Christoph Marischka

Künstliche Intelligenz in der Europäischen Verteidigung:

Eine autonome Aufrüstung?

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

DIE LINKE.
IM EUROPAPARLAMENT

Christoph Marischka

Künstliche Intelligenz in der Europäischen Verteidigung: Eine autonome Aufrüstung?

Inhalt

6 **Einleitung Özlem Alev Demirel: Warum Widerstand nötig ist!**

8 **1. Ein neuer Sputnik-Moment**

10 **2. Erwartete militärische Vorteile der Digitalisierung**

20 **3. Künstliche Intelligenz in der Genese des EU-Rüstungsfonds**

20 **3.1. Strategische Autonomie eines „Globalen Europas“**

24 **3.2. Der Fähigkeits-Entwicklungsplan**

26 **3.3. Autonome Syteme und KI in den „Prioritäten“**

27 **3.4. Der Europäische Verteidigungs-Aktionsplan**

28 **3.5 Das Pilotprojekt**

31 **3.6. Vorbereitende Maßnahme im Bereich Verteidigungsforschung (PADR)**

33 **3.7 Entwicklungshilfe für die Rüstungsindustrie (EDIDP)**

34 **3.8. PESCO**

36 **3.9. Digitalisierung und KI in frühen PESCO-Projekten**

37 **3.10. Digitalisierung und KI in späteren PESCO-Projekten**

40 **3.11. Die Fusion von Rüstungs-, Industrie und Digitalisierungspolitik**

44 **4. Eine europäische Revolution der Kriegführung?**

44 **4.1. Über verstreute Projekte zur gemeinsamen „Cloud"?**

46 **4.2. Eine technologiegetriebene, offensive Strategie**

48 **4.3. Die wirklichen Triebkräfte: Industrie und (Risiko-)Kapital**

51 **Impressum**

Einleitung Özlem Alev Demirel: Warum Widerstand nötig ist!

Hoch fliegende Pseudo-Satelliten, die weiträumige Gebiete monatelang überwachen; Drohnenschwärme, welche die Umgebung von Feldlagern und „kritischen Infrastrukturen“ sichern; Computersysteme, die Ziele vorschlagen und die optimale Schusslinie berechnen; Chat-Bots, die Jugendliche für den Militärdienst begeistern und die tatsächliche Lage auf fernen Gefechtsfeldern verschleiern sollen; automatisierte militärische Logistik und (Rüstungs-)Produktion: Viele der aktuellen Rüstungsprogramme der Europäischen Union und ihrer Mitgliedsstaaten haben auf die eine oder andere Weise mit Künstlicher Intelligenz zu tun.

Für die Bevölkerungen in Europa stellt die aktuelle, von Digitalisierung und Künstlicher Intelligenz (KI) getriebene Aufrüstung der Europäischen Union eine Bedrohung dar. Dies alleine schon deshalb, weil nicht zuletzt die Covid-19 Pandemie gezeigt hat, dass das Geld, das damit der Rüstungsindustrie zugeschustert wird, z.B. in der Pflege und im Gesundheitswesen dringend benötigt wird. Aber auch deshalb, weil diese spezifische Form von Rüstung nicht nur das Potential hat, völlig neue Formen der Überwachung und Propaganda innerhalb Europas hervorzubringen, sondern auch eine militärische Eskalation der latenten Konflikte unter und mit Großmächten anheizt und wahrscheinlicher macht. Während es sich bei den Erwartungen an eine „Super-KI“ vor allem um einen Hype zu handeln scheint, mit dem Industrie und (Risiko-)Kapital öffentliche Gelder für ihre Profite mobilisieren wollen, finden KI-Anwendungen im Zuge der aktuellen Aufrüstungsspirale nichtsdestotrotz auf allen Ebenen Einzug in militärische Systeme und Planung.

Es droht vielleicht kein plötzlicher, aber sicherlich ein schleichender Kontrollverlust. Denn die aktuelle Aufrüstungsspirale beinhaltet nicht nur die Entwicklung von Drohnenschwärmen und Killerrobotern, sie droht auch, die gängigen Unterscheidungen zwischen Krieg und Frieden, Zivilist*innen und Kombattant*innen aufzuheben und das Gefechtsfeld völlig zu entgrenzen – wie dies in der Cyberkriegführung bereits der Fall ist. Eine Studie der RAND Cooperation etwa, die im Auftrag der European Defence Agency in den Rüstungskatalog der EU (Capability Development Plan von 2018) eingegangen ist, prognostiziert eine nahezu vollständige Bedeutungslosigkeit des Völkerrechts nach 2035. Nationale und internationale Regularien tauchen darin primär als Hindernisse bei der Realisierung technologischer Möglichkeiten auf.[1]

Anstatt sich an diesem irren Wettrüsten zu beteiligen, wäre es wünschenswert für unserer aller Sicherheit, wenn sich die EU mit voller Kraft für die Regulierung von autonomen Waffensystemen, Cyberwar und Propaganda einsetzen würde. Um in Frieden leben zu können, brauchen wir eine scharfe Abgrenzung des Friedens vom Krieg - der zu ächten ist, anstatt ihn auf allen Ebenen, von der Verkehrs- und Forschungspolitik bis zur Platine in unseren Mobilfunknetzen zu antizipieren und vorzubereiten. Die Kampagnen „Cyberpeace“ und „Stop Killer Robots“ geben hierzu wichtige und realisierbare Impulse. Anders als die Rüstungsindustrie werden sie jedoch nicht mit dreistelligen Millionenbeträgen jährlich von der EU-Kommission gefördert. Stattdessen fördert die Kommission bereits seit Jahren gezielt die Zusammenarbeit zwischen zivilen Hochschulen und der Rüstungsindustrie. Auch hiergegen gibt es Widerstand, der am richtigen Punkt ansetzt: Wie viele Gelder werden in die Lösung gesellschaftlicher Probleme investiert und wie viele in die desaströse, beschleunigte und weitgehend unkontrollierte Aufrüstung der Militärapparate?

[1] *Marta Kepe, James Black, Jack Melling, Jess Plumridge: Exploring Europe's capability requirements for 2035 and beyond (June 2018), www.rand.org.*

„Für die Bevölkerungen in Europa stellt die aktuelle, von Digitalisierung und Künstlicher Intelligenz (KI) getriebene Aufrüstung der Europäischen Union eine Bedrohung dar.“

Inhalt

1. Ein neuer Sputnik-Moment

Im Mai 2017 gewann eine zuvor von Google/Alphabet eingekaufte und weiterentwickelte KI wiederholt gegen den damaligen (chinesischen) Weltranglistenersten, Ke Jie, im traditionellen chinesischen Brettspiele Go. Dies gilt als bahnbrechender Erfolg auf dem Feld des Maschinellen Lernens, der dessen nahezu unbegrenzten Potentiale unter Beweis zu stellen scheint. In der Sphäre der Geopolitik wurden dieses und andere Go-Spiele zwischen Mensch und Computer später mit dem sog. Sputnik-Schock verglichen,[2] als es der UDSSR vor den USA gelang, einen Satelliten in eine Umlaufbahn um die Erde zu schicken. Ähnlich wie dieser Sputnik-Schock damals massive Investitionen in die Grundlagenforschung und die Luft- und Raumfahrt durch die US-Regierung nach sich gezogen hatte, veröffentlichte China nur zwei Monate später eine KI-Strategie mit dem erklärten Ziel, bis 2030 weltweit führend in der KI-Entwicklung zu werden. Am 1. September 2017 wiederum erklärte der russische Präsident Putin in einer Rede vor russischen Schüler*innen Künstliche Intelligenz zur Zukunft der Menschheit: "Sie eröffnet kolossale Möglichkeiten, aber auch kaum abzusehende Gefahren. Wer auch immer in diesem Bereich führend wird, wird die Welt kontrollieren".[3]

Putins Worte und die Ziele der chinesischen Strategie erfuhren im transatlantischen Raum einen breiten Widerhall. Diesseits wie jenseits des Atlantik wurden sie in der Erwartung aufgegriffen, massive öffentliche Investitionen und politische Unterstützung für entsprechende Forschung auf allen Ebenen zu mobilisieren. In den USA waren diese Forderungen mit dem drohenden Verlust ihrer Rolle als einziger Supermacht und weltweitem Technologieführer verbunden. In Europa hingegen dienen sie der Vision, der Europäischen Union nicht nur einen neuen Schub der Integration zu verleihen, sondern diese im globalen Wettbewerb der Mächte zu einem Mitbewerber auf Augenhöhe mit den USA und China zu machen. Hatte die damalige EU-Außenbeauftragte Catherine Ashton schon anlässlich der Aufstellung des Europäischen Auswärtigen Dienstes 2010 im Rahmen der klassischen Geopolitik das Ziel ausgegeben, in Sachen Gestaltungsmacht mit den USA und China gleichziehen zu können, so werden in Bezug auf die neue, KI-getriebene Tech-Geopolitik auch jenseits Europas die EU, China und die USA als wichtigste Konkurrenten um die Spitzenposition genannt. Im Mai 2018 z.B. veröffentlichte das Wirtschaftsberatungsunternehmen Roland Berger gemeinsam mit einem Fondsverwalter für Risikokapital, Asgard, eine Studie zu KI in Europa. In der Einleitung heißt es klipp und klar: „Wir glauben, dass Europa im ‚Wettrüsten' zwischen den USA und China als dritter Mitspieler aufschließen kann".[4]

Als einer der wichtigsten Rohstoffe für den aktuellen Hype um KI gelten Daten. China sei hier aufgrund seiner umfassenden Überwachungsprogramme und die USA wegen der führenden Position ihrer Tech-/Plattformunternehmen (Google/Alphabet, Amazon, Facebook, Microsoft) gut aufgestellt. Die EU hingegen verfügt über einen großen und kaufkräftigen Binnen- und Gesundheitsmarkt, der zumindest potentiell vergleichbare Datenmengen liefern kann, sowie eine leistungsfähige Wissenschaft und Forschungsinfrastruktur. Darüber hinaus hat sich in der EU in den vergangenen Jahren eine strategische und effektive Industriepolitik herausgebildet, die von der Förderung von kleine und mittelständischen Unternehmen (SMEs) bis hin zu politisch forcierten Fusionen bestehender Konzerne von Weltrang auf europäischer Ebene die Planung und Realisierung ganzer Wertschöpfungsketten ermöglicht und konsequent auf Digitalisierung und Autonomie ausgerichtet wird. Ziel ist die sog. „digitale Souveränität" als Unabhängigkeit von (Vor-) Produkten und Dienstleistungen aus Drittstaaten beim Aufbau der eigenen digitalen Infrastruktur. Diese gilt zurecht als wesentliche Voraussetzung für die angestrebte globale Spitzenposition.

[2] Siehe z.B.: Paul Mozur: Google's AlphaGo Defeats Chinese Go Master in Win for A.I., NY Times (23. Mai 2017); Nicholas Thompson and Ian Bremmer: The AI Cold War That Threatens Us All, Wired.com (23.10.2018); Denise Feldner: Will a Chinese "Sputnik moment" in AI Unleash Dynamism in the West?, The Globalist (26.8.2018).

[3] James Vincent: Putin says the nation that leads in AI 'will be the ruler of the world' (4.9.2017), www.theverge.com.

[4] Roland Berger / Asgard: Artificial Intelligence – A Strategy for European startups, https://asgard.vc.

Diese Idee der „digitalen Souveränität“ ist aber mehr als ein industriepolitisches Leitbild, sondern geht von einem latenten Kriegszustand zwischen konkurrierenden Großmächten aus. Sie bedeutet damit eine Abkehr vom liberalen Weltbild, wonach globale Vernetzung und Wertschöpfungsketten und die daraus entstehenden Abhängigkeiten die Möglichkeiten und Wahrscheinlichkeit großer kriegerischer Konflikte reduziere. Stattdessen läuft sie auf die Schaffung informationstechnisch abgeschlossener und damit – in Zeiten hybrider Strategien und der Cyberkriegführung – kriegführungsfähiger Blöcke hinaus.

Diese Tech-Geopolitik integriert nicht nur die Vorstellung der EU als „Wettbewerbsstaat“ mit einer letztlich militärisch gedachten Geopolitik, sondern wird zugleich als Voraussetzung gesehen, um im Wettlauf um die militärische Anwendung Künstlicher Intelligenz zu bestehen. KI-gestützte Waffensysteme bieten insbesondere für eine Europäische Union eine Verheißung, die zwar eine militärisch gestützte Macht werden will, im Personalumfang jedoch nur über relativ kleine und national fragmentierte, aber technisch gut ausgerüstete Armeen verfügt. Autonome (Waffen-)Systeme und das sog. Manned-Unmanned Teaming prägen zahlreiche der aktuellen Rüstungs- und Forschungsprojekte und werden u.a. mit dem Ziel verfolgt, mit einem relativ überschaubaren Personalkörper gleichwohl auch militärisch mit den USA, Russland und China gleichzuziehen.

Historisch gesehen finden sich zahlreiche Beispiele dafür, dass technologische Überlegenheit nicht zwingend auch militärische oder politische Vorherrschaft hervorbringt. In die KI wurde auch in den vergangenen Jahrzehnten mehrfach große Hoffnungen gesetzt, die durch umfangreiche, militärisch inspirierte Investitionsprogramme unterfüttert, letztlich aber enttäuscht wurden. Auch im aktuellen Wettlauf um die Entwicklung disruptiver militärischer Anwendungen von KI ist keineswegs ausgemacht, dass sich diese oder die damit assoziierten strategischen Vorteile realisieren werden. Deshalb wird am Ende dieser Studie die Frage aufgeworfen, welche strategischen Folgen der verstärkte Einsatz von KI-Anwendungen im Militär haben wird und welche Gefahren diese beinhalten. Es erscheint aus dieser Perspektive notwendig, KI bzw. die hierin gesetzten Erwartungen auch als Akkumulationsregime zu begreifen, mit dem profitorientierte Akteure eine Umverteilung öffentlicher Mittel und die Re-Regulierung des Kapital- und Arbeitsmarktes durchsetzen wollen. Denn je mehr man sich von den globalen und v.a. wirtschaftspolitisch motivierten Diskursen zu KI wegbewegt und die konkrete Rüstungspolitik und die militärischen Strategien der EU und ihrer Mitgliedsstaaten in den Blick nimmt, desto mehr trifft man auf altbekannte Visionen militärischer Überlegenheit, die mit dem disruptiven Versprechen „Künstlicher Intelligenz“ als Game-Changer weniger zu tun haben, als mit den nicht mehr ganz so neuen Erwartungen an eine auf Informations- und Kommunikationstechnologie (IKT) gestützte Kriegführung. Im Folgenden werden deshalb die – oft auch eher kleinteiligen – Erwartungen an die Digitalisierung von Seiten der Streitkräfte dargestellt und anschließend ausführlich dargestellt, welche Rolle entsprechende Technologien beim Aufbau und der Umsetzung des Europäischen Verteidigungsfonds (European Defence Fund, EDF) spielen und gespielt haben.

Inhalt

2. Erwartete militärische Vorteile der Digitalisierung

Viele der Erwartungen, die Militärs in Digitalisierung und KI setzen, und die von Rüstung und Entwickler*innen geschürt werden, sind bereits Jahrzehnte oder gar Jahrhunderte alt. Die zentrale Vision der digitalisierten Kriegführung besteht in der Herstellung eines „gläsernen Gefechtsfelds" bzw. von „Informationsüberlegenheit". Sie soll es den Vorgesetzten ermöglichen, auf Grundlage eines umfassenden Lagebewusstseins Kommandos zu erteilen und auch durchzusetzen **(Command and Control, C2)**. Wie frühe, heroische Darstellungen großer Feldherren gerne den „Nebel des Krieges" ignoriert haben, so zeichnen sich bis heute Computerspiele dadurch aus, dass sie gerne die Vision vollständiger Information und Kontrolle vermitteln. Entsprechend lassen sich die Vorteile, die sich Militärs von der Digitalisierung erhoffen, tatsächlich mit gängigen Computerspielen vergleichen. Auf Kommandoebene liegt demnach stets ein Lagebild vor, auf dem eigene, verbündete und feindliche Kräfte sowie weitere mögliche Ziele und Hindernisse exakt lokalisiert und jederzeit empfänglich für neue Kommandos sind. Häufig lassen sich auf diesem Lagebild auch noch Indizes wie Kampfkraft, Munitionsbestand usw. nicht nur der eigenen, sondern auch der feindlichen Truppen und Einrichtungen anzeigen, sodass sich der Bedarf an Feuerkraft gut einschätzen bzw. kalkulieren lässt. Es ist kaum zu überschätzen, wie sehr dies die populäre Vorstellung von Krieg prägt und wie weit es zugleich jetzt – und vermutlich auch in der Zukunft – von der Realität entfernt ist. Um hier jedoch nicht in ferne Visionen der Spieleindustrie (und der Rüstung) abzugleiten, sollen im folgenden einige militärische Konzepte vorgestellt werden, die sich in Ansätzen bereits in der technischen Erprobungsphase und taktischen Implementierung befinden. Wir werden dabei feststellen, dass die technologische Entwicklung dabei sehr oft unter zivilen Szenarien in einem zivilen Kontext stattfinden.

Situation Awareness: Das „Situationsbewusstsein" ist eine sehr grundsätzliche Fragestellung der Künstlichen Intelligenz. Ob es z.B. um die Spracherkennung oder Computer Vision geht, ist die Einbeziehung des Kontextes entscheidend dafür, ob ein Ereignis ansatzweise richtig kategorisiert wird oder nicht. Nachdem die Forschung über Jahrzehnte weitgehend daran gescheitert ist, durch von Menschen formulierte logische Operationen so etwas wie Situationsbewusstsein in informationstechnische Systeme (ITS) zu implementieren, setzt man hierzu nun v.a. Hoffnungen in auf Big Data basierende Methoden des sog. Maschinellen Lernens.

Für einen unbemannten Flugkörper ist es von größter Relevanz, ob es sich bei einem erfassten Objekt um einen kleinen Vogel in unmittelbarer Nähe handelt, oder ein weit entferntes Flugzeug. Aus dem rein optisch erfassten Datenstrom lässt sich mithilfe des maschinellen Lernens womöglich eine halbwegs sichere Kategorisierung erstellen. Zuverlässiger wird diese jedoch, wenn die Daten der Kameras z.B. mit denen eines Laser-Entfernungsmessers oder eines Infrarot-Sensors „fusioniert" werden. Während der Mehrwert einer solchen „Sensor-Data-Fusion" auch bei menschlich nachvollziehbaren logischen Operationen ersichtlich ist, können Methoden des Maschinellen Lernens für ihr „Situationsbewusstsein" tendenziell alle verfügbaren Daten einbeziehen. Forschung zu Sensor-Data-Fusion bzw. dieser Form der Mustererkennung findet aus nachvollziehbaren Gründen bspw. im Kontext des autonomen Fahrens gegenwärtig in zahllosen zivilen Universitäten und auch in mittelständischen Betrieben statt, war jedoch bis vor wenigen Jahren eine typische Domäne militärtechnischer Forschung und ist für diese weiterhin von höchstem Interesse.

Welche Vorteile die Fortschritte beim maschinellen Lernen bzw. der Mustererkennung bieten, lässt sich an der Satellitenaufklärung verdeutlichen. Aktuell wird an Technologien geforscht, bei denen Satelliten (oder Drohnen) autonom entscheiden können, welche Gebiete mit welcher Auflösung aufgenommen werden. Aus der großräumigen Überwachung mit niedriger Auflösung werden „Regions of Interest" identifiziert, die mit großer Auflösung beobachtet werden. Das können z.B. Orte sein, an denen Veränderungen wahrgenommen werden oder sich verdächtige Personen aufhalten.[5] Veränderungen können dann in hoher Auflösung auf dem Gesamtbild sichtbar gemacht werden. Somit rückt eine detaillierte Überwachung großer Räume in quasi-Echtzeit näher an den Bereich des Möglichen.

Zugleich werden gegenwärtig sog. Pseudo-Satelliten entwickelt. Dabei handelt es sich um extrem leichte Flugzeuge, die in großer Höhe fliegen und alleine durch Solarenergie navigieren und kommunizieren können. Dadurch sind sie fähig, wochen- oder gar monatelang in der Luft zu bleiben und Gebiete zu überwachen.[6] Künstliche Intelligenz soll dafür sorgen, dass sie diese Aufgaben selbstständig durchführen und dabei z.B. auch in Abhängigkeit von den Wetterverhältnissen navigieren. Längst im Einsatz sind Bodenradare etwa zum Schutz von Feldlagern, die auf eine Entfernung von dutzenden Kilometer selbstständig Objekte klassifizieren, verfolgen und als mögliche Ziele identifizieren können. Eine netzwerkzentrierte Kriegführung geht im Idealfall davon aus, dass sich die Daten der hochfliegenden Pseudosatelliten, der Bodenradare und vieler anderer Aufklärungssysteme zu einem gemeinsamen Lagebild fusionieren lassen. Eine der größten Herausforderungen bleibt dann noch, wie man diese enorme Datenmenge und die daraus abgeleiteten Handlungsempfehlungen verständlich an einer Mensch-Maschine-Schnittstelle darstellen kann.

