalfonds Asgard 2018 veröffentlicht hat. Um eine zur USA und China wettbewerbsfähige Position zu erlangen, solle die europäische Politik Startups als wichtigste technologische und wirtschaftliche Triebkräfte der KI fördern. „Dies erfordert eine tiefgreifende Änderung der Form des öffentlichen Engagements im Innovationsökosystem und die Anpassung von Förderprogrammen speziell für Startups.“ Gefordert werden auch hier (auf europäischer Ebene) Steuererleichterungen für Forschung und Risikokapital, die Einrichtung einer Agentur nach dem Vorbild der DARPA und umfangreiche öffentliche Investitionen in riskante Investitionen. Vor allem aber zielt das Papier auf Maßnahmen ab, die öffentliche Mittel als Hebel und Absicherung für private Investitionen wirken lassen sollen: „Europa hat keine andere Wahl, als seine Finanzierungsquellen für Innovationen massiv zu diversifizieren und private Beteiligungsfonds, Investmentbanken, Pensionsfonds und Staatsfonds einzubeziehen.“[6]

Cyber-Agentur und SprinD

Den seit Jahren immer wieder erhobenen Forderungen nach einer deutschen DARPA kam die Bundesregierung, wie im Koalitionsvertrag angekündigt, nach. Einerseits gründete sie im gemeinsamen Verantwortungsbereich des Innen- und des Verteidigungsministeriums die sogenannte Cyber-Agentur als bundeseigene GmbH mit Sitz in Halle (Saale).[7]

Laut einem Bericht des im Verteidigungsministerium angesiedelten Aufbaustabs der Agentur besteht deren Aufgabe in der „zielgerichtete[n], am Bedarf der inneren und äußeren Sicherheit orientierte[n] Beauftragung“ von „Forschungseinrichtungen durch staatliche Einrichtungen“. Hierzu „analysiert“ sie die „Innovationslandschaft“. Nach den Worten des Gründungsdirektors Igel soll sie „Forschung stimulieren und koordinieren“: „Es geht um Forschungsfragen, die zum Beispiel das Bundeskriminalamt, die Bundespolizei, die Marine, die Luftwaffe haben könnten.“ Als Handlungsfelder identifizierte der Aufbaustab „unter anderem die Quantentechnologie, Künstliche Intelligenz oder alternative Rechnerarchitekturen“. Konkreter benannt werden unter anderem „DNA-basierte“, „organisch-elektrochemische“ sowie „neuromorphe und neuronale Architekturen“. Konkret werden auch „Autonomie und Entscheidungsfindung“ und „Lagebilder und Lagebilddarstellung“ sowie Sensorik als Forschungsthemen genannt. „[A]bhängig vom Schwerpunkt des spezifischen Programms“ ist dabei vorgesehen, dass die Agentur „Programmbüros an anderen Standorten in Deutschland“ einrichtet. „Dabei handelt die Cyberagentur bewusst als Wagniskapitalgeber und schließt nicht aus, dass sich manche beauftragten Forschungen und Entwicklungen als Irrweg erweisen.“

Parallel hierzu wurde im benachbarten Leipzig, ebenfalls als bundeseigene GmbH, die „Bundesagentur für Sprunginnovationen“ (SprinD) gegründet. Gründungsdirektor Rafael Laguna de la Vera, der selbst als Investor und Unternehmer tätig war, beschreibt deren Aufgabe so: „Wir nehmen die Projekte, die zu groß und zu riskant sind, wo ein normaler Finanzinvestor vielleicht nicht gut beraten ist, zu investieren. Wir entwickeln sie zu einem Grad, wo dann Business Angels [Finanzinvestoren] auch einsteigen können und auch sollen.“