Was hier für die abbildende Aufklärung beschrieben wurde, gilt ähnlich für die Signal Intelligence und die Open Source Intelligence (z.B. social media). Auch hier sammeln zunehmend autonome Systeme Daten und bereiten diese auf. Umfangreiche Forschung hierzu fand seit 2003 in den USA unter dem Total Information Awareness-Programm der USA statt, mit dem u.a. versucht wurde, die Aktivitäten von Personen im Internet und Sozialen Netzwerken so zu erfassen und auszuwerten, dass sie Prognosen darüber zulassen, wer möglicherweise in der Zukunft einen terroristischen Anschlag durchführen könnte. Von Satellitenstationen in Deutschland, Österreich und Zypern werden Kommunikationssatelliten über dem Nahen und Mittleren Osten abgehört,[7] wobei man versucht, aus den abgefangenen Metadaten Muster zu erkennen, die Vorhersagen über Ereignisse zulassen.

Sensor-to-Shooter: Die netzwerkzentrierte Kriegführung besteht nicht nur in der Vernetzung von Aufklärungssystemen untereinander, sondern auch derjenigen zwischen Aufklärungs- und „Wirksystemen". Die Folgen des Sensor-to-Shooter Konzepts sind – in Verbindung mit präzisen Möglichkeiten zur Lokalisierung – enorm. Bisher besteht oft noch eine erhebliche Zeitverzögerung zwischen der Erhebung von Aufklärungsdaten und der Wirkung von Waffensystemen. Weitere Zeit vergeht, bis die Wirkung des Beschusses erfasst ist und auf dieser Grundlage entschieden werden kann, ob weiterer Beschuss nötig ist oder z.B. Bodentruppen vorrücken können.

Aufklärungssysteme sollten möglichst klein und wendig sein, um unbemerkt hinter feindlichen Linien, in bebautem Gebiet und im besten Falle auch in Gebäuden selbst agieren zu können. Um eine große Wirkung zu erzielen, müssen Waffensysteme hingegen über eine große Sprengladung verfügen. Sie sind damit tendenziell auffällig, träge und verwundbar und werden deshalb gerne aus der Distanz angewandt. Bei Drohnen, wie sie aktuell für sog. gezielte Tötungen verwendet werden, handelt es sich letztlich um bewaffnete Aufklärungsdrohnen, eine Mischform, die nur in mehr oder weniger unumkämpften Luftraum zum Einsatz kommt. Ihre Bewaffnung reicht, um in asymmetrischen Konflikten zuverlässig Einzelpersonen zu töten oder ungeschützte Fahrzeuge außer Gefecht zu setzen, nicht aber, um gepanzerte Fahrzeuge oder Gebäude anzugreifen. Für eine gegnerische Luftwaffe oder Luftabwehr würden sie leichte Ziele darstellen. Auch die aktuell in der Entwicklung befindliche „Eurodrohne" soll sich mit Präzisionswaffen

[5] Entsprechende Forschung findet u.a. am Institut für Informationsverarbeitung (TNT) der Leibniz Universität Hannover (Germany), statt. Siehe z.B. Holger Meuel u.a.: Low Bit Rate ROI Based Video Coding for HDTV Aerial Surveillance Video Sequences, http://ftp.tnt.uni-hannover.de .

[6] Ein Beispiel hierfür ist der Solar High Altitude Pseudo-Satellite Zephyr von Airbus, der bereits von den britischen Streitkräften genutzt wird.

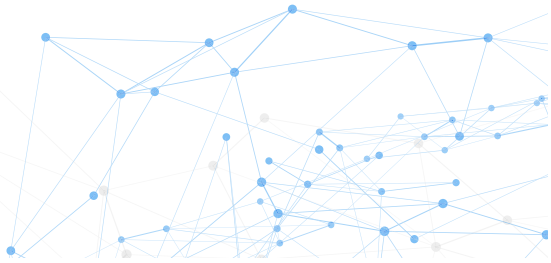
[7] Erich Möchel: Daten von der Königswarte für NSA-Projekt (6. Januar 2016), https://fm4v3.orf.at.

ausstatten lassen. Im Gefechtsfeld wird ihre Funktion jedoch auch in der Zielerfassung bestehen. Sie könnte dann entsprechend des Sensor-to-Shooter-Konzepts Ziele erkennen bzw. vorschlagen und deren genaue Koordinaten direkt an Waffensysteme weitergeben, die auch aus weiter Entfernung nahezu ohne Zeitverzögerung große Mengen kinetischer Energie ins Ziel bringen können. Auch die Ermittlung der Folgen des Beschusses kann dann unmittelbar erfolgen.

Dies verkürzt natürlich auch die Zeit, die für (menschliche) Entscheidungsprozesse zur Verfügung steht, weshalb in der Fachliteratur vom „Kampf mit der Geschwindigkeit von Maschinen" die Rede ist.[8] Auch wenn viele Regierungen der EU bislang beteuern, dass auch in Zukunft jede Anwendung von Waffengewalt durch einen Menschen bestätigt werden müsse, wird in den Armeen längst konzeptionell daran gearbeitet, dass Menschen zwar raumzeitliche Korridore definieren (oder vielmehr bestätigen), innerhalb dieser jedoch Ziele autonom identifiziert und bekämpft werden. Bei der Abwehr gegen Flugkörper ist dies z.B. auf vielen Kriegsschiffen europäischer Staaten bereits seit Jahren Praxis (wobei hier Sensor und Wirkmittel nicht über die Cloud vernetzt, sondern in einem System integriert sind).[9] Spätestens wenn es gilt, sich gegen sog. Überlastungsangriffe mit autonomen Systemen zu verteidigen, wird keine Zeit mehr sein für menschliche Entscheidungen und der Mensch aus der Schleife zwischen Sensor und Shooter ausscheiden.

Elektronische Kampfführung / Cyberdefence: Bemühungen, die feindliche Informations- und Kommunikationsstrukturen zu entschlüsseln, zu stören und zu täuschen, sind eine sehr alte militärische Aufgabe. Da diese Kommunikation spätestens seit dem Zweiten Weltkrieg vor allem im elektromagnetischen Spektrum stattfindet, wurden Versuche ihrer Entschlüsselung, Störung und Täuschung in den vergangenen Jahrzehnten oft unter dem Bergriff der Elektronischen Kampfführung zusammengefasst. Ein zentrales Mittel der Elektronischen Kampfführung ist das Jamming. Es kommt heute in asymmetrischen Konflikten u.a. beim Schutz vor improvisierten Sprengfallen (IED) zum Einsatz, die über das Mobilfunknetz gezündet werden. Damit das Jamming funktioniert, muss bekannt sein, auf welchen Frequenzen der Gegner kommuniziert. Die militärische Nutzung des elektromagnetischen Spektrums ist daher nahezu seit ihrem Beginn darauf angewiesen, die Nutzung der Frequenzen nach Prinzipien zu wechseln oder zu streuen, die möglichst schwer nachvollziehbar sind und/oder das Signal selbst zu verbergen. Seit dem findet ein beständiges Wettrüsten bei der Verschleierung der eigenen und der Aufdeckung und Störung der gegnerischen Kommunikation statt. Die United States Naval Academy beschrieb schon in den 1980er Jahren, dass Fortschritte dabei – zumindest unter technologisch vergleichbaren Kontrahenten – stets „nur eine endliche Überlegenheit hervorbringen. Schlussendlich wird ein Gegner eine neue Technik entwickeln und die Überlegenheit wird an ihn übergehen […] Technologische Überlegenheit und ständige Weiterentwicklung im Bereich der Elektronischen Kriegführung sind notwendig, um gegnerische Fortschritte auszugleichen".[10]

Bemühungen, die feindliche Informations- und Kommunikationsstrukturen zu entschlüsseln, zu stören und zu täuschen, sind eine sehr alte militärische Aufgabe.



[8] Lieutenant Colonel Thomas Doll, Uwe Beyer and Captain Thomas Schiller: Hyperwar - New Challenges for Army Development, Europäische Sicherheit und Technik (4. September 2019), https://esut.de/.

[9] Ein Beispiel hierfür ist das close-in weapon system „Goalkeeper" von Thales, das Nach Angaben des Herstellers u.a. bei der belgischen, niederländischen und portugiesischen Marine im Einsatz ist. Ausführlicher hierzu: ICRC: Autonomous weapon systems: Technical, military, legal and humanitarian aspects (expert meeting report), (November 2014), www.icrc.org.

[10] United States Naval Academy: Fundamentals of Naval Weapons Systems – Countermeasures (1989), https://fas.org.

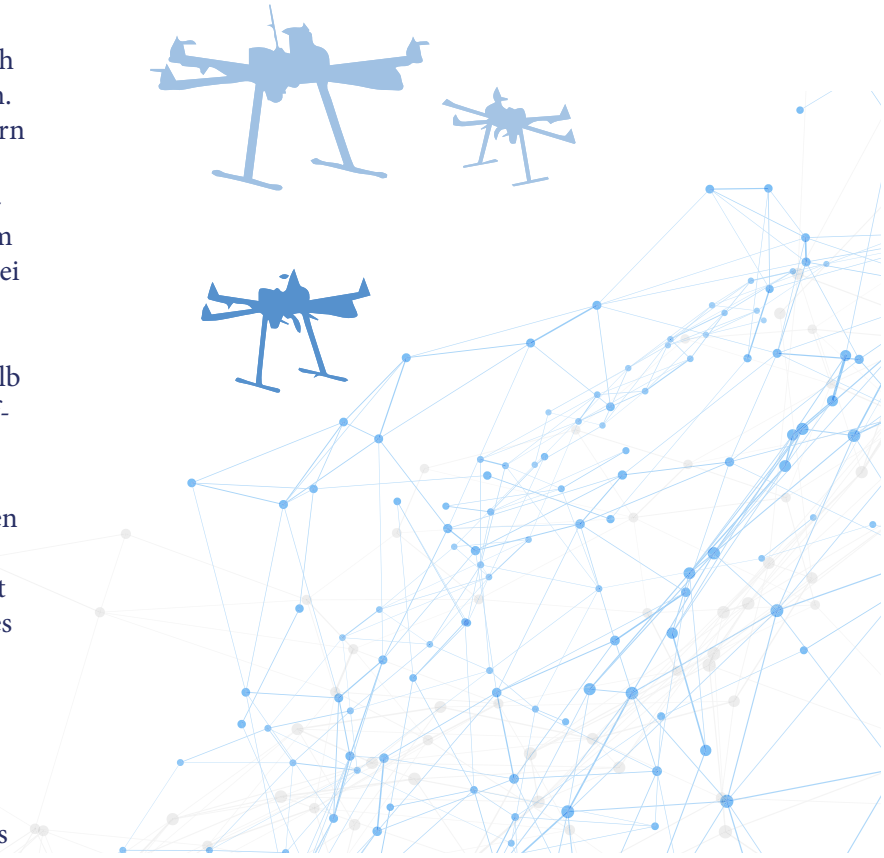
Die Erkennung von Kommunikations- wie Störsignalen war stets auch ein Feld der Mustererkennung und auch aktuell wird hier intensiv der Einsatz Künstlicher Intelligenz erprobt.[11] Mit der Digitalisierung des Schlachtfeldes hat sich die Abhängigkeit von funktionierenden Kommunikationsverbindungen zugleich erhöht und an Komplexität vervielfältigt. Die Handlungsmöglichkeiten hängen fast vollständig vom Zugang zu satellitengestützten Navigationssystemen und zum Cyberspace ab. Diesen Zugang zu sichern, hat zwar in den asymmetrischen Konflikten der letzten Jahrzehnte keine große Herausforderung dargestellt, ist jedoch von fundamentaler Relevanz für militärische Operationen gegen ansatzweise gleichwertige Gegner. So schrieb die US-Militärberaterin Chris Scott bereits 2012: „Wenn wir diese bandbreiten-intensiven Technologien gegen andere potentielle Gegner einsetzen wollen, müssen wir uns klar sein, dass der Zugang zum Cyberspace nicht immer möglich sein wird".[12]

Bemühungen, den Zugang zum Cyberspace bzw. zur Combat Cloud zu unterbinden, werden zunehmend unter dem Begriff Cyber A2/AD diskutiert: Bei Anti-Access and Area-Denial (A2/AD) Strategien geht es darum, feindlichen Kräften den Zugang zu einem Gebiet und das Manövrieren hierin zu erschweren. Obwohl der Cyberspace keinen territorialen Raum darstellt, ist doch v.a. der Zugang zu ihm räumlich gebunden. Die Wirkung und Präzision von Störsendern etwa nimmt mit der Entfernung rapide ab und ist damit von räumlicher Nähe abhängig. Deshalb wird auch hier zunehmend am Einsatz unbemannter Systeme geforscht. Bei Einsätzen weit jenseits des eigenen Territoriums sind die Kräfte im Feld meist auf Satellitenverbindungen angewiesen, weshalb Anti-Satellitenwaffen in möglichen zukünftigen Konflikte eine zentrale Rolle zukommen wird. Die Kommunikation mit weit entfernten Kommandos und Rechenzentren verläuft über die wesentlich schnelleren Kabelverbindungen, die mitsamt der damit verbundenen Infrastruktur weit jenseits des eigenen Territoriums und des eigentlichen Gefechtsfeldes angreifbar sind. Jenseits dieser auf das Gefecht bezogenen Gefahr von Cyber A2/AD verweist u.a. das NATO Exzellenzzentrum für kooperative Cyber Defence in Tallinn darauf, dass es durchaus auch eine strategische Ebene gibt, auf der ganze „Staaten verbunden oder [vom Cyberspace] getrennt werden können – auch gegen ihren Willen. Cyber-Blockaden können vorkommen und Staaten der Zugang zum Cyberspace verwehrt werden […] Wegen der schwerwiegenden Folgen einer Cyber A2/AD-Strategie für die gesamte Bevölkerung ist es wahrscheinlich, dass sie im Rahmen eines militärischen Konflikts als Teil einer größer angelegten Kampagne zum Einsatz kommen werden".[13] Was unter den (defensiv wirkenden) Begriffen Cybersecurity, Cyberdefence und Resilienz verstanden wird, ist also auf taktischer Ebene eine Erweiterung der Elektronischen Kampfführung und erfolgt auf strategischer Ebene in der Erwartung eines großen, zwischenstaatlichen Krieges und in der Absicht, diesen führbar zu machen. Da es sich beim Cyber- und Informationsraum um einen hybriden Raum handelt – zivile Institutionen und Personen nutzen dieselbe Infrastruktur (Kabel etc.) wie das Militär – findet auch die Forschung, Entwicklung und Umsetzung entsprechender Konzepte zu seiner Resilienz in einem hybriden Kontext, d.h. in enger Zusammenarbeit zwischen zivilen und militärischen (Forschungs-)Institutionen statt.

[11] Im August 2018 hat IBM seine KI-Basierte Malware „Deeplocker" vorgestellt. Auf seiner Homepage schreibt das Unternehmen: „AI is changing the game for cybersecurity, analyzing massive quantities of risk data to speed response times", www.ibm.com/security/artificial-intelligence.

[12] Chris Scott: Anti-Access Area-Denial (A2AD) in Military Domains and in Cyberspace (17. Dezember 2012), www.fedcyber.com.

[13] Alison Lawlor Russell: Strategic Anti-Access/Area denial in cyberspace (2015), NATO CCD COE Publications, https://ccdcoe.org.



Überlastungsangriffe: Ein wichtiges Forschungsgebiet der Künstlichen Intelligenz ist die Kooperation zwischen autonomen Systemen. Auch sie findet mit sehr ähnlichen Fragestellungen an zivilen Institutionen unter zivilen Szenarien und an militärischen Einrichtungen statt. So genannte Robo-Cups, bei denen zwei gegnerische Teams von Robotern gegeneinander Fußball spielen, bieten einen spielerischen Einstieg in grundlegende Fragestellungen der Selbstlokalisation, Sensorik, Objekterkennung und des Schwarmverhaltens autonomer Systeme und bringen junge Teams von (angehenden) Wissenschaftler*innen mit Unternehmen zusammen, die oft auch in der Rüstung aktiv sind. Forschung mit Schwärmen von handelsüblichen unbemannten Flugkörpern findet europaweit an hunderten Hochschulen statt und erfolgt oft unter rein spielerischen (Tanz, Formationsflug) Aufgabenstellungen oder Szenarien aus der Landwirtschaft, des Umwelt- oder Katastrophenschutzes. Die US Luftwaffe hatte bspw. auch das biologische Institut der Universität Marburg mit einer Studie zur nächtlichen Orientierung von Wüstenheuschrecken beauftragt, um diese auf mögliche Anwendungen für die Sensorik von kleinen Drohnen anzuwenden.[14] Das Institut für Flugsystemdynamik der Universität der Bundeswehr in München arbeitet bereits seit mindestens 15 Jahren konzeptionell an einem „kognitiven Agenten", der Schwärme größerer bewaffneter Drohnen koordinieren soll, die vorher bestimmte und priorisierte Ziele selbstständig ausschalten, dabei Verluste kompensieren und sich gegenseitig z.B. vor feindlichen Radarstellungen warnen sollen. Kleinere Schwärme handelsüblicher Drohnen wurden bereits in Libyen und Syrien von Milizen eingesetzt, um Stützpunkte anzugreifen und Sprengladungen abzuwerfen. Auch die israelische Luftwaffe setzt bei ihren Angriffen auf Syrien offenbar auf die Überlastung der Luftabwehr durch eine Kombination von Marschflugkörpern und Drohnen.[15] In der Frühphase das Syrienkonfliktes wurde darüber spekuliert, wie man für umfangreiche Luftschläge vom Mittelmeer aus die syrische Luftabwehr im dicht besiedelten Küstenstreifen zunächst mit Drohnen überlasten, orten und ausschalten könnte, bevor bemannte Flugzeuge Ziele im Hinterland attackieren.

Schwärme kleinerer Drohnen können zur Überwachung größerer Gebiete eingesetzt werden und in Verbindung mit dem Sensor-to-Shooter Konzept auch im Sinne des A2/AD zur Anwendung kommen – also Ziele für den Beschuss identifizieren. Besonders hohe Erwartung an Schwärme kleinerer Flugdrohnen setzt man offenbar im Bereich der Elektronischen Kampfführung, um gegnerische Sensorik zu überlasten oder Kommunikation zu stören (taktische Cyber AD). So beschreibt das Amt für Heeresentwicklung der Bundeswehr folgendes Szenario für den Einsatz eines taktischen Drohnen-Bataillons: „Die Luken der Transportfahrzeuge öffnen sich und 5000 UAS [unbemannte Luftsysteme] fliegen aus den Fahrzeugen. Sie formieren sich zu unterschiedlichen Schwärmen. Der Schwarm aus mehreren hundert Sensor-UAS erreicht gar eine Ausdehnung von über zwei Kilometern im Durchmesser und ist mit hochauflösenden Kameras ausgestattet. Andere Schwärme wiederum haben die Aufgabe gegnerische Drohnen zu stören oder dienen als Relais zur Kommunikation der eigenen UAS. Andere sind mit kleinsten Wirkmitteln zum Angriff gegnerischer Sensorik und zur Markierung bzw. Verfolgung von Zielen ausgestattet und zudem in Lage eine verlegefähige UAS-Sperre zu bilden. Ein Counter-UAS-Schwarm ist darauf trainiert, feindliche UAS abzufangen und zu vernichten".[16]

[14] Manfred Hitzeroth: Pentagon finanzierte Forschung der Uni Marburg, Oberhessische Presse (25. November 2013), www.op-marburg.de.

[15] Für eine unvollständige Liste von Einsätzen von Drohnen(-Schwärmen) durch nichtstaatliche Akteure siehe: Arthur Holland Michel: Counter-Drone Systems, Center for the Study of the Drone at Bard College (2019), https://dronecenter.bard.edu.

[16] German Army Concepts and Capabilities Development Centre: Artificial Intelligence in Land Forces (2019), www.bundeswehr.de.

Manned-Unmanned-Teaming: Die großen Europäischen Rüstungsprojekte setzen einen besonderen Fokus auf das sog. Manned-Unmanned-Teaming (MUM-T). Sowohl beim Future Combat Air System (FCAS) wie auch beim Main Ground Combat System (MGCS) soll das jeweils bemannte Kampfflugzeug bzw. der bemannte Panzer im Mittelpunkt eines Systems stehen, zu dem ansonsten unbemannte Fahrzeuge gehören. Die Systeme lassen sich modular zusammenstellen und erweitern. Die Drohnen können dann z.B. jeweils vorausfliegen oder vorausfahren, die Lage aufklären und Ziele markieren oder diese auch eigenständig bekämpfen. Grundsätzlich stehen dem Gesamtsystem damit mehr unterschiedliche Waffensysteme und Waffentypen zu Verfügung. Vor allem im Falle des Ground Systems können die autonomen Fahrzeuge zusätzlichen Treibstoff und Munition transportieren. Sie sollen auch mit abgesetzten Soldaten und Spezialkräften kooperieren und diesen z.B. Deckung bieten oder Verwundete bergen können.[17] Deutschland und Frankreich, die treibende Kräfte bei beiden Projekten sind, vereinheitlichen und aktualisieren bereits jetzt die Kommunikationstechnologien ihrer Streitkräfte. Teil der jeweiligen Projekte ist die Implementierung einer Battle Management Language, über die unbemannte Systeme integriert werden und mit Menschen kommunizieren können. Seit 2019 testet die Bundeswehr hierfür mit Unterstützung von Atos die Software Fire Weaver des israelischen Anbieters Rafael. Diese bietet laut Hersteller „den taktischen Streitkräften eine GPS-unabhängige, geopixelbasierte taktische gemeinsame Sprache zwischen allen Sensoren und Schützen, die eine optimale Situationswahrnehmung und ein verbessertes Verständnis des Gefechtsfeldes gewährleistet. Ziele, blaue Kräfte, empfindliche Standorte und andere Points of Interest, werden sofort und präzise geteilt und auf der Grundlage von 3D-Modellen [...] auf die Systemvisierelemente übertragen".[18] Das System „verbessert die menschliche Analyse und Entscheidungsfindung, indem es automatisch und sofort den relevantesten Effektor für jedes Ziel auswählt, unter Berücksichtigung der Einsatzregeln, des Standortes, der Sichtlinie, des aktuellen Munitionsstatus und vieler anderer Parameter".[19] Dabei kommen „die fortschrittlichen Algorithmen der künstlichen Intelligenz" zum Einsatz und „verarbeite[n] die Kampfdaten, analysier[en] sie und priorisier[en] die Feuerzuweisung".[20] Zumindest aus Sicht der Hersteller hat sich auf dem Gefechtsfeld also das Verhältnis zwischen Systeme und Mensch bereits umgekehrt: Die Algorithmen analysieren die Situation und machen Vorschläge für den Waffeneinsatz – denen der Mensch im Regelfall noch zustimmen muss.

Zwar unterscheidet das MUM-T konzeptionell noch zwischen verschiedenen Stufen der Steuerung von der vollen Kontrolle bis hin zur bloßen Information des Bedienpersonals.[21] Wenn aber die Besatzungen der Boden- und Luftsysteme unterstützt von einer Vielzahl von unbemannten Systemen tatsächlich mal in eine Gefechtssituation kommen sollten, werden sie zwangsläufig ein hohes Maß an Kontrolle abgeben müssen. Das gilt insbesondere im Luftkampf und wenn auch der Gegner autonome Systeme einsetzt. Als zentralen Vorteil des MUM-T benennt das Deutsch-Französische Forschungsinstitut Saint-Louis (ISL), dass es „zugleich die Effektivität des Gesamtsystems signifikant und den Schutz der Einsatzkräfte erhöhen kann – eine Schlüsselfrage für politische Entscheidungsträger*innen, auch weil in westlichen Gesellschaft die Akzeptanz von Verlusten in den eigenen Streitkräften sinkt".[22]

[17] Im Rahmen des EDIDP-Projekts iMUGS (s.u.) werden Roboterschwärme auf der Grundlage des Tracked Hybrid Modular Infantry System (TheMIS) von Milrem Robotics entwickelt, das auch mit Maschinengewehren und Raketenwerfern bestückt werden kann. Siehe: „Milrem Robotics led consortium awarded 30,6 MEUR by the European Commission to develop a European standardized unmanned ground system" (17.6.2020), www.edrmagazine.eu.

[18] „Die IDF wählen Rafaels Fire Weaver", Spartanat (4. Februar 2020), www.spartanat.com.

[19] „Interview with Yoav Har-Even, president of RAFAEL Advanced Defense Systems", Europäische Sicherheit und Technik (4. Dezember 2019), https://esut.de.

[20] Siehe FN 18.

[21] Marius Pletsch: Mensch-Maschine – EU-Großprojekte zum Manned-Unmanned-Teaming, AUSDRUCK #100 (März 2020), www.imi-online.de.

[22] French-German Research Institute of Saint-Louis (ISL): ISL's Research and Technology serving the future French-German Main Ground Combat System, www.isl.eu.

Autonome Logistik und Produktion: Viele Bereiche, in denen Computersysteme Menschen klar überlegen sind und bereits seit Jahrzehnten Entscheidungen abnehmen, betreffen die Logistik. Die Lagerhaltung und der Transport von Menschen und Material sind eine zentrale Aufgabe des Militärs, das bisweilen effektive Kriegführung mit effektiver Logistik gleichsetzt: „Erfolgreiche Führung beruht primär darauf, zur richtigen Zeit eine hinreichende Menge der richtigen Ressourcen richtig einzusetzen“.[23] Es ist deshalb naheliegend, dass Digitalisierung und auch Künstliche Intelligenz bereits jetzt umfangreich genutzt werden, um Versorgungsketten zu planen und zu implementieren. Methoden des Maschinellen Lernens werden v.a. in der Industrie in großem Maßstab für die präventive und vorausblickende Wartung entwickelt und zunehmend angewandt. Entsprechende Systeme, die auf der Grundlage von Sensordaten und Mustererkennung den Ausfall von Teilen vorhersagen und eine entsprechende Wartung einleiten, werden auch für das Militär angeboten – oft im Zusammenhang mit Assistenzsystemen, welche das Personal u.a. mit erweiterter oder virtueller Realität bei der Wartung unterstützen und damit weniger Anforderungen an die entsprechende Qualifikation stellen.[24]

Autonomen Systeme könnten aber weit hierüber hinaus eine grundsätzliche Wende einläuten, wenn sie nicht nur – wie bereits jetzt – in der Lagerhaltung, sondern auch im Transport zum Einsatz kämen. Das EUISS umschrieb dies 2017 mit folgenden Worten: „Die Frage lautet nun: können neue Technologien zum ersten Mal seit der Industriellen Revolution den Trend zu einem bestätig wachsenden logistischen Tross innerhalb der Streitkräfte umkehren“ indem sie „das Verhältnis zwischen Kampf- und Logistikeinheiten neu bestimmen“ und dadurch „‚mehr Wumms pro Euro‘ [‚more bang for the buck‘] ermöglichen?“[25] Transportflugzeuge und Containerschiffe fahren schon heute mit einer Vielzahl an Assistenzsystemen, welche eine Besatzung nahezu überflüssig machen. Die Industrie entwickelt bereits seit Jahren autonome Zeppelin-Drohnen für den Lufttransport großer Lasten über lange und Quadrokopter für den Transport leichter Frachten über kurze Strecken. Bereits seit 2011 setzen die USA in Afghanistan unbemannte Transporthubschrauber (K-MAX) für mittlere Frachten über mittlere Entfernungen ein. In zahlreichen europäischen Staaten unterstützt das Militär Entwicklungen aus dem Bereich des autonomen Fahrens und experimentiert aktuell v.a. damit, dieses in Konvois umzusetzen, bei denen z.B. nur noch das erste Fahrzeug besetzt ist. Projekte für den taktischen Transport aufs Gefechtsfeld werden auch von der europäischen Rüstungsindustrie u.a. im Kontext des MUM-T verfolgt.

Unter dem Titel „Erweiterte Logistik“ bemüht sich die Europäische Verteidigungsagentur (European Defence Agency, EDA) um das Mapping und die Harmonisierung nationaler und kommerzieller Logistiksysteme und der dabei verwendeten IT-Infrastruktur. Das könnte sich eines Tages als das Rückgrat eines „‚Zentralen Nervensystems‘ für militärische Logistik“[26] entpuppen, in das dann v.a. zivil entwickelte Konzepte rasch eingebunden werden können. Das IT- und KI-gestützte Management von Versorgungsketten war ein Schwerpunkt der Forschungsprogramme FRP7 und Horizon2020 der EU-Kommission. Wie das Europäischen Institut für Sicherheitsstudien (EUISS) bereits 2017 feststellte, „haben kommerzielle Unternehmen ihre Logistik durch wesentliche Investitionen in Forschung und Entwicklung transformiert. Während auch spezifisch militärische Anforderungen bestehen, lassen sich doch viele Technologien und Prozesse aus der kommerziellen Sphäre entlehnen“. Die Studie nennt u.a. die Unternehmen Amazon und DHL, an denen man sich orientieren könne, wobei „unbemannte Fahrzeuge dazu beitragen können, Bestände zu minimieren und damit den Bedarf an Personal für Konvois und die Versorgung der Kampfverbände zu reduzieren“.[27] Vom technischen Stand her wäre eine weitgehend auf autonome Fahrzeuge gestützte militärische Logistik recht schnell umsetzbar, sobald die rechtlichen und administrativen Hürden für das autonome Fahren auch im zivilen, privaten Gebrauch abgebaut werden. Wie wir sehen werden war dies von Anfang an Thema bei den Projekten im Vorfeld und im Rahmen des Europäischen Verteidigungsfonds.

[23] Siehe FN 16.

[24] Die hiermit verbundenen oder geschürten Erwartungen lassen sich z.B. dem Blog des Unternehmens C3.ai entnehmen, das mit Risikokapital aufgebaut wurde und mittlerweile neben der US Air Force auch viele Großunternehmen bedient. Predictive Maintenance ist nur eine der Dienstleistungen, die das Unternehmen Militär und Privatwirtschaft anbietet, eine andere besteht in der KI-gestützten Planung und Verwaltung des Beschaffungswesens, siehe: Philong Duong: AI-Based Predictive Maintenance to Enhance Readiness, Reduce In-Flight Failures (21. Juli 2020), https://c3.ai/.

[25] Torben Schütz and Zoe Stanley-Lockman: Smart logistics for future armed forces, EUISS Brief 30 (November 2017), www.iss.europa.eu.

[26] Ebd.

[27] Ebd.

Herausragende Bedeutung wird in Hinblick auf die Einsatzlogistik auch additiven Verfahren (3D-Druck) zugesprochen, die es v.a. ermöglichen sollen, dass Ersatzteile nicht mehr den weiten Weg von den (heimischen) Produktionsstätten ins Einsatzgebiet transportiert werden müssen, sondern vor Ort hergestellt werden können. Seit 2016 testet die US-Army kleine Drohnen, die vollständig mit einem 3D-Drucker hergestellt werden können. Das unter deutscher Führung stehende Unterstützungs-Bataillon der Operation Resolute Support in Afghanistan betreibt dort den ersten 3D-Drucker der Bundeswehr im Einsatz: „Die im hohen Norden Afghanistans stationierte Truppe verfügt somit über eine effektive und flexible Quelle für die kurzfristige Bereitstellung von Kleinteilen“.[28] Die Europäische Verteidigungsagentur (EDA) versucht hier, gemeinsame Lösungen für die Mitgliedsstaaten zu entwickeln und hat 2018 eine Studie zur additiven Fertigung (Additive Manufacturing, AM) für die logistische Unterstützung erstellt. Bereits im Folgejahr präsentierte sie im Rahmen der NATO-Übung Capable Logistician 2019 gemeinsam mit Frankreich und Spanien einen „vollständig ausgestatteten AM-Container mit dem Ziel, AM für die Landstreitkräfte unter realistischen Bedingungen zu testen und zu demonstrieren“.[29] Aktuell verfolgt sie drei Projekte (AMALIA, AMTEM, PACKOOL), die unterschiedliche Anwendungen unter dem Titel „Additive Manufacturing for logistic support“ verfolgen, sich aber durchaus auch mit „angemessenen Materialien … im Hinblick auf die Produktion neuer Typen von Gefechtsköpfen und Treibstoffen mit verbesserter Leistung“ beschäftigen.[30]

Mit dem Argument der Wettbewerbsfähigkeit unterstützt die EU-Forschungspolitik v.a. auch die Umstellung auf Robotik und Künstliche Intelligenz in der Produktion. Ein wegweisendes Projekt hierfür wurde von der Europäische Kommission ab 2012 finanziert und hat wesentlich die Kooperation von Airbus Defence & Space und dem Robotik-Unternehmen Kuka befördert: Das ebenfalls beteiligte Fraunhofer Institute for Factory Operation and Automation schrieb über das mit 3,6 Mio. Euro von der Kommission vorangetriebene Projekt VALERI: „Die Fabrik der Zukunft hält Einzug in der Luftfahrtindustrie: Ein Konsortium bestehend aus europäischen Forschungseinrichtungen und Industriepartnern entwickelt derzeit mobile und autonom agierende Roboter, die bei der Produktion von Flugzeugteilen zum Einsatz kommen und dort Hand in Hand mit dem Menschen arbeiten“.[31] Die Unternehmen, die für die Industrie 4.0 die Cloud-Infrastrukturen anbieten und stellen, sind tw. deckungsgleich mit jenen, welche entsprechende Dienstleistungen für das Militär erbringen.[32]

Mittelfristig ist vorstellbar, dass die Battle-Management-Software (green IT) mit der Datenverwaltung der militärischen Logistik (white IT) integriert wird. Die EDA arbeitet auch an KI-gestützten Systemen im Beschaffungswesen. Obwohl es sich dabei noch um Zukunftsmusik handeln dürfte, entfaltet die Digitalisierung des Gefechtsfeldes erst dann ihre vollen Potentiale, wenn sie mit der Digitalisierung der Logistik und der Produktion verbunden wird und auch hier dem Menschen Entscheidungen abnimmt. Die Produktion und (militärische) Logistik kann dann unmittelbar der jeweiligen antizipierten Lage auf den Gefechtsfeldern und dem daraus abgeleiteten Bedarf an Ressourcen angepasst werden.

[28] „Innovation in Afghanistan: Ersatzteile per 3D-Drucker“, Bundeswehr (20. August 2020), www.bundeswehr.de.

[29] European Defence Agency (EDA): Enhanced Logistics (10. Juli 2020), https://eda.europa.eu.

[29] European Defence Agency (EDA): Enhanced Logistics (10. Juli 2020), https://eda.europa.eu.

[30] Ebd.

[31] Fraunhofer Institute for Factory Operation and Automation: Robotics in Aircraft Manufacturing (VALERI), www.iff.fraunhofer.de.

[32] Siehe Fußnote 24 zu C3.ai.

Information Warfare: Vor allem Russland, aber auch anderen geopolitischen Rivalen der NATO und der EU wird gegenwärtig eine hybride Kriegführung vorgeworfen, die sich u.a. auf Cyberangriffe und Desinformationskampagnen stützt, welche darauf abzielen, westliche Gesellschaften, die EU und ihre Mitgliedsstaaten zu destabilisieren. Die USA haben mehrfach angekündigt und berichtet, nicht näher definierte Cyberangriffe gegen den Islamischen Staat in Syrien und dem Irak durchzuführen. Auch von Deutschland, Frankreich und anderen Europäischen Staaten bestehen glaubhafte Berichte über bereits durchgeführte, offensive Cyber-Operationen.

Mit der bereits angesprochenen (s. Elektronische Kampfführung) Cyberkriegführung eng verbunden ist die Informationskriegführung, die sich bislang nicht primär auf militärische Strukturen abstützt. Beide stellten einen Schwerpunkt der Übung „European Union Hybrid Exercise Multilayer 18" dar.[33] In den letzten Jahren hat die EU umfangreiche Bemühungen entwickelt, feindliche „Desinformation" zu bekämpfen und stattdessen definierte Zielgruppen mit sog. strategischer Kommunikation zu erreichen. Katalysatoren waren dafür einerseits der Konflikt mit Russland im Zuge der Ukraine-Krise 2014 wie auch das Aufkommen des sog. Islamischen Staates, denen beiden eine gezielte Desinformation vorgeworfen wurde. Die Reaktionen reichten von Bemühungen, entsprechende Profile bei Social-Media-Anbietern sperren zu lassen, bis hin zur eigenen Beeinflussung durch gezielt platzierte Nachrichten.

Zunehmend setzt sich dabei eine Sichtweise durch, in Analogie zur Cybersicherheit die Informationsflüsse kontinuierlich zu überwachen und dabei nicht nur schädliche Software, sondern auch schädliche Informationen zu identifizieren und vom eigenen Informationsraum auszuschließen. Dies geschieht gegenwärtig in Kooperation mit Social-Media-Anbietern wie Facebook, auf die eingewirkt wird, damit sie Inhalte unter Tatbeständen wie „Fake News" oder „Hate Speech" unterbinden. Die Ankündigung des US-Präsidenten Trump, chinesischen Social-Media Anbietern wie TikTok und WeChat den Zugang zum amerikanischen Markt zu verwehren, sind Ausdruck ähnlicher Bemühungen. Das in der Globalstrategie der EU (siehe 3.1.) ausgegebene Ziel, „illegale Inhalte zu überwachen und aus den Medien zu entfernen" ist deshalb nur eine vage, legalistische Andeutung dessen, was perspektivisch bevorsteht.

Hervorgehoben werden muss in diesem Kontext eine Entschließung des Europäischen Parlaments aus dem Jahre 2016 zur „Strategische Kommunikation der EU, um gegen sie gerichteter Propaganda von Dritten entgegenzuwirken". Darin wird festgestellt, „dass Desinformation und Propaganda zur hybriden Kriegsführung gehören" bei der es sich „um eine Kombination aus verdeckten und offenen militärischen und nicht militärischen Maßnahmen handelt". Deshalb werden die Mitgliedsstaaten „nachdrücklich" aufgefordert, „die gemeinsame Nutzung von Kapazitäten sowie die Spionageabwehr zur Abwehr derartiger Maßnahmen zu intensivieren". Von den EU-Institutionen wird gefordert, „streng zu überwachen, aus welchen Quellen die europafeindliche Propaganda finanziert wird" und „Daten und Fakten zum Konsum von Propaganda zu sammeln". Dabei weist das EU-Parlament mit Nachdruck darauf hin „anzuerkennen, dass es sich bei strategischer Kommunikation und bei Informationskriegen nicht nur um eine außenpolitische, sondern auch um ein innenpolitische Angelegenheit handelt" und „zeigt sich besorgt über die zahlreichen EU-internen Multiplikatoren der gegen die Union gerichteten Propaganda". Deshalb sollten die Mitgliedsstaaten „feindliche Informationsmaßnahmen, die in ihrem Hoheitsgebiet durchgeführt werden oder darauf abzielen, ihre Interessen zu untergraben, aktiv, vorbeugend und gemeinsam zu bekämpfen". Dazu gehört u.a. „die Finanzflüsse zu unterbinden, mit denen Einzelpersonen und Einrichtungen finanziert werden sollen, die strategische Kommunikation betreiben und zu Gewalt und Hass anstacheln". Auf der anderen Seite wird u.a. gefordert, „dass der Pluralismus der Medien, lokale Medien, der investigative Journalismus und fremdsprachige Medien, insbesondere in den Sprachen Russisch, Arabisch, Farsi, Türkisch, Urdu und weiteren Sprachen, deren Sprecher der Propaganda in besonderem Maße ausgesetzt sind, besonders ernst genommen werden und zu diesem Zweck ausreichend Ressourcen bereitgestellt werden" müssten. Eine weitere Forderung

[33] Für das zugrundeliegende Szenario siehe: Note from the General Secretariat of the Council „EU HEX-ML 18 (PACE) European Union Hybrid Exercise Multilayer 18 (Parallel and Coordinated Exercise) Exercise Instructions (EXINST) (26. Oktober 2018), https://data.consilium.europa.eu.

besteht darin, „unabhängige Medienunternehmen, Denkfabriken und nichtstaatliche Organisationen insbesondere in der Muttersprache der Zielgruppe unmittelbar [zu] unterstütz[en]“.[34]

Europäische Armeen experimentieren längst mit sog. „Chat-Bots“ und KI-basiertem Micro-Targeting bei ihrer Öffentlichkeitsarbeit und der Rekrutierung der eigenen Bevölkerung. Dies geschieht ganz überwiegend in Zusammenarbeit mit privaten, hierauf spezialisierten Unternehmen.[35] Dabei hat selbstverständlich das Ziel der Information – Zustimmung bzw. Interesse an einer militärischen Laufbahn – Priorität über deren objektiven Wahrheitsgehalt. Ähnliches gilt für die Strategische Kommunikation gegenüber den Bevölkerungen konkurrierender bzw. feindlicher Staaten, die recht offen zum Dissens gegen ihre Regierungen animiert werden sollen. Es sei in diesem Zusammenhang darauf hingewiesen, dass das Täuschen feindlicher Kräfte im Kriegsvölkerrecht als völlig legitime Handlung anerkannt und auch die Propaganda in Friedenszeiten in keiner nennenswerten Weise völkerrechtlich reglementiert ist. Da beides(!) aktuell nicht mehr primär im militärischen Rahmen unter dem Titel „Defence“ vorangetrieben und weiterentwickelt wird,[36] wird der Informationskrieg in dieser Untersuchung im Weiteren keine große Rolle mehr spielen. Deshalb sei an dieser Stelle gesagt, dass der Einsatz Künstlicher Intelligenz in der strategischen Kommunikation dramatischste Auswirkungen haben kann: Wenn verschiedene Parteien mithilfe privatwirtschaftlicher Unternehmen autonome bzw. KI-gestützte Systeme finanzieren, die in zunehmend voneinander abgeschlossenen Informationsräumen Misstrauen und Unzufriedenheit in anderen Gesellschaften verbreiten sollen, hat das potentiell katastrophale Auswirkungen. Anders als im Falle der Cyberkriegführung und der autonomen Waffensysteme bestehen bislang nicht einmal Ansätze einer Diskussion über die internationale Regulierung von Informationskrieg und Propaganda und damit Ideen, wie sich hier eine weitere Eskalation der geopolitisch motivierten und zunehmend automatisch generierten „Fake News“ aufhalten ließe. Hier wäre die Zivilgesellschaft gefragt. Eine internationale, staatsferne Bewegung „blockfreier“ JournalistInnen und Medien könnte hierfür ein Anfang sein.