Künstliche Intelligenz in den Landstreitkräften

2019 veröffentlichte das Amt für Heeresentwicklung ein *Positionspapier* zum Thema *Künstliche Intelligenz in den Landstreitkräften*. Es stellt ein Ergebnis des Formats *Technology meets Capabilities* dar, einer Workshopreihe, die dem Austausch zwischen dem Heer, „der Forschung und der Industrie" dienen soll. In ihm werden nicht nur fünf zentrale *Handlungsfelder* (Anwendungsbereiche von KI) benannt (Bildanalyse, taktische unbemannte Systeme, Führung, Material und Infrastruktur, Analyseverfahren), sondern auch sechs *Treiber* (T1-T6), die „nicht beeinflusst oder vermieden werden" könnten – Sachzwänge sozusagen, die im wesentlichen mit wachsendem Tempo und Datenmengen begründet werden und damit, wie sie potentiellen Feinden Vorteile verschaffen könnten (die man als Bundeswehr stattdessen lieber selbst realisieren will). Die grundsätzliche Logik wird bereits als T[reiber]1 dargestellt: „Ein gegnerischer Einsatz von KI-basierten Komponenten kann zu Fähigkeitslücken des Heeres führen." Jede antizipierte Fähigkeit des Gegners sollte also zuvor selbst erlangt werden oder es sollten zumindest Abwehrmechanismen zur Verfügung stehen.

Unter T2 (*Zunehmende Dynamik des Gefechtes*) wird antizipiert, dass KI dazu beitrage „in Gefechten mit erhöhter Dynamik schneller, zielgerichteter und effektiver führen und agieren zu können" während T5 (*Zunehmende Informationsmenge und -dichte*) unterstellt, „KI erlaubt eine möglichst effektive und effiziente Nutzung von Information und sichert somit die Informations- und Führungsüberlegenheit beim Umgang mit einer hohen Menge von Daten unter hohem Zeitdruck". T6 (*Zunehmende Dynamik in der IT-und KI-Entwicklung*) wirkt zunächst eher als Wiederholung von T1, nämlich dass „Rüstungskonzerne potentieller Gegner an der Entwicklung KI-gestützter Waffensysteme arbeiten […]. Die sich daraus ergebende Erosion eigener Fähigkeiten führt über die Zeit zu einer deutlichen Bedrohungszunahme." Befürchtet und zugleich vorbereitet wird als „zentrales Element der zukünftigen Gefechtsführung" der „Hyperwar", „die Kombination klassischer Gefechtsführung mit Wellen von Cyberangriffen und Angriffen durch große Mengen automatisiert und autonom gesteuerter Systeme".

Es geht also um Tempo bzw. Dynamik und das nicht nur auf dem Schlachtfeld, sondern auch in der Forschung, Entwicklung und Implementierung. „In stark automatisierten und autonomen Systemen definiert sich die Überlegenheit ganz wesentlich über die Qualität der Algorithmen, der Rechenleistung und den Grad der Miniaturisierung […]. Da diese Komponenten praktisch komplett auf Dual-Use beruhen, bestimmt die Geschwindigkeit der zivilen Entwicklungen auch das Tempo des Wettrüstens im internationalen Umfeld."[8]

„Move Fast and Break Things"

Der *Cyber Innovation Hub* (CIH) der Bundeswehr bezeichnet sich als alles mögliche: „Do-Tank", „das digitale Schnellboot für unsere Streitkräfte", „erste militärische digitale Innovationseinheit in Europa", Bindeglied zwischen „agilem Startup-Mindset" und der Bundeswehr. Eingerichtet wurde er schon 2017 – noch unter Verteidigungsministerin von der Leyen im Zuge der Aufstellung des Organisationsbereiches und Kommandos der Bundeswehr für den Cyber- und Informationsraum – in einer Fabriketage in Berlin mit vielen Paletten, Vintage-Möbeln und „Raum für Ideen". Ziel war es explizit, eine Schnittstelle zwischen militärischer Kultur und Denken einerseits und jener Kultur zu schaffen, wie man sie für die Startup-Szene, Entrepreneure und Risiko-Kapitalgeber:innen imaginiert: jung, divers, leger und extravagant. Dieses Spannungsfeld bestimmt auch die Außendarstellung des CIH: Auf der Homepage wird man geduzt und die Bilder von den Veranstaltungen suggerieren ein ungezwungenes Miteinander von Uniformierten und lässig gekleideten Zivilist:innen in bewusst unaufgeräumt und spontan wirkenden Arrangements von Sitzgelegenheiten. Hier darf man auch mal Fehler machen oder zumindest übertreiben, z. B. mit einem auf Facebook veröffentlichten Mime des CIH, welches das Bild eines zugleich fahrenden und schießenden Panzers mit dem Motto von Mark Zuckerberg verband: „Move Fast and Break Things."