Europäische Armeen experimentieren längst mit sog. „Chat-Bots“ und KI-basiertem Micro-Targeting bei ihrer Öffentlichkeitsarbeit und der Rekrutierung der eigenen Bevölkerung.

[34] European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)), https://eur-lex.europa.eu.

[35] So berichtet die PR-Agentur Castenow über ihre im Auftrag des Bundesverteidigungsministeriums durchgeführte Kampagne zum Bundeswehreinsatz in Mali: „Der Chatbot spricht die User direkt über den Facebook-Messenger an und berichtet in Echtzeit [...] Ergänzend zu den Social-Aktivitäten wurden zielgruppennahe Medien (Spotify, X-Box, DMAX, Kino) genutzt, um Einsatz und Serie in den Köpfen potentieller Bewerber zu verankern[...] Im Mittelpunkt steht dabei der größte deutschsprachige ChatBot: Die YouTube-Serie MALI nimmt die Community mit in den Auslandseinsatz der Soldaten und beantwortet deren Fragen im direkten Dialog via ChatBot, der im Facebook-Messenger integriert wurde. Der Einsatz der Soldaten wird so zum Teil der Lebensrealität junger Menschen – transparent und so nah, als wäre ein Freund/eine Freundin gerade dort.“ Siehe: www.castenow.de/.

[36] Eine Ausnahme stellt u.a. die Ausschreibung im Rahmen des EDIDP-Programms (s.u.) aus dem Jahr 2020, wo explizit KI-Anwendungen für die Strategische Kommunikation (or logistics planning or airspace management…) angesprochen werden, siehe European Commission (EC): C(2019) 2205 final - Annex.

Inhalt

3. Künstliche Intelligenz in der Genese des EU-Rüstungsfonds

3.1. Strategische Autonomie eines „Globalen Europas"

Im Jahre 2003 verabschiedete der Rat der Europäischen Union erstmals eine gemeinsame außenpolitische Strategie (ESS) unter dem Titel „Ein sicheres Europa in einer besseren Welt". Bereits der Titel deutet einen letztlich globalen Gestaltungsanspruch des neuen Akteurs an, der geradezu zwangsläufig die Rolle einer Weltmacht einnehmen müsse: „Als Zusammenschluss von 25 Staaten mit über 450 Millionen Einwohnern, die ein Viertel des Bruttosozialprodukts (BSP) weltweit erwirtschaften, ist die Europäische Union, der zudem ein umfangreiches Instrumentarium zur Verfügung steht, zwangsläufig ein globaler Akteur".[37] Drei Jahre später veröffentlichte die European Defence Agency (EDA) ihre Initial Long Term Vision (ILTV), welche die militärischen Voraussetzungen zur Umsetzung dieser Strategie auslotete – und sich deutlich skeptischer zeigte. Bereits im zweiten Absatz wird die Demographie angesprochen und später weiter ausgeführt: „Europa wird zurückgehalten durch niedrige Geburtenraten (gegenwärtig 1,5) […] 2025 werden Europäer*innen nur noch 6% der Welbevölkerung ausmachen […] Der Rekrutierungspool der Streitkräfte (16-30 Jahre) wird bis 2025 um über 15% zurückgehen". Um trotzdem globale Handlungsfähigkeit aufzubauen und zu erhalten, betont die ILTV die Rolle von Wissenschaft und Technologie, insbesondere der Informationstechnologie, um „das nötige Maß an Informationsüberlegenheit" zu erhalten, das es ermöglicht, sich auch mit begrenzter, aber präziser und optimal dosierter kinetischer Energie zu behaupten: „Kriegführung wurde als Kombination von Aufklärung und kinetischer Energie beschrieben. Die Eröffnungskampagnen in Afghanistan und Irak haben ohne Zweifel bestätigt, dass wir eine Transformation vom Zeitalter der industriellen ins Zeitalter der informationallen Kriege erleben – in dem Aufklärung (oder Wissen, Information) eine immer wichtigere Ressource für erfolgreiche Operationen wird [...]".[38]

Sowohl in der ESS als auch der ILTV spielten Szenarien einer klassischen, zwischenstaatlichen Konfrontation zwischen annähernd gleichwertigen Gegner ansonsten allerdings keine nennenswerte Rolle. Zwar wird auf den absehbaren wirtschaftliche Aufstieg Chinas und Indiens ebenso hingewiesen, wie auf die Notwendigkeit, die eigene rüstungsindustrielle Basis gegenüber den USA zu erhalten und zu stärken. Als Opponenten bei militärischen Konfrontationen werden jedoch primär nicht-staatliche Akteure gesehen und als mögliche Einsatzgebiete sog. scheiternde Staaten, in denen die EU in Vertretung einer weitgehend konsensualen Staatengemeinschaft interveniert. Die Fähigkeit hierzu untermauert demnach allerdings die Rolle der aufstrebenden Weltmacht EU gegenüber den USA, China und anderen Akteuren, die sich als global Player verstehen oder zu positionieren versuchen. Damit ging in den frühen Strategiepapieren ein Technologie-Verständnis einher, das sich noch deutlich von der Tech-Geopolitik unterscheidet, die sich aktuell durchsetzt.
Als zentrale Akteure werden dabei private Anbieter gesehen, die sich politischer Steuerung weitgehend entziehen und deren Dienste und Infrastrukturen auch von konkurrierenden Staaten und nicht-staatlichen Akteuren nahezu gleichberechtigt genutzt werden können: „Die Bereitstellung von Technologie und Wissen vollzieht sich jenseits der Kontrolle durch Regierungen, wobei der kommerzielle Sektor tonangebend ist […] Unsere eigenen, universellen Kommunikationsmittel werden bereits umfassend von unseren Gegenern ausgenutzt, sowohl als Plattform für ihre Ideen und Propaganda, als auch als Kommunikationsnetzwerke". Anders als in den aktuellen Diskursen der „digitalen Souveränität" wird nicht einmal darüber nachgedacht, ob sich dies ändern ließe oder dies auch nur wünschenswert wäre. Im Gegenteil herrscht z.B. in der ILTV noch das liberale Paradigma der Interdependenz vor:

[37] *Council of the European Union: European Security Strategy – A Secure Europe in a Better World (2003), https://data.consilium.europa.eu.*

[38] *EDA: An initial long-term vision of European defence capability and capacity needs (2006), www.consilium.europa.eu.*

„All dies hat – zumindest im europäischen Kontext und in der absehbaren Zukunft – die Plausibilität von Szenarien reduziert, die einen traditionellen, zwischenstaatlichen Krieg beinhalten, bei dem sich vergleichbare, konventionelle Truppen gegenüberstehen".

Insbesondere im Zuge der Umsetzung der außen- und verteidigungspolitischen Neuerungen des 2009 in Kraft getretenen Lissabon-Vertrages wurde jedoch bereits in den Folgejahren offener von internationaler, geopolitischer Konkurrenz gesprochen sowie von der Notwendigkeit, europäische Interessen auch offensiv zu vertreten. So begründete die damalige EU-Außenbeauftragte Catherine Ashton den Aufbau des Europäischen Auswärtigen Dienstes (EEAS) und die Notwendigkeit, dass Europa seine Fähigkeiten bündeln und mit einer Stimme sprechen müsse, in einer Rede vor dem Europäischen Parlament am 10. März 2010 explizit mit „dem Aufstieg Chinas und anderer als führende internationale Player […] Europas Anteil an der Weltbevölkerung ist im letzten Jahrhundert von 25% um 7% gefallen. In den vergangenen 60 Jahren ist unser Anteil am globalen BIP von 28% auf 21% gesunken. Die Volkswirtschaften Chinas, Indiens und anderer Staaten laufen uns mit 10% Wachstum im Jahr davon. Wirtschaftliches Gewicht übersetzen sich in politischen Einfluss und Selbstbewusstsein. Man kann es überall spüren: von den Verhandlungen über den Klimawandel oder zum Iran bis hin zu großen Energie-Abkommen in Afrika oder Zentralasien. Wenn wir an einem Strang ziehen, können wir unsere Interessen wahren. Wenn nicht, werden andere für uns entscheiden. Es ist wirklich so einfach".[39]

Etwa zeitgleich mit dem EEAS nahm 2011 die Group on Grand Strategy ihre Arbeit auf. Sie vereinigte einige der wichtigsten Strateg*innen aus der EU sowie Vertreter*innen der wichtigsten Denkfabriken. Da es sich nicht um eine offizielle EU-Institution handelt, brauchte sie bei ihren Veröffentlichungen kein Blatt vor den Mund zu nehmen. Einer ihrer Gründer, James Rogers, formulierte in seinem Vorschlag für eine „Neue Geographie Europäischer Macht": „Während sich einzelne europäische Mächte vermutlich weiterhin in Bezug auf wirtschaftlichen Output und Militärausgaben in den oberen Rängen werden halten können, wird der Abstand zwischen ihnen und den fünf größten Akteuren – China, Indien, die USA, Brasilien und Russland – absehbar zunehmen. Darüber hinaus wird sich die Position der europäischen Mächte relativ zu einigen kleineren Mächten – wie der Türkei, Mexiko, Indonesien, Iran, Nigeria, Südafrika – ebenfalls absehbar verschlechtern. Diese aufstrebenden Mächte schenken ihrem ökonomischen und politischen Zugriff auf Geographien beträchtliche Aufmerksamkeit, nicht nur innerhalb ihrer eigenen Territorien, sondern auch jenseits dieser". Ähnlich solle sich zukünftig auch die EU verhalten und eine eigene Einflusssphäre definieren, erschließen und gegen „ihre Widersacher" verteidigen: „Angesichts der Tatsache, das bestimmte Mächte versucht haben, sich in Schlüsselregionen Vorteile zu verschaffen und dort einzunisten, sollte die Europäische Union mehr tun, um das minimale geographische Gebiet, das für die weitere Expansion ihrer Wirtschaft nötig ist, abzusichern".[40] Diese „Grand Area" der Europäischen Union soll „das minimale geographische Gebiet, das für die weitere Expansion ihrer Wirtschaft nötig ist", umfassen und beinhaltet große Teile Afrikas, die ölreiche kaspische Region, den Mittleren Osten sowie große Teile des Indischen Ozeans, wo es gilt, Schiffahrts- und Handelsrouten zu kontrollieren. Sie definiert sich durch fünf Kriterien. Eines davon besteht darin, dass sie „alle grundlegenden Ressourcen bereitstellt, um die europäische Produktion und zukünftige industrielle Bedürfnisse zu versorgen"; eine weitere darin, dass die „Europäische Union darauf hinarbeiten kann, diese kosteneffizient zu verteidigen, indem sie ihre Gemeinsame Sicherheits- und Verteidigungspolitik entsprechend ausbaut".

In den Jahren seit 2011 ist der Kampf um Einflusssphären zwischen den europäischen Mächten, ihren Verbündeten und Konkurrenten zumindest in Syrien und der Ukraine so weit eskaliert, dass sich von ihnen unterstützte Konfliktparteien vor Ort offen bekämpften. Seit dem wird v.a. Russland eine aktive hybride Kriegführung vorgeworfen, die auf die Destabilisierung der Europäischen Union und ihrer Gesellschaften abziele. Damit spielen im strategischen Diskurs auch Szenarien einer unmittelbaren militärischen Konfrontation zwischen der NATO bzw. der EU und Russland eine verstärkte Rolle. Auch der zunehmend aggressiv geführte Diskurs,

[39] Catherine Ashton, High Representative of the Union for Foreign Affairs and Security Policy: Rede vor dem Europäischen Parlament am 10. März 2010 in Straßburg, www.europarl.europa.eu.

[40] James Rogers: A new geography of European Power, Egmont Paper #42 (Januar 2011), http://aei.pitt.edu.

wonach die EU über eigene Atomwaffen verfügen müsse, unterstreicht, dass sich die militärische Planung nicht nur auf Krisenmanagementoperationen und Konfrontationen mit militärisch-technisch klar unterlegenen Gegnern beschränkt, sondern auch eine militärische Konfrontation mit anderen Weltmächten nicht (mehr) ausgeschlossen wird.

Diese neue Ausrichtung spiegelt sich v.a. in der 2016 verabschiedeten Globalstrategie (Global Strategy for European Foreign and Security Policy) wieder,[41] welche die ESS von 2003 ablöste und im direkten Vergleich einen deutlich anderen Zungenschlag aufweist. Bereits in der Einleitung der damaligen EU-Außenbeauftragten Federica Mogherini wird die Bandbreite der Herausforderungen so beschrieben: „Unsere Außen- und Sicherheitspolitik muss auf globale Spannungen und lokale Dynamiken reagieren, sie muss mit Großmächten sowie zunehmend brüchigen Identitäten zurechtkommen". Auch im Dokument selbst wird nicht nur in erstaunlicher Offenheit eine verstärkte militärische Präsenz im süd- und ostasiatischen Raum und die Aufrüstung der dortigen Konkurrenten Chinas angekündigt, sondern auch die Notwendigkeit angedeutet, sich auf harte Konfrontationen in Europa und der unmittelbaren Nachbarschaft vorzubereiten: „Während die NATO besteht, um ihre Mitglieder – von denen die meisten europäisch sind – gegen Angriffe von Außen zu verteidigen, müssen sich die Europäer besser ausrüsten, trainieren und organisieren, um entschieden zu diesen gemeinsamen Bemühungen beizutragen und auch selbstständig zu handeln, wo und wenn es nötig ist". Als Ziel wird sowohl im Vorwort wie auch an verschiedenen Stellen im Dokument selbst die „strategische Autonomie" angegeben, die u.a. bedeutet, dass die EU ihren Zugang zu Rohstoffen und Energie sichert und eine eigenständige rüstungsindustrielle Basis für alle denkbaren militärischen Fähigkeiten schafft: „Verteidigungsfähigkeiten im gesamten Spektrum sind nötig, um auf externe Krisen zu reagieren, die Fähigkeiten unserer Partner auszubauen und Europas Sicherheit zu garantieren".

Insofern deutet sich in der Globalstrategie bereits der Paradigmenwechsel zur Tech-Geopolitik an, indem zunehmend autonome Produktionsketten in der Rüstungsindustrie angestrebt und eine aktive, geopolitisch motivierte Technologie- und Industriepolitik als Voraussetzung für „strategische Autonomie" und damit die „Sicherheit" Europas formuliert wird: „Dies beinhaltet die Stärkung unserer technologischen Fähigkeiten, die darauf abzielen, Bedrohungen abzufedern, die Resilienz kritischer Infrastrukturen, Netzwerke und Dienste zu erhöhen und die Cyberkriminalität einzudämmen. Das bedeutet, innovative Informations- und Kommunikationstechnologien (IKT) zu fördern, welche die Verfügbarkeit und Integrität unserer Daten sichern, und zugleich innerhalb des europäischen Digitalraums Sicherheit herzustellen durch Strategien zur räumlichen Verteilung von Datenzentren und zur Zertifizierung von digitalen Produkten und Dienstleistungen". Die Vorstellung eines „Europäischen Digitalraums" scheint hier noch in einem gewissen Spannungsverhältnis zum „freien und sicheren Internet" zu stehen, für das sich die EU ebenfalls stark machen solle. Die im selben Strategiedokument ausgegebene Aufgabenstellung, „illegale Inhalte zu überwachen und aus den Medien zu enfernen" jedoch unterstreicht, dass hier bereits wesentliche Akzentverschiebungen hin zur Digitalen Souveränität stattgefunden haben.

[41] European External Action Service: Shared Vision, Common Action - A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy, https://eeas.europa.eu.

„Die Bereitstellung von Technologie und Wissen vollzieht sich jenseits der Kontrolle durch Regierungen, wobei der kommerzielle Sektor tonangebend ist“

Inhalt

3.2. Der Fähigkeits-Entwicklungsplan

Quasi zeitgleich mit der Veröffentlichung der EU Globalstrategie (EUSG) begann die Revision des Fähigkeiten-Entwicklungs-Plans (Capability Development Plan CDP), der darauf abzielt, „den Entscheidungsprozess auf Ebene der EU und der Mitgliedsstaaten in Bezug auf die Entwicklung militärischer Fähigkeiten zu unterstützen und damit zu mehr Kohärenz in der Verteidigungsplanung der Staaten beizutragen".[42] Der erste CDP war bereits 2008 veröffentlicht worden, gefolgt von früheren Revisionen 2012 und 2014. Die darin identifizierten Defizite allerdings „basierten bislang v.a. auf [stattgefundenen] Missionen der Gemeinsamen Sicherheits- und Verteidigungspolitik". Mit der Globalstrategie wurde jedoch ein neues „Set möglicher Szenarios für die militärische Planung [ins Spiel gebracht]: Die Notwendigkeit, die Union und ihre Bürger zu schützen", so Daniel Fiott vom EUISS.[43] Dies bedeutet, dass sich Rüstung nicht mehr primär auf sog. Krisenmanagement in asymmetrischen Konflikten fokussieren soll, sondern auch auf Cyber-Angriffe und hybride Kriegführung durch militärisch und technologisch gleichwertigere Gegner sowie die klassische Verteidigung im Sinne eines handfesten Krieges mit einem mehr oder weniger gleichwertigen Gegner. Da Rüstungsprojekte im Bereich der klassischen Verteidigung bislang primär im Rahmen der NATO einerseits, v.a. aber auch in nationaler Verantwortung durchgeführt wurden, bedeutet dies mehr als nur eine graduelle Aufwertung des CDP. Er beschränkt sich nicht mehr auf die über die Verteidigung hinausgehenden Fähigkeiten der Mitgliedsstaaten, sich an EU-Missionen weltweit durch einzelne Kompetenzen zu beteiligen, sondern fordert letztlich eine grundlegende Reform und Modernisierung der jeweiligen Streitkräfte im Sinne einer gemeinsamen europäischen Verteidigung durch Beteiligung an gemeinsamen Rüstungsprojekten und Spezialisierung auf einzelne Fähigkeiten. Die Voraussetzung dafür wäre letztlich eine möglichst umfangreiche und an zivile Logistik und Produktion angeschlossene Combat Cloud – welche die deutsch-französische Vorherrschaft in einer „Europäischen Verteidigungsidentität" zementieren würde – und dementsprechend umkämpft ist.

Ein Mechanismus, der diese Kooperation und Modernisierung vorantreiben soll, ist ein „koordinierter jährlicher Verteidigungsbericht" (Coordinated Annual Review on Defence, CARD), der ebenfalls Ende 2016 vom Rat beschlossen wurde. CARD soll eine „Vogelperspektive" über die Rüstungsausgaben und -Projekte der Mitgliedsstaaten liefern und so „die Konsistenz der Verteidigungsplanung der Mitgliedsstaaten fördern".[44] Die EDA hat daraufhin in Kooperation mit dem Europäischen Auswärtigen Dienst eine Methodologie erarbeitet und diese ab 2017 – parallel zur Erarbeitung des CDP – für ein Jahr in einem Versuchslauf umgesetzt, der noch auf dem CDP von 2014 beruhte. Demnach besteht ein Berichts-Zyklus aus vier Stufen. Zunächst werden (1.) die bestehenden Informationen aus den einzelnen Mitgliedsstaaten aus den Datenbanken der EDA von dieser aufgearbeitet und dienen dann (2.) als Grundlage für einen bilateralen Dialog mit den Mitgliedsstaaten, um die erstellte Analyse der EDA zu validieren und zu vervollständigen. Darauf folgt (3.) die alle Mitgliedsstaaten übergreifende Analyse, in der die EDA „Trends in den Verteidigungsausgaben … und Möglichkeiten zur Kooperation bei Verteidigungsprojekten identifiziert". Hieraus wird nach erneuter Diskussion mit den Mitgliedsstaaten (4.) ein Bericht mit Empfehlungen formuliert, der dem Rat vorgelegt wird. Dabei soll CARD „nicht nur eine Momentaufnahme der gegenwärtigen Verteidigungslandschaft liefern. Er soll auch auf wahrscheinliche zukünftige Entwicklungen … wie technologische Trends und die industriellen Fähigkeiten hinweisen, um sich diese zunutze zu machen".[45] Der erste vollständige CARD-Zyklus sollte im September 2019 beginnen, auf dem in Hinblick auf Rüstung deutlich ausgeweiteten CDP von 2018 beruhen und den Mitgliedsstaaten Ende 2020 seinen Bericht vorlegen.[46]

[42] EDA: Fact sheet Capability Development Plan (28 June 2018), www.eda.europa.eu.

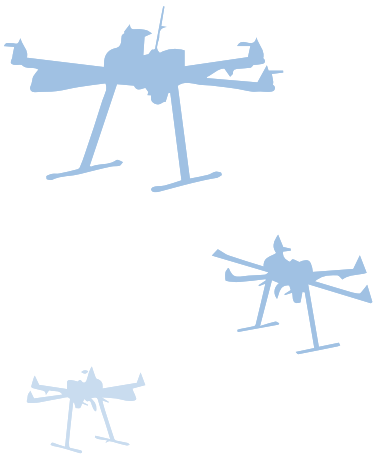
[43] Daniel Fiott: EU defence capability development – Plans, priorities, projects, EUISS Brief #6 (June 2018), www.iss.europa.eu.

[44] EDA: CARD's on the table, European Defence Matters #18 (November 2019), www.eda.europa.eu.

[45] Ebd.

[46] Council of the EU: Council Conclusions on Security and Defence (17 Juni 2019), www.consilium.europa.eu.

Der im Juni 2018 vorgestellte CDP identifizierte „ein Paket von Prioritäten für die Fähigkeitsentwicklung … mit einer verstärkten Berücksichtigung der High-End-Kriegführung“. Es ist wichtig festzuhalten, dass diese Prioritäten eine „kurzfristige Perspektive“ (basierend auf Erfahrungen und Defiziten der GSVP-Missionen), eine „mittelfristige Perspektive“ (2018-2030) und eine „längerfristige Perspektive“ einschließen. Zusammengefasst jedoch erscheinen die elf identifizierten und beschlossenen „Prioritäten“ entschlossen und demonstrieren den klaren Willen, sich für einen umfassenden Krieg in der Zukunft vorzubereiten und zu rüsten. Eine der Prioritäten ist beispielsweise mit dem Titel „Luftkampffähigkeit“ überschrieben und zielt u.a. auf die „Luftüberlegenheit“, ballistische Raketenabwehr und A2/AD-Fähigkeiten – also die Möglichkeit, anderen Kräften den Zugang zu einem Gebiet zu verwehren.



Inhalt

3.3. Autonome Syteme und KI in den „Prioritäten“

Nahezu alle elf CDP-Prioritäten weisen in ihrer näheren Beschreibung[47] – mehr oder weniger enge – Bezüge zu Digitalisierung und oft auch KI auf. Dies gilt insbesondere für die “Fähigkeiten zu reaktiven Cyber-Operationen”, welche u.a. “Technologien für das Situationsbewusstsein im Cyberraum, defensive Cyber-Technologien, autonome Systeme zur Cyber-Sicherheit, und Fähigkeiten zur Cyber-Aufklärung” umfassen, bei denen es um die schnelle Analyse großer Mengen Code und Daten geht. Unter den “Fähigkeiten zum Bodenkampf” werden unbemannte Systeme prominent erwähnt und herausgestellt: „Alle Fähigkeiten [unter diesem Titel] werden in einem operativen Umfeld gedacht, das sowohl bemannte, als auch unbemannte Systeme sowie das damit verbundene MUM-T umfasst“. Ähnliches gilt für die Bereiche der „Bewegungsfreiheit der Marine“, der „Unterwasser-Überwachung“, der Domäne Weltraum und unter dem Titel „Luftüberlegenheit“. Auch zu letzterem wird explizit festgehalten: „zukünftig werden alle diese [Luftkampfsysteme] in der Zusammenarbeit von bemannten und unbemannten Systeme operieren, die in größere Gesamtsysteme integriert sein werden“. Explizite Erwähnung findet Künstliche Intelligenz bei der Frage der „Integration militärischer Luftfähigkeiten in eine sich verändernde Luftfahrt“, wo „automatisierte Techniken zur Luftraumverwaltung“ prognostiziert und „die Notwendigkeit“ konstatiert wird, „bestehenden und zukünftigen bemannten und unbemannten Luftfahrzeugen Zugang zum europäischen Luftraum für Zwecke der Ausbildung, des Transports, der Verlegung und zu operationelle Zwecke zu sichern“. Ohne prominente Hervorhebung werden wie hier unbemannte Transportkapazitäten für den taktischen und strategischen Lufttransport sowie insbesondere für die medizinische Evakuierung an verschiedenen Stellen antizipiert. Darüber hinaus finden autonome Systeme und Künstliche Intelligenz prominente Erwähnung unter der Container-Kategorie der „domänenübergreifenden Fähigkeiten“, wo ohne konkreten Anwendungsbezug Technologien aufgelistet werden, welche die EU für ihre zukünftige Kriegführung als zentral erachtet: „Künstliche Intelligenz (KI), unbemannte Systeme, ferngesteuerte oder autonome medizinische Systeme, autonome oder automatisierte Steuerung [guidance, navigation and control, GNC], Entscheidungssysteme für bemannte und unbemannte Systeme, Schwarmsteuerung, fortschrittliche Werkstoffe, Prozesse und Technologien“.[48]

[47] *EDA: The EU Capability Development Priorities (2018 CDP revision), www.eda.europa.eu.*

[48] *Ebd.*

Inhalt

3.4. Der Europäische Verteidigungs-Aktionsplan

Der neue Zungenschlag der EU Global Strategy vom November 2016 kam nicht von ungefähr und stand mit anderen, konkreten Initiativen in Zusammenhang, die letztlich zum Aufbau eines eigenen EU-Rüstungshaushalts und der Forcierung gemeinsamer Rüstungsprojekte führten. Die „Rede zur Lage der Union" (State of the European Union speech) des damaligen Kommissionspräsidenten Juncker im September 2016 trug bereits im Titel den Anspruch, ein „Europa, das schützt, stärkt und verteidigt" aufzubauen. Darin hieß es unter anderem mit Blick damals auf Syrien: „Europa muss mehr Härte zeigen. Dies gilt vor allem in unserer Verteidigungspolitik […] Eine starke europäische Verteidigung braucht eine innovative europäische Rüstungsindustrie. Deshalb werden wir noch vor Jahresende einen Europäischen Verteidigungsfonds vorschlagen, der unserer Forschung und Innovation einen kräftigen Schub verleiht." Pläne hierfür sollten noch im selben Jahr als Teil eines Europäischen Verteidigungs-Aktionsplans (European defence action plan, EDAP) vorgelegt werden.[49] Der EDAP erschien im November 2016 und verweist auf die deutlich höheren Rüstungsausgaben der USA und die „in beispiellosem Ausmaß" gestiegenen Rüstungsetats u.a. Chinas, Russlands und Saudi Arabiens und fordert ganz im Sinne der strategischen Autonomie, „dass die Mitgliedstaaten gemeinsam das gesamte Spektrum der Land-, Luft-, Raumfahrt- und Seefähigkeiten erwerben, entwickeln und erhalten". Explizit orientiert er sich an den in der Globalstrategie formulierten Prioritäten: „Nachrichtengewinnung, Überwachung und Aufklärung, ferngesteuerte Flugsysteme, Satellitenkommunikation und autonomer Zugang zum Weltraum und zu ständiger Erdbeobachtung; militärische Spitzenfähigkeiten einschließlich der strategischen Grundvoraussetzungen sowie Fähigkeiten zur Gewährleistung von Cybersicherheit und maritimer Sicherheit".[50]

Während ein großer Teil des EDAP von der militärischen Relevanz der EU-Weltraumprogramme handelt und sich mit der Frage auseinandersetzt, wie bestehende (zivile) Finanzprogramme wie etwa der Europäische Fonds für strategische Investitionen (EFSI) oder gar Erasmus+ genutzt werden können, um Lieferketten einer High-Tech-Rüstungsindustrie auszubauen und mit Personal zu versorgen, dreht er sich im Kern um den Europäischen Verteidigungsfonds. Dieser solle aus zwei „Fenstern" bestehen. Das eine sollte auf gemeinsame Forschungsprojekte ausgerichtet sein und für die Jahre 2017-2019 mit 90 Mio. Euro ausgestattet sein (PADR, s. 3.6.). Das andere Fenster dient der Entwicklung von Fähigkeiten und soll Anreize schaffen, dass sich Mitgliedsstaaten auf einzelne Fähigkeiten konzentrieren und hierfür gemeinsame Technologien einführen bzw. Prototypen oder Machbarkeits-Studien auf dem (gemeinsamen) europäischen Rüstungsmarkt beauftragen (EDIDP s. 3.7.). Ein gemeinsamer „Koordinierungsmechanismus" soll gewährleisten, dass beide Fenster ineinander greifen, dass also die gemeinsam angestoßene Forschung sich auch in die gemeinsame Entwicklung und gemeinsame Rüstungsprojekte übersetzt. Diese anvisierte Übersetzung gemeinsamer Forschungs- in konkrete Rüstungsprojekte ist eine wesentliche Innovation gegenüber den vorangegangenen Forschungsprogrammen der Kommission (FP7 und Horizon 2020). Der EDAP argumentiert dabei primär mit Einsparungen und Effizienz: nicht alle Staaten für sich sollen technologische und industrielle Fähigkeiten entwickeln und aufrechterhalten, indem sie kleine Margen bei ihren jeweiligen nationalen Anbietern bestellen.[51] Zugleich ist jedoch offensichtlich, dass hier auch die Grundlagen einer v.a. von Deutschland und Frankreich vorangetriebenen EU-Armee von der industriellen Basis her geschaffen und ein von beiden Ländern dominierter Rüstungsmarkt ausgebaut werden soll, dessen Wertschöpfungsketten sich über die Union verteilen und zugleich weitmöglichst auf diese beschränkt bleiben.

[49] *Jean-Claude Juncker: State of the Union 2016, https://publications.europa.eu.*

[50] *European Commission: European Defence Action Plan (COM(2016) 950 final), https://eur-lex.europa.eu.*

[51] *Ebd.*

Inhalt

3.5 Das Pilotprojekt

Zur Allokation der 90 Mio. Euro für Forschungsprogramme, die zum Aufbau des EDF beitragen sollten, wurde 2017 eine „Vorbereitende Maßnahme im Bereich Verteidigungsforschung“ (Preparatory Action on Defence Research, PADR) ins Leben gerufen. Diese wiederum basierte auf einem „Pilotprojekt“, das die EDA ebenfalls 2016 auf Initiative des Europäischen Parlaments ins Leben gerufen hatte. Dieses unterstützte für den überschaubaren Betrag von insgesamt 1,4 Mio € drei Aktivitäten, die allesamt einen Bezug zu Künstlicher Intelligenz haben und auf umfassender ziviler Forschung aufbauen konnten, diese jedoch unter explizit militärischen Prämissen weiterentwickeln sollten:

Unmanned Heterogeneous Swarm of Sensor Platforms (EuroSWARM)
Das Projekt EuroSWARM wurde mit insgesamt 434.000 € finanziert und zielte auf das Design und die Kooperation von mobilen und stationären luft- und bodengebundenen Sensorplattformen ab. Ein Teilbereich davon war die autonome Allokation von Aufgaben und Zielen auch unter der Bedingung, dass einzelne Plattformen oder Sensoren ausfallen bzw. ein unerwartetes Verhalten zeigen. Ein weiterer Teilbereich war die Fusion der Sensordaten zur Identifikation und Verfolgung möglicher Ziele sowie zur Herstellung eines Lagebildes. Versuche wurden mit kommerziell verfügbaren Plattformen sowohl innerhalb als auch außerhalb von Gebäuden durchgeführt.[52]

Beteiligt waren neben der Swedische Agentur für Verteidigungsforschung (Totalförsvarets forskningsinstitut, FOI) die französische Luftfahrtforschungsbehörde ONERA (Office National d'Etudes et de Recherches Aérospatiales) sowie die Universitäten Patras (Griechenland) und Cranfield (GB). Die Universität Patras beschreibt das Szenario folgendermaßen: „Ein Szenario, das den Interessen von militärischen und polizeilichen Akteuren entspricht, besteht aus einem Gebiet großer Relevanz, das permanent überwacht werden muss. Es wird [hier] angenommen, dass das Szenario in einem Gefechtsfeld in einem Konflikt mit einem gut bewaffneten und kompetenten Gegner stattfindet […] Da das Gelände die Sichtbarkeit des geschützten Gebietes einschränkt, ist eine zentralisierte Sensorik ineffizient. Stattdessen sollten die Wachmannschaften bodengebundene Sensoren verwenden, die großflächig um das Lager verteilt sind und frühzeitig Anzeichen für gegnerische Aufklärung oder Verbände erkennen können. Die bodengebundenen Sensoren erfassen die Präsenz von Menschen, Fahrzeugen und Tieren und geben sofort Alarm, wenn potentielle Ziele in der Umgebung sind“. Falls die stationären Sensoren verdächtige Bewegungen wahrnehmen, sollen die mobilen unbemannten Systeme ausschwärmen und einerseits dem Wachpersonal Bilder (und andere Sensordaten) liefern und zugleich selbst über die Fähigkeiten zur „Erkennung verdächtigen Verhaltens durch das Ziel“ verfügen.[53]
Das Centre of Autonomous & Cyberphysical Systems der Cranfield University, die u.a. aus dem militärisch geprägten College of Aeronautics hervorgeht und über einen eigenen Forschungsflughafen verfügt, erhielt mit 130.000 € die umfangreichsten Zuwendungen im Rahmen von EuroSWARM. Es nennt als Auftraggeber für sonstige Projekte u.a. die Rüstungsunternehmen BAE Systems, Lockheed Martin, Leonardo, Airbus und Thales sowie die Europäische Weltraumagentur. Seine Forschungsschwerpunkte beschreibt das Centre u.a. so: „Gegenwärtige Forschung beinhaltet die luftgestützte Überwachung des Verkehrs am Boden durch autonome Sensorplattformen hinsichtlich versteckter Bedrohungen, die Entwicklung eines Untersuchungsrahmens zum Verständnis des Verhaltens multipler unbemannter Luftfahrzeuge und die Entwicklung von Algorithmen zur Kollisionsvermeidung und Wegplanung unbemannter Fahrzeuge, die jenseits des menschlichen Gesichtsfeldes operieren“.[54]

[52] EDA: PP Call PP-15-INR-01 Information on the awarded project, www.eda.europa.eu.

[53] „EUROSWARM“, www.aml.euroswarm.upatras.gr.

[54] „Centre for Autonomous and Cyber-Physical Systems“, www.cranfield.ac.uk.

Inside Building Awareness and Navigation for Urban Warfare (SPIDER)

Das Projekt SPIDER zielt darauf ab, „Operationen der urbane Kriegführung zu unterstützen (urbaner Kampf oder Geiselsituationen), indem es zum verbesserten Situationsbewusstsein in Gebäuden beitragen“ soll. Hierzu sollen einerseits Radar-Sensoren außerhalb der betreffenden Gebäude zum Einsatz kommen, um von dort die Präsenz und Bewegungen von Menschen innerhalb des Gebäudes zu registrieren. Andererseits sollen Roboter ins Innere der Gebäude vordringen, „um in Echtzeit eine Karte der Innenräume zur Verfügung zu stellen“ und den Soldaten vor dem Zugriff Bilder aus dem Inneren liefern zu können.[55] Auch hier sollen die Daten der verschiedenen Sensoren fusioniert werden. Eine zentrale Aufgabenstellung für das unbemannte Fahrzeug im Inneren des Gebäudes besteht in der simultanen Selbstlokalisierung und Kartierung (simultaneous localization and mapping, SLAM), das generell eine zentrale Fragestellung für autonome Systeme ist, sofern diese in unbekannten Umgebungen agieren. Das SLAM stellt hohe Bedingungen an das maschinelle Sehen und die Objekterkennung. Zugleich sind damit sehr allgemeine Fragestellungen der Selbstwahrnehmung und der Modellierung der Umwelt verbunden, welche die KI-Forschung grundsätzlich beschäftigen und bei denen bereits länger große Durchbrüche erwartet werden, die aber bislang weitgehend ausgeblieben sind.

Dass entsprechende Durchbrüche mit SPIDER angepeilt wurden, ist zu bezweifeln, denn auch dieses Projekt weist mit 433.000 € noch eine überschaubare Finanzierung und Reichweite auf. Größter Empfänger ist hier das portugisische Unternehmen TEKEVER, das bereits in den vorangegangenen Jahren an zahlreichen „zivilen“ Forschungsprojekten der EU-Kommission beteiligt war. Bereits ab 2004 erhielt das Unternehmen von der EU-Kommission im Rahmen des Projekts AVITRACK Förderung für die Überwachung des Flughafen-Umfeldes, „um die regulären Handlungen zu modellieren, zu interpretieren und zu überprüfen und Objekte und Personen zu verfolgen“, indem „Echtzeit-Informationen aus Video- und Infrarot-Aufnahmen genutzt werden“.[56] Ab 2012 wurde das Unternehmen u.a. für Forschung im Bereich neuartiger Gyroskope (Projekt AGEN)[57] und Flügelformen[58] speziell für UAVs finanziert. 2013 folgten eine Studie zur Nutzung privater Smartphones und anderer mobiler Endgeräte für die Lagebilderstellung von Sicherheitsbehörden (iSAR+) und ein (etwas utopisches) Projekt zur neuartigen Steuerung von Flugzeugen durch neuronale Aktivitäten (BRAINFLIGHT).[59] Parallel zur Beteiligung am EDA-Pilotproject SPIDER begann die von der EU finanzierte Forschung im Rahmen der Projekts ROBORDER, „ein vollständig funktionsfähiges autonomes System zur Grenzüberwachung mit unbemannten Luft-, Boden- und Unterwasser-Systemen, die sowohl eigenständig, wie auch in Schwärmen agieren können und multimodale Sensoren in einem interoperablen Netzwerk integrieren“. Seit 2019 ist TEKEVER unter der Leitung von Airbus Defence and Space am „zivilen“ EU-Forschungsprojekt ARESIBO beteiligt, welches mittels erweiterter Realität die „Zusammenarbeit zwischen Menschen und (stationären und mobilen) Sensoren“ optimieren und das Situationsbewusstsein u.a. durch „angepasste Verarbeitung der Sensordaten, Korrelationen zwischen heterogenen Daten und Informationen und die Generierung von Wissen durch Deep Learning“ verbessern soll.[60] Nach eigenen Angaben ist TEKEVER aktuell „führend im Markt für unbemannte Systeme und Dienste, entwickelt die nächste Generation von Satelliten und hilft Nutzer*innen ihr Unternehmen digital zu transformieren.“. Während die Angebote zur digitalen Transformation auf der Homepage des Unternehmens vage sind, werden im Bereich UAV drei Drohnen unterschiedlicher Größe angeboten, von denen das größte (AR5 – „The European Maritime Patroller“) bis zu 20 Stunden eine „autonome Überwachung großer Land- und Seeflächen mit einer onboard durchgeführten Mustererkennung“ anbietet. Die kleinste Version (AR4) wird als „kampferprobt durch verschiedene Streitkräfte und Sicherheitsbehörden“ angeprisen und verspricht u.a. die „kontinuierliche Überwachung sensibler Gebiete durch Mustererkennung zur Zielfindung“.[61]

Neben TEKEVER sind an SPIDER noch das Unternehmen Aralia Systems – nach eigenen Angaben ein führender Anbieter für intelligente Videoüberwachung auf Flughäfen, das ans bulgarische Verteidigungsministerium angegliederte Institut “Professor Tsvetan Lazarov” und das Instituto de Telecomunicações (IT – Aveiro) beteiligt. Bei letzterem handelt es sich um eine gemeinsame For-

[55] EDA: PP Call 15-INR-02_02 Information on the awarded project, www.eda.europa.eu.