Ziel ist es ganz offenkundig, sich an die Startup-Szene anzubiedern und dieser die Bedürfnisse des Militärs mitzuteilen. Auf der anderen Seite sollen auch das Militär und Beschaffungswesen transformiert werden: Weg von komplizierter, hierarchischer und langfristiger Planung, die alle Eventualitäten einbeziehen und jeden Fehler vermeiden will, hin zu flachen Hierarchien, rascher Entscheidungsfindung und Bereitschaft zu Risiken und Scheitern.

Eines der vielen Veranstaltungsformate des CIH ist die sogenannte *Smart Solutions Challenge*. Dabei sind Angehörige der Bundeswehr aufgerufen, Produkte zu entwerfen und anschließend als *Intrapreneure* zu agieren. Umgesetzt wird dies offenbar nach dem Vorbild der Fernsehshow *Die Höhle des Löwen*. Bei der letzten Runde der Challenge wurden aus zunächst 85 Vorschlägen von Angehörigen des CIH und der Bundeswehr-Universitäten elf Projekte ausgewählt, die weiterkamen. Kriterium war hier unter anderem „ob die Projekte schnell zu realisieren

Foto: Stephan Röhl, CC BY-SA 2.0

Christoph Marischka

Christoph Marischka ist Mitglied im Vorstand der Informationsstelle Militarisierung e. V. und aktiv im *Bündnis gegen das Cyber Valley*. Aus seiner Auseinandersetzung mit diesem KI-Forschungscluster ging auch das Buch *Cyber Valley – Unfall des Wissens* hervor.

sind". Anschließend erhielten die dahinterstehenden Teams bzw. *Intrapreneure* vom CIH Unterstützung bei der weiteren Ausarbeitung – darunter Kontakt zu jenen Dienststellen, bei denen eine spätere Verwendung des Produkts möglich wäre – sowie ein *Pitch-Coaching*, um sie auf die Präsentation vor der Jury vorzubereiten. Diese dauerte letztlich drei Minuten, wobei die Jury anschließend noch fünf Minuten Zeit hatte, Nachfragen zu stellen. Als Vertreter:innen der Privatwirtschaft gehörten der Jury Uwe Horstmann (*Founding Partner Project A Venture Capital*), Vera Schneevoigt (*Chief Digital Officer bei Bosch*) und Deepa Gautam-Nigge (*Global Lead SAP Next-Gen Ecosystem*) an. Drei Projekte wurden schließlich ausgewählt und mit „den nötigen Ressourcen" ausgestattet.

Bundeswehrgeneral Alfons Mais, der seine Karriere vor allem bei den Heeresfliegern – unter anderem in Bosnien, Kosovo und Afghanistan – gemacht hat, gab im Juli 2021 dem Handelsblatt ein Interview, in dem er unter anderem „ethische Vorbehalte" im Hinblick auf „Robotik […] verknüpft mit Künstlicher Intelligenz" problematisierte. Das Interview endet mit der Positionierung: „Ich frage die Parlamentarier immer wieder: Wollen Sie sich junge Menschen Europas vorstellen, die zum Beispiel gegen chinesische Roboter kämpfen müssen?". Das im Thesenpapier des Amtes für Heeresentwicklung als T1 eingeführte Argument des Wettrüstens wird auch hier wieder mit dem Anspruch moralischer Überlegenheit ins Feld geführt: „Während wir noch über die ethische Dimension von Künstlicher Intelligenz diskutieren, haben potenzielle Gegner wie zum Beispiel China oder Russland diese Bedenken nicht."