[56] cordis.europa.eu/project/id/502818.

[57] cordis.europa.eu/project/id/322466.

[58] cordis.europa.eu/project/id/314139.

[59] cordis.europa.eu/project/id/308914.

[60] cordis.europa.eu/project/id/833805.

[61] „About“, „AR5“ und „AR4-EVO“, http://uas.tekever.com.

schungseinrichtung von sechs portugiesischen Hochschulen, die wesentlich von staatlichen und EU-Institutionen (darunter die ESA) sowie der Privatwirtschaft, darunter Siemens, finanziert wird.

Standardisation of Remotely Piloted Aircraft System (RPAS) Detect and Avoid (TRAWA)

Beim Projekt TRAWA geht es um die Integration von ferngesteuerten Flugzeugen (RPAS) in den zivilen Luftraum. Wenn Privatpersonen z.B. handelsübliche Quadrocopter steuern, handelt es sich insofern um keine Integration in den zivilen Luftraum, als diese juristisch – und zumeist auch technisch – auf Höhen beschränkt sind, in denen kein bemannter Luftverkehr stattfindet. In der Nähe von Flughäfen ist der Betrieb solcher Drohnen untersagt und bei handelsüblichen Modellen auch oft technisch (via geofencing) unterbunden. Die Integration in den zivilen Luftraum hingegen zielt auf ein alltägliches Nebeneinander bemannter und unbemannter Systeme mit unterschiedlichen Flugeigenschaften auch z.B. im westeuropäischen Luftraum ab, das ein hohes Maß an Standardisierung voraussetzt. So ist grundsätzlich von der Möglichkeit auszugehen, dass die RPAS den Kontakt zu menschlichen Piloten verlieren können oder ohne menschliche Steuerung reagieren müssen. Gegenstand der Standardisierung sind deshalb u.a. die Sicherheit der Kommunikationsverbindungen und die im Notfall autonomen Ausweichsysteme (Sense & Avoid).

Das Projekt TRAWA setzt jedoch auf einer grundsätzlicheren Ebene an, die der unmittelbaren und autonomen Kollisionsvermeidung vorausgeht. Standardisiert werden soll hier u.a. die Reichweite der Sensorik (in Abhängigkeit von der Geschwindigkeit), um frühzeitig mögliche Annäherungen von anderen Luftfahrzeugen zu erkennen und nach dem Prinzip des „Remain Well Clear" den nötigen Abstand zu halten.[62] Unter der Führung des Netherlands Aerospace Center (NLR) waren an TRAWA neben zwei (eng miteinander verwobenen, auf UAV spezialisierten) italienischen Beratungsunternehmen (EuroUSC und Deepblue) und einem britischen Beratungsunternehmen das Deutsche Zentrum Luft- und Raumfahrt (DLR) beteiligt. Laut Darstellung der EDA erfolgte das Projekt „in Unterstützung" der „Arbeitsgruppe 105" der Europäischen Organisation für Zivilluftfahrt-Ausrüstung (EUROCAE). Die EUROCAE ist eine nahezu vollständig von der Industrie getragene Institution zur Standardisierung des Luftverkehrs, deren Arbeitsgruppe 105 zu unbemannten Systemen klar von den Rüstungsunternehmen Airbus Defence & Space, Thales und Safran dominiert wird. Über die Ergebnisse von TRAWA ist öffentlich wenig bekannt,[63] alleine der Homepage von EuroUSC ist zu entnehmen, dass es neben der Sensorik u.a. um die Darstellung möglicher Ausweichrouten an den Mensch-Maschine-Schnittstellen zu den Piloten ging.[64] Das ebenfalls beteiligte DLR hingegen bezieht sich auf TRAWA in einer „Blaupause" unter dem Titel „Concept for Urban Airspace Integration". Darin entwirft das DLR eine Vision, in der sich „alle Flugzeuge in allen Lufträumen" bewegen können: „das vorgeschlagene Konzept sieht vor, den Luftraum sowohl für Fahrzeuge mit hohem wie mit niedrigem Stand der technischen Ausrüstung zu öffnen". Ermöglicht werden soll dies durch ein „U-Space System", in dem eine von Menschen kontrollierte und verantwortete Flugsicherung keine Rolle mehr zu spielen und stattdessen einem „zentralen System" zu weichen scheint: „Das U-Space System verwaltet die Bereitstellung von Informationen (Verkehrsdaten und Annäherungs-Warnungen), das Luftraum-Management und die Steuerung von Verkehrsflüssen. Die Positionen und weitere Flugdaten von Luftfahrzeugen würden unter Berücksichtigung sämtlicher Bedingungen des Luftraums an ein zentrales System übertragen. Einsätze mit höherer Priorität (z.B. Rettungshubschrauber) würden an das System übermittelt, das daraufhin die nötigen Anpassungen in den betroffenen Segmenten des Luftraums vornimmt […] Falls ein*e Nutzer*in des Luftraums die Anweisungen nicht befolgt und in geschützte Räume eindringt, können verschiedene Maßnahmen ergriffen werden. Das Luftraum- und Verkehrs-Managementsystem könnte versuchen, die Kontrolle des Luftfahrzeuges zu übernehmen (unter der Voraussetzung dass eine entsprechende Verbindung besteht) und den Flug beenden oder umleiten. Wenn das nicht möglich ist, könnten weitere Maßnahmen (einschließlich Verteidigungs-Maßnahmen) nötig sein".[65]

[62] EDA: PP Call 15-STAN-CERT-01_02 Information on the awarded project, www.eda.europa.eu.

[63] Für eine etwas ausführlichere Kontextualisierung siehe: Directorate General for External Policies of the Union: European armaments standardisation, study requested by the SEDE Subcommittee, www.iss.europa.eu.

[64] „TRAWA", www.eurousc-italia.it.

[65] DLR: Blueprint - Concept for Urban Airspace Integration (December 2017), www.dlr.de.

Inhalt

3.6. Vorbereitende Maßnahme im Bereich Verteidigungsforschung (PADR)

Anschließend an die mit 1,4 Mio. Euro geförderten Pilotprojekte nahm der Europäische Verteidigungsfonds 2017 seine Arbeit auf. Für die ersten zwei Jahre (bis Ende 2019) war er mit 90 Mio. Euro ausgestattet, die er im Rahmen einer „vorbereitenden Maßnahme im Bereich Verteidigungsforschung" (Preparatory Action on Defence Research, PADR) des ersten Fensters, also für „Forschung" vergab. In der ersten Ausschreibung (2017) waren drei Programmlinien vorgesehen, die mit insgesamt 25 Mio. Euro ausgestattet waren. Die erste und wichtigste Linie zielte auf „den Start eines einzelnen, komplexen Projekts", welches „den Mehrwert von unbemannten Systemen bei der Verbesserung des Situationbewusstseins unter Beweis stellen sollte, wobei diese mit anderen bemannten und unbemannten Systemen gemeinsam operieren und kooperieren sollten". Ergebnis war das Projekt Ocean2020, das unter Führung des italienischen Unternehmens Leonardo das MUM-T zur Verbesserung des Lagebildes auf See weiterentwickeln sollte. Beteiligt waren 43 Unternehmen und Institutionen aus fünfzehn Staaten, darunter mit Indra (Spanien), Safran (Frankreich), Saab (Schweden), MBDA und Hensoldt (Deutschland) viele der europaweit führenden Rüstungsunternehmen. Das Projekt enthielt insgesamt eine Förderung von 35 Mio. Euro. Es gipfelte im November 2020 in einer Demonstration unter Führung der italienischen Marine, an der sechs Marineschiffe aus vier Staaten (Italien, Frankreich, Griechenland, Spanien) sowie neun unbemannte Systeme (Luft-, Boden- und Unterwasserfahrzeuge) verschiedener Hersteller beteiligt waren. Vier Satellitensysteme und zwei bodengebundene Netzwerke stellten die Kommunikation unter den beteiligten Fahrzeugen und mit vier Operationszentralen (in Italien, Spanien, Griechenland, Portugal) und „dem Prototypen eines Europäischen Kommandozentrums" in Brüssel sicher. Eine zweite solche Übung sollte 2020 unter Führung der schwedischen Marine in der Ostsee stattfinden.[66]

Die zweite PADR-Linie diente der Forschung im Zusammenhang mit der individuellen Ausrüstung und dem Schutz der Einsatzkräfte, darunter verbesserte Tarnsysteme und den ABC-Schutz (atomare, biologische und chemische Stoffe). Eines der unter dieser Linie geförderten Programme zielte auf die Standardisierung der von Soldaten am Körper getragenen IKT (Projekt GOSSRA) – und umfasste mit Rheinmetall (Deutschland), Leonardo, Indra und Saab ein sehr ähnliches Spektrum der Rüstungsindustrie, wie Ocean2020. Die dritte Linie diente der strategischen technologischen Zukunftsforschung mit dem Ziel, „realistische Szenarien für zukünftige Konflikte zu entwickeln, die dazu beitragen können, EU-finanzierte Rüstungsforschung zu gestalten".[67] Hier erhielt das italienische Unternehmen Engeneering Informatica den Zuschlag für das Projekt Pythia (Predictive methodologY for TecHnology Intelligence Analysis), das ein „einfaches und intuitives System zur technologischen Vorausschau" versprach, „das auf der automatischen Auswertung von Texten und Big Data basiert".

Der zweite Call (2018) stellte 40 Mio. Euro in Aussicht und umfasste wiederum drei Linien, von denen die erste auf ein einzelnes, großes Projekt abzielte, das mit bis zu 12 Mio. gefördert werden konnte. Hierbei ging es um die Entwicklung eines militärischen Anforderungen entsprechenden leistungsfähigen „Minicomputers" (system-on-a-chip) als Beitrag zur Schaffung einer „europäischen Lieferkette für spezifische und kritische Technologien des elektronischen Designs". Die zweite Linie stellte bis zu 5,4 Mio. Euro für ein Projekt in Aussicht, das einen „europäischen Hochleistungs-Laser" konzipieren sollte, der u.a. der Abwehr konventioneller Raketen, schneller Boote und „taktischer bemannter und unbemannter Luftfahrzeuge" dienen könnte. Die dritte Linie sah bis zu 1,9 Mio. Euro für ein Projekt vor, das wiederum unter dem Titel „strategische technologische Zukunftsforschung" u.a. „Komponenten und

[66] *www.ocean2020.eu/.*

[67] *„Preparatory Action on Defence Research: 2017 research topics description", https://ec.europa.eu/.*

Materialien“ identifizieren sollte, „die nicht in der EU verfügbar sind, aber in den Produkten enthalten sind, welche in der EU entwickelt und bereits jetzt oder zukünftig von den Streitkräften der EU genutzt werden“. Damit will man der (zukünftigen) Abhängigkeit von Drittstaaten – konkret werden auch die USA genannt – entgegenwirken. Weitere 20 Mio. Euro schrieb der zweite Call für ergänzende Module zum Hauptprojekt des ersten Calls Ocean2020 aus.[68]

Der dritte Call (2019) umfasste 25 Mio. Euro und und schrieb diese u.a. für fünf Studien zu sich anbahnenden „Game-Changers“ aus, darunter Künstliche Intelligenz, Quantencomputing, Erweiterte Realität, Artilleriewaffen und satelliten-unabhängige Navigationssysteme. Jede Studie konnte mit bis zu 1,5 Mio. Euro dotiert werden und sollte „das Entstehen eines innovativen europäischen Ökosystems mit engen Verbindungen in die Verteidigungsindustrie stimulieren“.[69] Eine zweite Programmlinie lobte weitere Studien aus, die letztlich themenoffen „radikal neue Zukunftstechnologien jeder Art mit unbekannten Auswirkungen“ untersuchen sollten, die “grundlegende technologische Überlegenheit über potentielle Gegner“ hervorbringen könnten. Als explizites Ziel wurde ausgegeben „neue Akteure bei der Forschung und Innovation im Verteidigungsbereich“ zu aktivieren, „darunter herausragende junge Forscher*innen, ambitionierte SMEs im High-Tech-Bereich, visionäre Forschungszentren großer Unternehmen und Forschungs-Organisationen“.[70] Zuletzt wurde eine Studie zur „Interoperabilität und Standardisierung von Systemen, Subsystemen, Komponenten und Prozeduren in [unbemannten] Plattformen in netzwerkzentrierten Umgebungen“ ausgeschrieben. Auch in dieser dritten Ausschreibungen sind die acht (bekannten) geförderten Projekte von altbekannten Granden der Rüstungsindustrie dominiert: darunter Thales und Nexter (Frankreich), Diehl und MBDA (Deutschland). Besonders auffällig ist die geografische Verteilung der beteiligten Unternehmen und Institutionen: Frankreich ist insgesamt 25 Mal beteiligt, gefolgt von Italien mit sieben, Spanien und den Niederlanden mit je vier, Deutschland und Belgien mit je drei und die Slowakische Republik mit zwei Beteiligungen. Darüber hinaus sind Portugal, UK, Lettland, Österreich, Polen, die Tschechische Republik und Griechenland nur jeweils einmal vertreten.

[68] EDA: 2018 Calls for proposals on Preparatory Action on Defence Research, https://ec.europa.eu.

[69] EDA: 2019 Calls for proposals and General Annexes, https://ec.europa.eu.

[69] EDA: 2019 Calls for proposals and General Annexes, https://ec.europa.eu.

[70] Ebd.

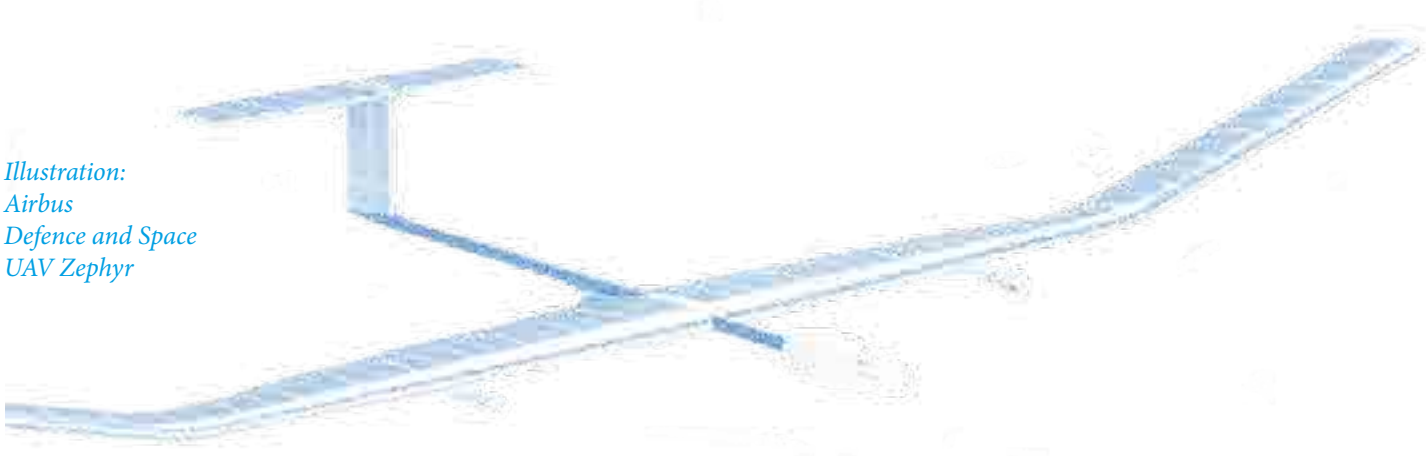


Illustration: Airbus Defence and Space UAV Zephyr

Inhalt

3.7 Entwicklungshilfe für die Rüstungsindustrie (EDIDP)

Während das PADR entsprechend dem Design des EDF der „Forschung“ dienen sollte, sollte es anschließend um Projekte der „Entwicklung“ gehen. Hierfür wurden vom EDF für die Jahre 2019 und 2020 500 Mio. Euro im Rahmen des „Europäischen Programms zur industriellen Entwicklung im Verteidigungsbereich (European Defence Industrial Development Programme, EDIDP) bereitgestellt. Der entsprechende Durchführungsbeschluss der EU-Kommission vom 19. März 2019 orientiert sich stark am CDP von 2018 und listet insgesamt 19 Themenbereiche auf, in denen Gelder vergeben werden. In zwei Fällen werden diese Gelder direkt, also ohne Ausschreibung vergeben. So erhält ein Konsortium aus Airbus Defence & Space, Dassault (Frankreich) und Leonardo für die Jahre 2019 und 2020 insgesamt 100 Mio. Euro aus dem EDIDP – also ein Fünftel des Gesamtbetrags – für die Entwicklung der Eurodrohne. Begründet wird diese direkte Mittelvergabe mit der strategischen Relevanz des Projekts und den hohen technischen Anforderungen an das System, wodurch das bereits bestehende Konsortium ein quasi-Monopol auf dessen Umsetzung habe. Sehr ähnlich begründet wird die direkte Vergabe von 37 Mio. Euro für die „Entwicklung eines sicheren und interoperablen Kommunikationssystems“ (ESSOR) an ein Konsortium aus Thales, Leonardo, Indra, Radmor (Polen), Bittium (Finnland) und Rhode & Schwarz (Deutschland).

Für vier Themenbereiche sollen sowohl 2019 als auch 2020 Projekte ausgeschrieben werden: Für die Cybersicherheit von Kommunikationssystemen (32 Mio.), für Luftkampf-Fähigkeiten, darunter elektronische Kriegführung (34 Mio.), für eine Modernisierung der Artillerie (13,5 Mio.) und für „innovative und zukunftsweisende Lösungen im Verteidigungsbereich“ durch SME (17,5 Mio.). Letzteres ist eine Art Sonder- und Containerkategorie, die auch kleineren (Rüstungs-)Unternehmen Zugang zum EDF verschaffen soll und hierzu wiederum über dreißig Themenbereiche auflistet, zu denen man sich „innovative“ Vorschläge erhofft.

Die größten Beträge wurden 2019 für die Entwicklung einer autonomen europäischen Satelliten-Navigation, einer permanenten (KI-gestützten) Aufklärungskapazität aus dem Luft- und Weltraum und einer Architektur für die Integration unterschiedlichster unbemannter Fahrzeuge in MUM-T-Verbände in Aussicht gestellt. An diesem Projekt (iMUGS) unter Führung des estnischen Unternehmens Milrem Robotics sind neben Safran, Diehl und Bittium mit Nexter und KMW auch die zentralen Akteure bei der Entwicklung des deutsch-französischen Projekts Main Ground Combat System (MGCS) beteiligt. Anders sieht es beim Projekt DRONEDGE-E aus, bei dem „die automatisierte Generierung von Algorithmen durch Künstliche Intelligenz“ zur „autonomen Steuerung von Drohnenschwärmen in Echtzeit“ beitragen soll. An dem mit knapp 2 Mio. Euro geförderten Projekt sind vier eher kleine Unternehmen beteiligt, die bislang noch nicht im Zusammenhang mit Rüstungsprojekten in Erscheinung getreten sind.

Die drei Themenbereiche, die in den Ausschreibungen 2020 am umfangreichsten gefördert wurden, sind die Entwicklung von Unterwasser-Roboter für unterschiedliche militärische Anwendungen, Entwicklungen zur verbesserten Überwachung des Weltraums und die weitere Verbesserung der Maritimen Überwachung mit je gut 20 Mio Euro. Deutlich geringer fällt mit 5,7 Mio. Euro die Ausschreibung zu „Verteidigungstechnologien mit Unterstützung Künstlicher Intelligenz“ aus. Auch hier hatte die Kommission sehr unterschiedliche Unterthemen vorgeschlagen, zu denen Projektanträge eingereicht werden könnten, darunter „Systeme zur Entscheidungsunterstützung, prädiktive Algorithmen zur Antizipation von Bedrohungen durch die Analyse von Big Data und neuronale Netzwerke“ oder auch zur Unterstützung von „sich wiederholenden Aufgaben wie der Strategischen Kommunikation (STRATCOM), logistischer Planung, dem Management des Luftraums ...“.[71]

[71] *C(2019) 2205 final - Annex, https://ec.europa.eu.*

Inhalt

3.8. PESCO

Während die Gelder im Rahmen des EDF, also PADR und EDIDP, suprastaatlich von der Kommission im Rahmen des EU-Haushaltes vergeben werden, handelt es sich bei der „Ständigen Strukturierten Zusammenarbeit“ (Permanent Structured Cooperation, PESCO) um ein intergouvernmentales Programm, das von den Mitgliedsstaaten und zumindest primär aus deren Rüstungshaushalten finanziert wird. Angestrebt wird jedoch ein Ineinandergreifen beider Programme. So betont die EU-Kommission in ihrem Factsheet über das EDIDP 2019, dass neun der 16 geförderten Projekte einen Bezug zu PESCO-Projekten aufweisen.[72] Zukünftig sollen PESCO-Projekte in der Forschung bis zu 100% und in der Entwicklungsphase zu bis zu 30% aus dem EDF finanziert werden können. Kommission und EDA schaffen damit Anreize zu ehrgeizigeren gemeinsamen Rüstungsprojekten der Mitgliedsstaaten und nehmen zugleich Einfluss auf deren Ausgestaltung.