Auch Mais kennt hierfür die Lösung: „Ich bin überzeugt, dass wir auch bei klassischen militärischen Problemen jetzt mit Startups zusammenarbeiten müssen […]. Es dauert einfach zu lange. Militärische Plattformen wie Panzer oder Hubschrauber sind heute fahrende und fliegende Computer. Da sind zehnjährige Innovationszyklen eigentlich nicht mehr akzeptabel […]. In Deutschland sind wir einfach zu risikoavers. Das wäre auch ein Vorteil an Startup-Kooperationen. Startups betreten den Markt schon mit einem anderen Risikobewusstsein, das wir nutzen, unterstützen und auch auf unserer Seite akzeptieren müssen, wenn dabei Ressourcen nicht zum Ziel führen."[9]

The Startup Nation

Mais wirbt auch für das israelische Modell der *Startup Nation*: „Das Militär in Israel beispielsweise hat eine unglaubliche Innovationskraft. Der Druck der permanenten Bedrohung sorgt dafür, dass alles wie in einer Brutkammer viel schneller geht. Und durch das riesige Reservistenkorps ist die Rückkoppelung zur Industrie viel besser." Auch Roland Berger und Asgard verweisen auf die Israel als Vorbild. Hier heißt es unter anderem: „Israel steht weltweit an dritter Stelle, was die Zahl der KI-Startups im Land angeht, und an erster Stelle, was die Zahl der KI-Unternehmen pro Einwohner angeht. Aufgrund von Bedenken hinsichtlich der nationalen Sicherheit wurde ein Schwerpunkt auf KI-Sicherheitsanwendungen gelegt. In der Tat basieren heute 30 Prozent des israelischen Grenzschutzes auf KI-Systemen." Auch die EU-Grenzschutzbehörde Frontex arbeitet mit mehreren Startups zusammen, die aus dem Umfeld des israelischen Militärs entstanden sind. So findet sich unter den sogenannten *Frontex Files* eine Präsentation des Unternehmens Seraphim Optronics, in dem es seine Überwachungssysteme ((M)UGI, (Mini-)Unattended Ground Imaging Sensors) vorstellt. Ein anderes, ebenfalls von ehemaligen Militärangehörigen gegründetes Startup, Windward, hat Frontex Lizenzen seiner Software verkauft, die KI-gestützt Daten aus dem Schiffsverkehr auswerten und Risikobewertungen vornehmen. Beide Unternehmen (und teilweise auch die dahinterstehenden Kapitalfonds) werden in einer Liste mit (aktuell) 67 Unternehmen und Forschungseinrichtungen aufgeführt, die auf unterschiedliche Arten in das EU-Grenzregime eingebunden sind, welche unter dem Titel *Border Business* auf dem Portal *migration-control.info* veröffentlicht wurde.[10] Dabei wird auch klar, dass das israelische Modell gar nicht so einzigartig ist oder zumindest längst Nachahmung findet. So wurde etwa auch das französische Unternehmen A-NSE von einem ehemaligen Vize-Admiral der französischen Marine gegründet und lieferte unter anderem für Frontex Überwachungszeppeline. Gerade im Hinblick auf KI-Anwendungen finden sich auf dieser Liste weitere Startups auch aus anderen Staaten, darunter Travizory Border Security aus der Schweiz, das KI-gestützt und auf Grundlage biometrischer Daten für Flughäfen und Visa-Behörden arbeitet und Reisende kategorisiert. Auch das niederländische Startup *Pandora Intelligence* hat Frontex schon seine Dienste angeboten und beschreibt sich selbst als Lieferant „der neuesten Generation von Analyse-Software für Polizeibehörden, Regierungen und Ministerien, Nachrichtenagenturen und -dienste, militärische Organisationen und Sicherheitsregionen."[11]

Wie auch Windward setzt Pandora Intelligence auf die KI-gestützte Auswertung von öffentlich zugänglichen Daten. Das Feld der Unternehmen, welche entsprechende Anwendungen – nicht nur in den Bereichen Verteidigung und Innere Sicherheit, sondern auch bei Gesundheitsanwendungen, Immobilien- und sonstigen Investitionsfonds – anbieten, ist nahezu unüberschaubar. Absehbar werden zumindest nicht alle die geweckten Erwartungen erfüllen können und dauerhaft Abnehmer finden. Öffentliche Auftraggeber wie Polizeien (oder eben Frontex) und im wachsenden Maße auch das Militär sind beliebte Referenzen, auch wenn sie oft nur kurzfristige Lizenzen im Rahmen der Marktsichtung erwerben. Auch die Zahl der (Risiko-)Kapitalfonds, die sich auf entsprechende Portfolios spezialisiert haben, ist in den vergangenen Jahren deutlich angewachsen. Über gute Kontakte z. B. in die Sicherheitsbehörden (aber auch ins Gesundheitswesen, Verkehrsministerium …) können sie ihren Schützlingen zumindest kurzfristig Aufträge verschaffen. Vieles spricht dafür, dass auch das reichlich dubiose Unternehmen *Augustus Intelligence* ein solches Geschäftsmodell verfolgte. Gegründet wurde es 2019 von einem ehemaligen Mitarbeiter von Roland Berger und Pascal Weinberger, einem Entrepreneur und mutmaßlichen Startup-Multimillionär, der jedoch bereits mehrfach zumindest der Hochstapelei überführt wurde. Aktionär der ersten Stunde und später auch einer der Direktoren war der ehemalige Verteidigungsminister zu Guttenberg; der ehemalige Verfassungsschutzpräsident Maaßen und der ehemalige BNP-Präsident Hanning hatten Aktienoptionen erhalten und wurden im Gegenzug als Berater geführt. Vermutlich wurde von ihnen erwartet, dass sie sich wie Guttenberg und Amthor bei der Bundesregierung um Unterstützung des Unternehmens bemühen, das angeblich über 100 Mio. US $ an Investitionen eingesammelt hatte und zwischenzeitlich mit bis zu 250 Mio. US $ bewertet wurde. Welche famosen KI-Anwendungen das Unter-

nehmen den umworbenen Ministerien anzubieten hatte, blieb allerdings bis zuletzt unklar. Im April 2021 meldete es schließlich Insolvenz an.

Dieses Schicksal droht der Investmentgesellschaft In-Q-Tel nicht, denn diese wird direkt aus dem Haushalt des US-amerikanischen Auslandsgeheimdienstes CIA finanziert. Nach Angaben des deutschen Verfassungsschutzes vergibt es „Risikokapital an junge Unternehmen, insbesondere im Bereich der Informationstechnologie“[12], wobei es offenbar darum geht, die entsprechenden Technologien für das US-amerikanische Militär bzw. die Geheimdienste zugänglich zu machen oder zumindest dem Zugriff Dritter zu entziehen. Ende 2020 war In-Q-Tel beim Dresdner Startup *Morpheus Space* eingestiegen, einer auf Antriebe für Nano-Satelliten spezialisierte Ausgründung der TU Dresden, die zuvor auf verschiedenen Ebenen Fördergelder aus der öffentlichen Hand erhalten hatte. Dies sorgte für Kritik von verschiedenen Seiten.

Dass öffentliche Gelder in private Profite überführt werden, indem Risiken sozialisiert und Gewinne privatisiert werden, ist jedoch eine zentrale Funktion des angestrebten Ökosystems und eine – gar nicht so neue – Form der politischen Steuerung technologischer „Innovation“.

Anmerkungen

1 *Walter Dornberger (2020) Peenemünde – Die Geschichte der V-Waffen. RhinoVerlag, Ilmenau 2. Auflage 2020.*

2 *Vgl. beispielhaft: Petra Molnar, Lex Gill (2018) Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf.*

3 *Einen sehr guten Überblick über diskutierte Anwendungsbereiche liefert z. B. das Programm der Tagung „Künstliche Intelligenz – Chancen und Risiken für die Bundeswehr“ der Studiengesellschaft der Deutschen Gesellschaft für Wehrtechnik mbH, einsehbar unter: https://www.dwt-sgw.de/fileadmin/redaktion/SGW-Veranstaltungen/2019/9F9_KI2/9F9_KI_Bw_Programm_281019.pdf*

4 *Die Stellungnahme findet sich unter: https://www.mpg.de/11543958/Stellungnahme-Wissenschaft-und-Industrie.pdf.*

5 *Martin Stratmann (2017) Der Staat muss auch riskante Projekte fördern, Tagesspiegel (18.10.2017), dokumentiert unter: https://www.mpg.de/11679923/der-staat-muss-auch-riskante-projekte-foerdern.*