[72] *EDA: Fact sheet European Defence Industrial Development Programme 2019, https://ec.europa.eu.*

Die PESCO war eines der Kernelemente des Vertrages von Lissabon (2007) und einer der wesentlichen Gründe, warum dieser Vertrag von der Friedensbewegung in den Europäischen Mitgliedsstaaten überwiegend abgelehnt wurde. Er ermöglicht es „Mitgliedstaaten, die anspruchsvollere Kriterien in Bezug auf die militärischen Fähigkeiten erfüllen und die im Hinblick auf Missionen mit höchsten Anforderungen untereinander weiter gehende Verpflichtungen eingegangen sind ...eine Ständige Strukturierte Zusammenarbeit im Rahmen der Union“ zu begründen. Innerhalb dieser Struktur gilt nicht mehr das sonst in der Verteidigungspolitik vorherrschende Einstimmigkeitsprinzip, sondern teilweise die qualifizierte Mehrheit. Die Voraussetzung für die Teilnahme ist die Akzeptanz gemeinsamer Vorgaben für die Rüstungsausgaben, Rüstungsprojekte und Truppengenerierung für gemeinsame Einsätze, deren Einhaltung regelmäßig überprüft und auch sanktioniert werden kann. Das erklärte Ziel der PESCO ist eine Stärkung der europäischen Verteidigungsidentität als Voraussetzung einer stärkeren, auch militärisch untermauerten Rolle der EU in der internationalen Politik. Bereits früh wurde jedoch darauf hingewiesen, dass PESCO auch ein Vehikel sein könnte, die deutsch-französische Führung innerhalb der Europäischen Union und in Hinblick auf deren Rüstungsindustrie auszubauen. Es ist somit kein Wunder, dass es nach In-Kraft-Treten des Vertrags von Lissabon zunächst recht lange gedauert hat, PESCO dann aber nach der Ankündigung des Austritts Großbritanniens aus der EU sehr schnell vorangetrieben wurde. Vier Tage nach dem Brexit-Referendum vom 23. Juni 2016 meldeten sich der deutsche und der französische Außenminister mit einem gemeinsamen Papier zu Wort, in dem sie forderten, „Deutschland und Frankreich [müssen] gemeinsam dafür eintreten, die EU Schritt für Schritt zu einem unabhängigen und globalen Akteur zu entwickeln. [...] Gruppen von Mitgliedstaaten sollten so flexibel wie möglich eine dauerhafte strukturierte Zusammenarbeit im Verteidigungsbereich einrichten können oder mit einzelnen Operationen vorangehen“.[73] So geschah es dann auch. Deutschland und Frankreich betonten vehement ihre Absicht, PESCO zu aktivieren, setzten damit Italien und Spanien unter Zugzwang und drohten auch den restlichen Mitgliedsstaaten wieder einmal mit einem „Europa der zwei Geschwindigkeiten“. Im November 2017 unterzeichneten letztlich 23 Mitgliedsstaaten – viele von ihnen nach Experteneinschätzung „zähneknirschend“ – die Notifizierungsurkunde.[74] Am 11. Dezember 2017 beschloss der Rat die Aktivierung der PESCO, seit dem sind in diesem Zusammenhang nur noch die beteiligten Staaten im Rat stimmberechtigt.

[73] *Jean-Marc Ayrault and Frank-Walter Steinmeier: Ein starkes Europa in einer unsicheren Welt (28.6.2016), https://www.diplomatie.gouv.fr.*

[74] *Vgl: Jürgen Wagner: PESCO – das militaristische Herz der Europäischen Verteidigungsunion, Europäische Studien zur Außen- und Friedenspolitik Nr. 1/2019, www.imi-online.de.*

Bereits im Vertrag von Lissabon wurden als Kriterien für die Beteiligung an PESCO u.a. folgende Bedingungen formuliert. Die Mitgliedstaaten Verpflichten sich zu

- „einer möglichst weit gehenden Angleichung ihres Verteidigungsinstrumentariums, indem sie insbesondere die Ermittlung des militärischen Bedarfs harmonisieren, ihre Verteidigungsmittel und -fähigkeiten ge-

meinsam nutzen und gegebenenfalls spezialisieren sowie die Zusammenarbeit auf den Gebieten Ausbildung und Logistik stärken";
• „einer eventuellen Mitwirkung an der Entwicklung gemeinsamer oder europäischer Programme für wichtige Güter im Rahmen der Europäischen Verteidigungsagentur" und
• „seine Verteidigungsfähigkeiten durch Ausbau seiner nationalen Beiträge und gegebenenfalls durch Beteiligung an multinationalen Streitkräften, an den wichtigsten europäischen Ausrüstungsprogrammen und an der Tätigkeit der [Europäischen Verteidigungsagentur] intensiver zu entwickeln".[75]

Im Beschluss des Rates zur Aktivierung der PESCO wurden u.a. folgende Verpflichtungen hinzugefügt bzw. konkretisiert:

• regelmäßige reale Aufstockung der Verteidigungshaushalte;
• mittelfristig schrittweise Aufstockung der Investitionsausgaben für Verteidigungsgüter auf 20 % der Gesamtausgaben im Verteidigungsbereich;
• mehr gemeinsame und „kollaborative" Projekte im Bereich der strategischen Verteidigungsfähigkeiten;

Außerdem enthät er die

• Verpflichtung zur größtmöglichen Unterstützung der CARD; Verpflichtung zur intensiven Einbeziehung eines künftigen Europäischen Verteidigungsfonds in die multinationale Auftragsvergabe; Verpflichtung zur Ausarbeitung harmonisierter Anforderungen für alle unter den teilnehmenden Mitgliedstaaten vereinbarten Projekte im Bereich der Fähigkeitenentwicklung; Verpflichtung, die gemeinsame Nutzung bestehender Fähigkeiten zu erwägen
• Verpflichtung zu vermehrten Bemühungen zur Zusammenarbeit im Bereich der Cyberabwehr, etwa Informationsaustausch, Ausbildung und operative Unterstützung.[76]

[75] *Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft (Document C2007/306/01), https://eur-lex.europa.eu.*

[76] *European Council: Council Decision (CFSP) 2017/2315 (11. December 2017) establishing permanent structured cooperation (PESCO) and determining the list of participating Member States, https://eur-lex.europa.eu.*

Inhalt

3.9. Digitalisierung und KI in frühen PESCO-Projekten

Als PESCO offiziell aktiviert wurde, befanden sich bereits die meisten der ersten 17 Projekte in Planung,[77] deren Umsetzung von den an PESCO beteiligten Staaten im März 2018 beschlossen wurde. Dieses erste Paket umfasste u.a. den Aufbau eines „Europäischen Sanitätskommandos", das die medizinische Unterstützung und Versorgung für gemeinsame Einsätze zentral organisieren sollte, ein „Kompetenzzentrum für Ausbildungsmissionen der Europäischen Union" und ein „Netzwerk von Logistik-Drehscheiben". Ein zentrales Projekt ist dabei die sog. Krisenreaktionsinitiative (EUFOR Crisis Response Operation Core, CROC), die darauf abzielt, für bestimmte Aufgaben bereitstehende militärische Fähigkeiten der Mitgliedsstaaten zu erfassen und somit für kurzfristig erstellte Krisenoperationspläne entsprechende Zusammenstellungen der multinationalen Truppen zu empfehlen.

Gleich drei Projekte betreffen die maritime Sicherheit bzw. die Erstellung eines maritimen Lagebildes unter Einbeziehung autonomer Systeme, womit sie recht unmittelbar an die „zivile" Sicherheitsforschung zur Grenzsicherung anschließen können. So soll ein Projekt zu Überwachung und Schutz von Häfen und der See (HARMSPRO) „ein integriertes System von maritimen Sensoren, Software und Plattformen […] entwickeln, das Daten prozessiert und fusioniert und dadurch hilft, maritime Bedrohungen zu ekrennen und zu identifizieren". Das Projekt „Upgrade der maritimen Überwachung" soll „landbasierte Aufklärungssysteme, see- und luftgestützte Plattformen zusammenführen, um den Mitgliedsstaaten in Echtzeit Informationen zur Verfügung zu stellen", während sich ein weiteres Projekt mit „maritimen (semi-)autonomen Systemem für die Minenabwehr" beschäftigt.

Zwei weitere Projekte könnten mittelfristig dazu zu dienen, eine EUropäische „Combat Cloud" aufzubauen bzw. zu ermöglichen: Das „European Secure Software Defined Radio" und das Projekt „Strategic Command and Control (C2) System for CSDP Missions". Das Bundesverteidigungsministerium beschreibt den Mehrwert des angestrebten Systems mit folgendem Szenario: „Beispielsweise könnte der Rat der Europäischen Union einstimmig einen umfangreichen Ansatz zur Stabilisierung eines Landes in der Sahelzone beschließen. Vor diesem Hintergrund würden sowohl Streitkräfte der EU-Mitgliedstaaten zur Bekämpfung von Terroristen als auch zivile Polizeikräfte zur Sicherung der Staatsgrenzen entsandt. Damit die einzelnen Elemente dieses integrierten Ansatzes der EU nahtlos ineinandergreifen können, würde das im Rahmen des PESCO-Projekts Strategic C2 System entwickelte einheitliche Führungssystem Informationen für die beteiligten Entscheider bereitstellen. Diese Informationen werden zum Beispiel in Form von Lagebildern oder durch Aufzeigen möglicher Logistikketten bereitgestellt. So können die Militär- und Polizeikräfte koordiniert und effektiv zur nachhaltigen Stabilisierung des betreffenden Staates eingesetzt werden".[78]

Zwei weitere Projekte betreffen die Cyber Defence. Hierzu soll einerseits eine Plattform geschaffen werden, über die Mitgliedsstaaten Informationen über mögliche Angriffsvektoren und Gegenmaßnahmen, andererseits jedoch auch schnelle Cyber-Eingreifkräfte (Cyber Rapid Response Teams, CRRTs) geschaffen werden, welche mit „verlegbaren Cyber-Werzeugkästen" ausgestattet Mitgliedsstaaten und EU-Institutionen bei Cyberangriffen unterstützen sollen.

[77] *Lucie Béraud-Sudreau u.a.: Keeping the momentum in European defence collaboration - an early assessment of PESCO implementation (Mai 2019), IISS Research Paper, www.iiss.org.*

[78] *Siehe: BMVg: Strategic C2 System for CSDP, www.bmvg.de.*

Inhalt

3.10. Digitalisierung und KI in späteren PESCO-Projekten

Ein knappes Jahr später, im November 2018, wurden 17 weitere PESCO-Projekte beschlossen. Auch hier spielen unbemannte Systeme, MUM-T und Schwarmverhalten in vielen Projekten eine Rolle. Neben dem bereits seit Jahren von Deutschland und Frankreich vorangetriebenen Projekt der Eurodrohne, das hiermit in den PESCO-Rahmen überführt wurde, soll u.a. ein Aufklärungsballon als Pseudo-Satellit entwickelt werden, der eine „Fähigkeit zur dauerhaften Überwachung, Zielerfassung und Aufklärung" mit „herausragenden Dual-Use-Eigenschaften" stellen soll. Schwärme von bemannten und unbemannten Systemen sollen ABC-Überwachung „as a Service" (CBRN SaaS) liefern und das Projekt DIVEPACK ein modulares System des MUM-T für die Unterstützung von Taucher*innen durch unbemannte Unterwasserfahrzeuge (UUV) entwickeln. Außerdem ist die Entwicklung eines „integrierten unbemannten Bodenfahrzeugs" geplant, das sowohl für den Transport, als auch für die Aufklärung eingesetzt werden kann, und über eine „autonome Fähigkeit zur Weg- und Missionsplanung mit unterschiedlichen Optionen für das MUM-T" verfügt. Ein weiteres Projekt zielt auf ein eigenes, gemeinsames System zur Bekämpfung von Drohnen (Counter Unmanned Aerial System, U-CAS) ab. Ein neu zu entwickelndes Raketensystem, das sowohl von der Luft wie vom Boden gestartet werden kann, soll ebenfalls über eine „autonome Zielerfassung" verfügen.

Andere Programme des zweiten PESCO-Paketes zielen eher auf die Harmonisierung und Standardisierung ab. So wollen die Tschechische Republik und Deutschland eine Machbarkeitsstudie durchführen, welche die Kapazitäten der Mitgliedsstaaten zur Elektronischen Kampfführung (EW) erfasst und die Möglichkeiten eines gemeinsamen Systems und einer gemeinsamen EW-Einheit ausloten soll. Zwei weitere Projekte streben den Aufbau EUropäischer Netzwerke zur geografischen, meterologischen und ozeanografischen (GeoMETOC) Unterstützung von EU-Missionen und zum „militärischen Situationsbewusstsein im Weltraum" an und ein weiteres die Entwicklung von Endgeräten, die das europäische Satelliten-Navigations-Netzwerk zur Positionsbestimmung nutzen. Außerdem soll eine Standardisierung der Verfahren zum Test und Evaluation (neuer) Waffensystem erfolgen. Auch das bereits länger geplante und nun in den PESCO-Rahmen überführte Upgrade des Kampfhubschraubers Tiger (Mark III) bezieht sich wesentlich auf die Modernisierung und Anpassung seiner Kommunikationsschnittstellen. Griechenland und Zypern haben angekündigt, gemeinsam ein C2-System für multinationale Einsätze von Spezialkräften zu entwickeln und eine gemeinsame Geheimdienst-Akademie der EU aufzubauen, in der auch neue Technologie entwickelt und erprobt werden soll. Im Mai 2019 wurde darüber hinaus der Aufbau eines „schnellen Cyber-Eingreifteams" unter Führung Litauens beschlossen.

Das dritte PESCO-Paket wurde im November 2019 mit 13 Projekten beschlossen und verfolgt neben einem unbemannten System zur U-Boot-Abwehr (MUSAS) keine weitere Entwicklung unbemannter Fahrzeuge. Es enthält jedoch wiederum ein Projekt, das die Integration von RPAS in den zivilen Luftraum vorbereiten soll. V.a. lässt sich im dritten Paket ein klarer Schwerpunkt auf die Elektronische Kriegführung und die Cyber Defence erkennen. So wollen Spanien, Frankreich und Schweden ein gemeinsames System zur luftgestützten elektronischen Kampfführung entwickeln, das auf bemannte wie unbemannte Luftfahrzeuge aufgesetzt werden kann und über feindlichem Gebiet den Zugang zum elektromagnetischen Spektrum bzw. zum Cyberspace unterdrücken soll. Zugleich wird ein Zentrum für Cyber-Fachkräfte und -Innovationen (EU Cyber Academia and Innovation Hub) geschaffen, um ein Cyber-affines „Ökosystem" zu schaffen, das technisch gut ausgebildetes Personal hervorbringt und so den Nachschub an zukünftigen Mitarbeiter*innen in diesem Bereich sichert. Unter deutscher Führung ist ein gemeinsames Koordinationszentrum für den Cyber- und Informationsraum (Cyber and Information Domain Coordination Center, CIDCC) geplant, das „als ständige multinationale militärische Struktur" dienen soll. Unter ungarischer Führung ist die Schaffung einer „Simulations-Cloud" für die taktische Ausbildung geplant, welche die räumlich über die EU verteilten Ausbildungszentren vernetzen und so gemeinsame Übungen im virtuellen Raum ermöglichen soll.
Hinter dem Acronym EcoWAR (EU Collaborative Warfare Capabilities) steht die geplante Entwicklung einer „Fähigkeit zur kollaborativen Kampfführung" bei der Ansätze zur netzwerkzentrierten Kriegführung zwischen Luft- und Bodentruppen, bemannten und unbemannten Systemen aus verschiedenen Mitgliedsstaaten entwickelt werden sollen.

Insgesamt wurden bislang 47 PESCO Projekte beschlossen. Das International Institute for Strategic Studies (IISS) hat allerdings bereits nach der Verabschiedung des zweiten Paketes darauf hingewiesen, dass für die meisten Projekte keine klaren Terminpläne und Verpflichtungen aus den nationalen Haushalten existierten und diese von weiterer Finanzierung aus dem EDF abhängig seien, über deren Priorisierung noch keine klaren Vorstellungen bestehen.[79] Eine Analyse des Centre for European Policy Studies (CEPS) wies außerdem im Dezember 2019 darauf hin, dass die Zahl der durchschnittlich an einem Projekt beteiligten Staaten von 7.6 in der ersten auf 3.6 in der dritten Runde gesunken sei.[80] Zweifellos demonstrieren Umfang und Zielsetzung der PESCO-Projekte den klaren Willen zu einer umfangreichen und zunehmend harmonisierten Modernisierung und Aufrüstung der beteiligten europäischen Armeen. Zugleich müssen diese jedoch auch als Ausdruck eines durch die Einrichtung des EDF ausgelösten Goldrausches der nationalen Rüstungsindustrien und ihrer letztlich weiterhin konkurrierenden Positionierung um die etwa 1 Mrd. Euro gesehen werden, die zukünftig jährlich aus dem EDF ausgeschüttet werden sollen. In welchem Umfang die Projekte die angekündigten Ergebnisse liefern werden, ist damit noch lange nicht ausgemacht. Konkrete Folgen haben PESCO und EDF allerdings bereits jetzt auf einer anderen Ebene: Während nationale und transnationale Rüstungsunternehmen schon immer einen guten Zugang zu den Entscheider*innen auf EU-Ebene hatten, ist nun die Vertretung der Interessen der Rüstungsindustrie(n) ein elementarer Bestandteil der EU-Bürokratie und der ihr zugeordneten Vertreter*innen der Mitgliedsstaaten

[79] Siehe FN 77.

[80] Steven Blockmans / Dylan Macchiarini Crosson: Differentiated integration within PESCO – clusters and convergence in EU defence, CEPS Research Report No. 2019/04 (December 2019, www.ceps.eu.

Zweifellos demonstrieren Umfang und Zielsetzung der PESCO-Projekte den klaren Willen zu einer umfangreichen und zu nehmend harmonisierten Modernisierung und Aufrüstung der beteiligten europäischen Armeen.