6 *Asgard, Roland Berger (2018) Artificial Intelligence – A strategy for European startups, https://www.rolandberger.com/publications/publication_pdf/roland_berger_ai_strategy_for_european_startups.pdf.*

7 *Die folgenden beiden Absätze sind weitgehend gleichlautend einem anderen Text des Autors entnommen, der sich mitsamt der jeweiligen Quellen unter folgender URL finden lässt: https://www.imi-online.de/2020/07/02/ein-diskreter-dammbruch-der-ruestungsforschung/*

8 *Das Thesenpapier, aus dem alle Zitate in diesem Abschnitt entnommen sind, findet sich hier: https://www.bundeswehr.de/resource/blob/156024/d6ac452e72f77f3cc071184ae34dbf0e/download-positionspapier-deutsche-version-data.pdf.*

9 *Larissa Holzki (2021): Bundeswehrgeneral fordert: „Auch bei klassischen militärischen Problemen jetzt mit Start-ups zusammenarbeiten“, Handelsblatt.de (29.07.2021).*

10 *Siehe: https://migration-control.info/bobusi/.*

11 *Zitiert nach dem entsprechenden Eintrag in der „Border Business Liste“, siehe: https://migration-control.info/bobusi/pandora-inteligence (Stand 2.11.2021).*

12 *Bundestags-Drucksache 19/23509, https://dserver.bundestag.de/btd/19/235/1923509.pdf.*

Thomas Reinhold

Zur Rolle und Verantwortung der Informatik für die Friedensforschung und Rüstungskontrolle

Die Ursprünge des Internets, so wie wir es heute kennen, basierten auf der Idee eines Austauschs von Ideen, Informationen und Codes. Obwohl die technischen Konzepte bereits durch den Wunsch nach einem staatlichen und militärischen Kommunikationssystem motiviert waren, w… überstehen konnte, waren ein … Nutzer:innen Akademiker:innen … Laufe der Jahre entwickelten sie … freien Informationsfluss unterstü… nach aus, als könnte sich diese Idee hin zu einem weltweit freien und zugänglichen Netz entwickeln. Seit einigen Jahren, spätestens jedoch seit der Entdeckung von Stuxnet im Jahr 2010, wissen wir jedoch, dass auch Militär und Geheimdienste den sogenannten Cyberspace als Domäne für ihre Zwecke entdeckt haben. Angesichts der Abhängigkeiten moderner Gesellschaften von IT-Diensten und den zugrunde liegenden Infrastrukturen ist es zweifelsohne notwendig, die nationale IT-Sicherheit zu fördern und militärische Abwehrkapazitäten in diesem Bereich aufzubauen. Allerdings zeigen die Snowden-Enthüllungen oder der UNIDIR-Cyber-Index[1], dass immer mehr Staaten den Cyberspace auch als militärische Domäne betrachten, in der sie offensive Fähigkeiten entwickeln (müssen) oder diese bereits einsetzen. So ist es bei den US-Streitkräften inzwischen Pflicht, dass jeder Einsatz im Feld durch eine eigene Cyber-Einheit be… strategische Unterstützung und …g ist. Diese Entwicklung ist auch …gegangen, wo die Bundeswehr … Einheit, das Kommando *Cyber- und Informationsraum* (KdoCIR), eingerichtet hat, welche ab diesem Jahr voll einsatzfähig sein soll[2]. Inwieweit dieses neue Kommando offensive Fähigkeiten entwickeln und einsetzen darf (und auch wird), ist allerdings trotz zahlreicher öffentlicher Nachfragen und parlamentarischer Debatten weiterhin offen. Vieles deutet jedoch darauf hin, dass die bereits bestehenden Fähigkeiten der Vorgänger-Einheit *Computer-Netzwerk-Operationen* für solche Zwecke weitergenutzt und ausgebaut werden.

Wo militärische Kräfte in den Cyberspace vordringen, hat die internationale Gemeinschaft nach wie vor Schwierigkeiten, die in den letzten Jahrzehnten für die internationale Sicherheits-

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