Inhalt

3.11. Die Fusion von Rüstungs-, Industrie und Digitalisierungspolitik

Unter der Kommissionspräsidentin Ursula von der Leyen wurden zusammenhängend mit dem EDF und Themen der Digitalisierung grundlegende Umstrukturierungen vorgenommen. In ihren Ernennungsschreiben an die zukünftige Kommissar*innen hat sie als Ziel klar ausgegeben, dass diese Kommission „eine ‚geopolitische Kommission' sein wird": „Was wir jetzt tun, wird bestimmen, in welcher Welt unsere Kinder leben werden und die Rolle Europas in der Welt definieren". Hierzu gelte es auch, „die internen und externen Aspekte unserer Arbeit besser zusammen zu führen".[81]

Die wesentlichsten Umstrukturierungen betrafen das Kommissariat für den Binnenmarkt und das neu geschaffene Kommissariat unter dem sperrigen Titel „Ein Europa für das digitale Zeitalter", das mit Margrethe Vestager besetzt wurde, die zuvor Wettbewerbskommissarin war. Als eine von drei Exekutiv-Vizepräsident*innen wird sie einer Kommissionsgruppe vorstehen. Ihre Aufgabe soll darin bestehen, „sicherzustellen, dass Europa die Potentiale des digitalen Zeitalters umfänglich ausschöpft, seine Industrie und Innovationsfähigkeit stärkt. Das wird ein Schlüssel sein bei der Stärkung unserer technologischen Führerschaft und strategischen Autonomie". Konkret wurde von ihr dahingehend u.a. erwartet, eine „langfristige Strategie für die Zukunft der europäischen Industrie", eine neue Strategie für kleine und mittelständische Unternehmen, eine „europäische Daten-Strategie" und einen „europäischen Zugang zu Künstlicher Intelligenz" zu erarbeiten. Dabei solle sie „die gegenseitige Befruchtung zwischen der zivilen, der Verteidigungs- und der Raumfahrt-Industrie sicherstellen".[82]

Auch das (ehemals sehr mächtige) Kommissariat für Industrie und Binnemarkt, das mit Thierry Breton besetzt wurde, wurde massiv umstrukturiert und der Exekutiv-Vizepräsidentin Vestager untergeordnet, die ihrerseits direkt vom Generalsekretariat der Kommissionspräsidentin unterstützt wird. Als Mitglied der Arbeitsgruppe von Vestager soll auch Breton an der Formulierung der o.g. Industrie-, SME- und KI-Strategien mitwirken. Darüber hinausgehend ist v.a. Bretons Aufgabenbereich vom Gedanken der strategischen Autonomie und der Geopolitik geprägt. Als konkrete Aufgaben wurden ihm u.a. aufgetragen, „Europas technologische Souveränität auszubauen", der Aufbau eines „einheitlichen Binnenmarktes für Cybersicherheit", Strategien zur „Prävention und Bekämpfung von Desinformation und falschen Informationen im Internet" sowie der Aufbau einer „gemeinsamen Cyber-Einheit".[83] Vor allem aber kommt Breton dabei aber die Aufgabe eines Rüstungskommissars zu. Er soll den Ausbau eines „konkurrenzfähigen europäischen Marktes für Verteidigungsgüter" und einer „starken und innovativen Raumfahrt-Industrie" vorantreiben und dabei die „elementare Verknüpfung von Raumfahrt- und Verteidigungsindustrie" stärken. Außerdem wurde er mit der Umsetzung des Aktionsplans zur militärischen Mobilität beauftragt. Für diese Aufgaben steht ihm – erstmals in der Geschichte der EU – mit dem Europäischen Verteidigungsfonds ein Rüstungsetat zur Verfügung, den er weiter konzipieren und aufbauen soll. Unterstützt wird er bei der Erfüllung dieser Aufgaben gleich durch drei Generaldirektionen: die Generaldirektion „CONNECT" (Kommunikationsnetze, Inhalte und Technologien), die Generaldirektion „GROW" (Binnenmarkt, Industrie, Unternehmertum und KMU) und die Generaldirektion „DEFIS" (Verteidigungsindustrie und Weltraum).[84]

[81] *Ursula von der Leyen: Mission letter Thierry Breton (1 December 2019), https://ec.europa.eu.*

[82] *Ebd.*

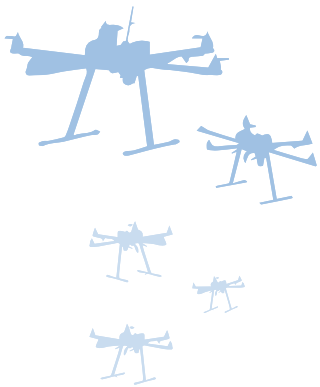
[83] *Ursula von der Leyen: Mission letter Thierry Breton (1 December 2019), https://ec.europa.eu.*

[84] *Ebd.*

[85] *Christoph Marischka: (Diese) Industriepolitik ist Rüstungspolitik, Telepolis (12. November 2019), www.heise.de/tp/.*

[86] *2018 listete SIPRI das Unternehmen auf Platz zehn der Top 15 Rüstungsproduzenten weltweit (ohne China) mit einem Umsatz im 9,5 Mrd. US$ im Rüstungsgeschäft bei einem Gesamtumsatz von 18,8 Mrd. US$, vgl: https://www.sipri.org.*

Obwohl für dieses Amt zunächst Sylvie Goulard vorgesehen war, die jedoch wegen möglicher Interessenskonflikte vom Europäischen Parlament abgeleht wurde, scheint Thierry Breton für das Amt eines „EU-Kommisars für digitale Rüstung“ hervorragend geeignet. Vor und nach seiner Funktion als französischer Wirtschaftsminister unter Jacques Chirac besetzte er Spitzenpositionen in französischen Rüstungs- und Elektronik-Konzernen und war federführend an strategischen Übernahmen, Fusionen, Spin-offs und Unternehmenskooperationen beteiligt, aus denen u.a. die Unternehmen Thales und Atos hervorgingen.[85] Während es sich bei Thales mittlerweile um eines der größten Rüstungsunternehmen weltweit handelt,[86] bezeichnet sich Atos als „weltweit führender Anbieter für die digitale Transformation mit über 110.000 Mitarbeitern in 73 Ländern und einem Jahresumsatz von mehr als 11 Milliarden Euro“. Tatsächlich ist Atos in Sachen Digitalisierung und Systemintegration auf vielen Geschäftsfeldern aktiv, hat sich jedoch 2011 mit der Übernahme von Siemens IT Solutions and Services und 2014 mit der Übernahme des französischen Bull-Konzerns – jeweils unter Breton – die wichtigsten (privaten) IT-Dienstleister der deutschen und französischen Streitkräfte einverleibt. Zuletzt hat sich Atos durch weitere strategische Übernahmen jedoch auch auf dem Markt für digitalisierte Gesundheitsdienstleistungen gut positioniert.



Thales führt die Liste der größten Nutznießer der Forschungsprogramme FP7 (2007-2013) und Horizon2020 (2014-2020) der EU-Kommission an, Atos nimmt darauf den fünften Platz ein.[87] Viele dieser Forschungsprojekte behandelten unter mehr oder weniger zivilen Szenarien (Katastrophenschutz, Grenzsicherung etc.) Fragestellungen der Sensorik, der Sensor-Data-Fusion und der Mensch-Maschine-Schnittstellen oder gar die Integration all dieser Komponenten in einem Gesamtsystem, das auf quasi-militärischem Niveau Ansprüchen der Cybersicherheit genügen sollte. Vom optimalen Design der Schaltkreise in optischen Sensoren über Bauteile für Rechenzentren bis hin zu konzeptionellen Überlegungen der Situationswahrnehmung in der Augmented Reality wurden im Rahmen der als zivil deklarierten Forschungsförderung Projekte unterstützt, welche die Unternehmen schnell auch auf ihre militärische Kundschaft zuschneiden konnten. Aktuell ist Atos mit der Umsetzung des Programms Scorpion CIS (combat information system) betraut, mit dem die IT-Infrastruktur der französischen Streitkräfte durch eine gemeinsame Battle Management Language harmonisiert wird. Gleichzeitig ist Atos nicht nur wichtigster privater Anbieter der „weißen IT“ der deutschen Bundeswehr, sondern auch hier gemeinsam mit Rafael mit der Implementierung einer Combat Cloud betraut.[88] Thales stellt zwar auch Raketen und Gefechtsköpfe her, eine zentrale Rolle zumindest in Europa spielt das Unternehmen jedoch im Bereich der „taktischen Kommunikationslösungen für See-, Luft und Bodentruppen“ sowie bei der Hardware im Bereich der Luft- und Raumfahrt. Die Lieferketten sind dabei gut abgestimmt mit dem größten europäischen Rüstungsunternehmen, Airbus (Platz 3 unter den größten Nutznießern der zivilen Forschungsförderung der Kommission), mit dem zusammen Thales die Combat Cloud für das FCAS (Future Combat Air System) entwickelt. Mit Atos, Thales und Airbus sind damit zentrale Akteure benannt, auf denen sich eine harmonisierte IKT unter europäischen Streitkräften abstützen wird, die man als Vorbedingung für die großen EU-Rüstungsprojekte zum MUM-T betrachten kann – und die andere europäischen Streitkräfte in Zugzwang bringen und an die beteiligten Anbieter binden wird.

[87] So der Stand 2017, vgl: Kai Biermann ans Christian Fuchs: 800.000 Euro für einen Terror-Airbag, der nie fertig wurde, Die Zeit (23. Februar 2017), www.zeit.de.

[88] ATOS: Ccorpion combat information system - Data at the Heart of the Battlefield, https://atos.net.

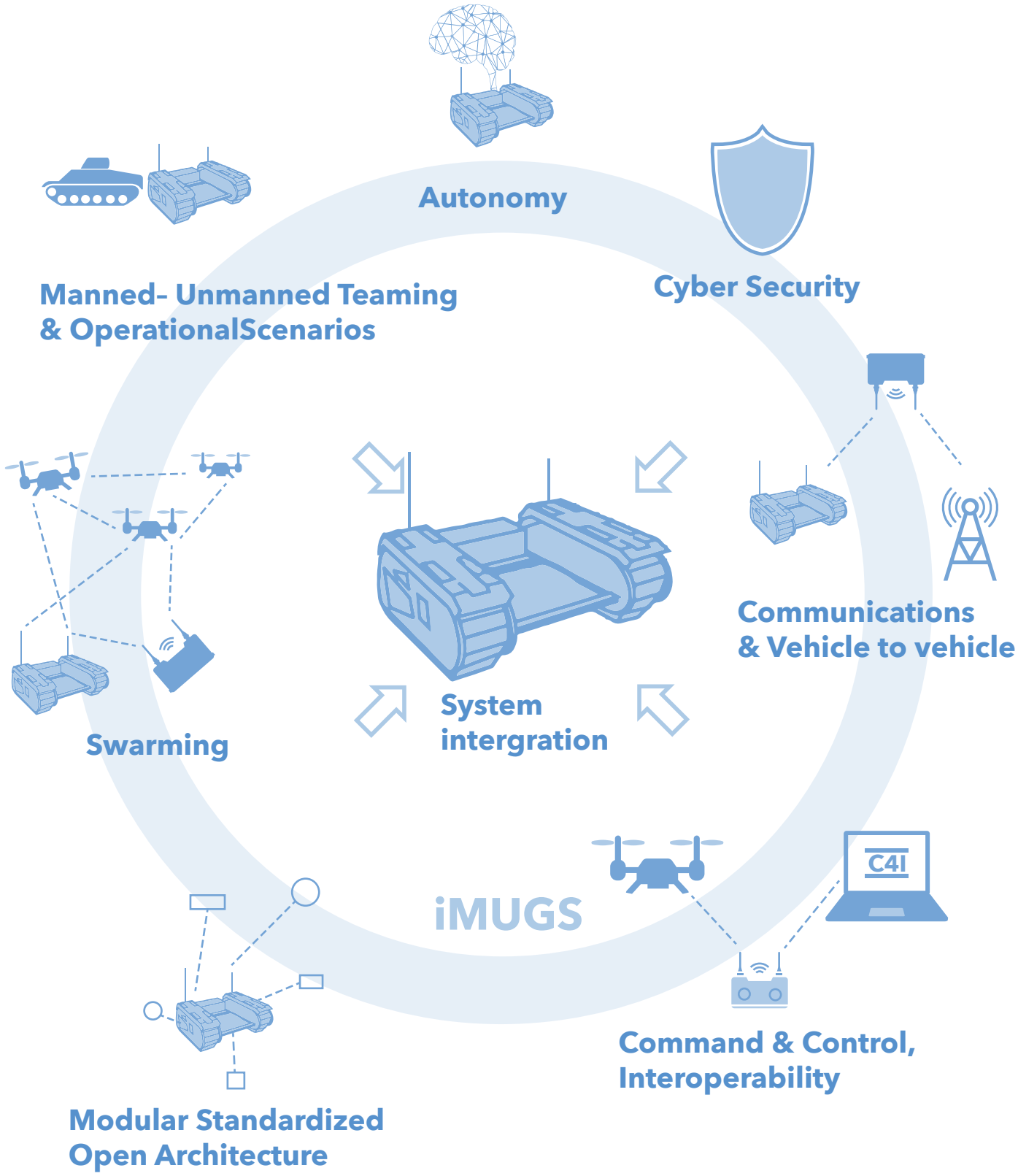
Interessant ist, dass die Ernennung Bretons zum Kommissar für den Binnenmarkt unter einer deutschen Kommissionspräsidentin erfolgte. Denn Breton steht für eine Industriepolitik, die von deutscher Seite gerne mal als „Staatskapitalismus“ bezeichnet[89] und kritisiert wird. Die strategischen Fusionen, die u.a. zur heutigen Position von Thales und Atos (und z.B. auch von STMicroelectronics) führten, wurden unter dem zwischenzeitlichen Wirtschaftsminister wiederholt vom französischen Staat durch Anteilsübernahmen und andere (industrie-)politische Maßnahmen vorangetrieben und ermöglicht, was in Deutschland notorisch als Eingriff in den Wettbewerb abgelehnt wird. Die berühmteste Abweichung von diesem Kurs der deutschen Regierungen bestand in der gemeinsam mit Frankreich strategisch und politisch vorangetriebenen Gründung von Airbus, das der Marktmacht von Boeing etwas entgegensetzen – und durchaus auch mit Blick auf deren militärische Relevanz – die Basis einer europäischen Luft- und Raumfahrtindustrie bilden sollte. Die zuletzt v.a. auch durch den Brexit intensivierte deutsch-französische Kooperation und europäische Führungsrolle begünstigte jedoch ein Umdenken auf deutscher Seite. So wurde in beiden Ländern das Joint Venture zwischen den jeweils größten Herstellern von Panzern – Krauss-Maffei Wegmann und Nexter Systems – gerade auch mit Blick auf die gemeinsame Entwicklung des Main Combat Ground System politisch unterstützt. Im Februar 2019, recht kurz nach dem Antritt der neuen Kommission unter von der Leyen, veröffentlichte der deutsche Wirtschaftsminister Altmaier einen Entwurf für eine „Nationale Industriestrategie 2030“,[90] die von eher ideologisch geprägten liberalen Kommentatoren als Abkehr vom Prinzip des freien Wettbewerbs gegeißelt wurde. Denn sie enthielt die Aufforderung, das geltende Beihilfe- und Wettbewerbsrecht zu überprüfen und ggf. zu reformieren, um zeitlich begrenzten Beihilfen „in Bereichen von Innovationen mit hoch innovativen Basiswirkungen“ zu ermöglichen. Insbesondere „[b]ei den überragend wichtigen Fragen von Plattform-Ökonomie, Künstlicher Intelligenz und Autonomem Fahren“ erscheine, „wie seinerzeit im Falle von Airbus eine unmittelbare staatliche Beteiligung zur Erreichung des Ziels erforderlich und gerechtfertigt“. In Klammern wird diese Möglichkeit staatlich geförderter oder erzwungener Fusionen zu einem deutsch-europäischen Konzern, der mit „Wettbewerbern aus den USA oder China auf Augenhöhe“ konkurrieren kann, als „KI-Airbus“ bezeichnet.

Wie auch im Falle von Airbus würde ein möglicher KI-Airbus im Kern aus der Fusion deutscher und französischer Unternehmen hervorgehen und unter der gemeinsamen politischen Kontrolle beider Staaten stehen. Im Bereich der Forschung jedenfalls gehen beide Staaten bereits voran und planen aktuell den Aufbau eines deutsch-französischen Forschungszentrums für Künstliche Intelligenz, zu dessen Vorbereitung aktuell beide Staaten entsprechende Forschungscluster aufbauen, die in einer zweiten Ausbaustufe miteinander vernetzt werden sollen.

[89] Der Beitrag von Aline Robert: „Frankreich fordert Überarbeitung der EU-Wettbewerbsregeln“, Euractiv (4. Juni 2019), www.euractiv.de etwa ist nur in seiner deutschen Version mit der polemischen Überschrift „Mehr Staatskapitalismus wagen“ überschrieben.

[90] Bundesministerium für Wirtschaft und Energie (BMWi): Nationale Industriestrategie 2030 (Februar 2019), www.bmwi.de.

Inhalt


Autonomy
Cyber Security
Manned- Unmanned Teaming
& OperationalScenarios
Communications
& Vehicle to vehicle
Swarming
System
intergration
iMUGS
C4I
Command & Control,
Interoperability
Modular Standardized
Open Architecture

4.1 Über verstreute Projekte zur gemeinsamen „Cloud"?

Aus den oben vorgestellten Forschungsprogrammen, welche als Vorbereitung und Implementierung des Europäischen Rüstungsfonds verstanden werden sollten, lassen sich folgende taktische und strategischen Folgen ableiten:

• Es besteht ein klar erkennbarer Wille zur **massiven Aufrüstung und Modernisierung** der Europäischen Armeen und zur Stärkung der Fähigkeiten und Autonomie der technologischen und rüstungsindustriellen Basis der EU (European Defence Technological and Industrial Base, EDTIB). Strategisch lässt sich beides nicht durch die vermeintliche Notwendigkeit zu (international wenig umstrittenen) Krisenmanagementoperationen begründen, sondern nur durch das Ziel, militärisch neben den USA und China als konkurrenzfähiger Akteur wahrgenommen zu werden und zumindest Gebiete kontrollieren zu können, in denen diese entgegengerichtete Interessen verfolgen.

• **KI-Anwendungen** spielen bei fast allen angestrebten Projekten zur Modernisierung und Aufrüstung der Europäischen Streitkräfte eine Rolle und sie werden insbesondere in Form zunehmend autonomer Systeme, einer immer stärkeren Verdichtung der Lagebilder und der Beschleunigung der Kriegführung diese wesentlich verändern. Ansätze zur Entwicklung einer auf Big Data und Maschinellem Lernen basierenden Super-KI, wie sie den ökonomischen und zunehmend auch populären Diskurs um KI prägt, lassen sich bislang eher in Ansätzen erkennen. So befindet sich unter den untersuchten Rüstungsprojekten keines, das erkennbar darauf abzielt, große Mengen an Daten aus Manövern, EU-Militärmissionen oder realen Gefechten auch nur zu Trainings- und Simulationszwecken zu sammeln oder gar angereichert mit Datensätzen aus dem zivilen Umfeld mittels selbstlernender Algorithmen zu analysieren. Bemühungen zum Aufbau der Infrastrukturen, die (im ökonomischen Diskurs) als nötig erachtet werden, um immense Datenmengen und Rechenleistung zusammenzubringen, sind bislang allenfalls in Ansätzen erkennbar (Siehe 4.3.).

• Zentrale Themen der Rüstungsprojekte sind **autonome Fahrzeuge, Schwärme und das Manned-Unmanned Teaming**. An entsprechenden Technologien zur „Kampfwertsteigerung" hat die EU vermutlich auch wegen ihres relativ geringen Mobilisierungspotentials (bzw. Anteils an der Weltbevölkerung) ein besonderes Interesse. Taktische Umstrukturierungen der Streitkräfte um unbemannte Systeme sind bereits erkennbar und es scheint realistisch, dass diese innerhalb eines überschaubaren Zeitrahmens von etwa zehn Jahren in vielen Truppenteilen standardmäßig integriert sein werden. Weit fortgeschritten ist dies bereits im Hinblick auf Aufklärungssysteme; bei Assistenzsystemen (z.B. zum Transport) und der Elektronischen Kriegführung ist ebenfalls mit einer schnellen Implementierung zu rechnen.
Im Rahmen von des MGCS oder des PESCO-Projekts iMUGS werden auch Systeme entwickelt, die der populären Vorstellung von Killer-Robotern nahe kommen. Ihre Realisierung hängt jedoch davon ab, inwiefern gesellschaftliche Widerstände gegen solche Waffensysteme überwunden werden können. Strategisch ist festzustellen, dass die meisten Projekte zwar – quasi als Nebeneffekt – dystopische Möglichkeiten für die Innere Sicherheit eröffnen, strategisch jedoch offensiv ausgerichtet sind, indem sie vom Einsatz in einem feindlichen oder zumindest umkämpften Gebiet ausgehen.

• Dies gilt umso mehr für die **Fähigkeiten in der Domäne Weltraum**. Zwar wird bei der Entwicklung europäischer Pseudo-Satelliten explizit deren „Dual Use" angesprochen, militärisch jedoch haben diese primär Nutzen bei der Überwachung umkämpfter oder feindlicher Gebiete bzw. entsprechender Grenzgebiete jenseits der Reichweite kleinerer (unbemannter) Aufklärungssysteme. Dasselbe gilt für die Satelliten-Kommunikation und die Überwachung des Weltraums, welche diese sicherstellen soll: Sie ist v.a. für Einsätze jenseits des eigenen Territoriums interessant in Szenarien, in denen andere Staaten (oder ähnlich mächtige Akteure) über Weltraumwaffen verfügen. So sinnvoll es zunächst erscheinen mag, Systeme zur Satelliten-Navigation zu entwickeln, die unabhängig vom (US-kontrollierten) GPS sein können, so beinhaltet dies zumindest im militärischen Kontext auch den Anspruch, ggf. gegen den Willen der USA militärisch aktiv zu werden.

• Es existieren klare Ansätze, mit der harmonisierten Digitalisierung der europäischen Streitkräfte auch einer **European Combat Cloud** näherzukommen. Besonders Deutschland und Frankreich verfolgen dieses Ziel v.a. im Rahmen ihrer Industriepolitik und kleinteilig durch Rüstungsprojekte, wobei auch KI-gestützte Systeme zur Entscheidungsunterstützung implementiert werden. Das PESCO-Programm „Strategic C2 System" strebt zumindest eine entsprechend Vernetzung von der taktischen bis zur strategischen Ebene an (siehe FN 79). Die Harmonisierung und Standardisierung der IKT europäischer Streitkräfte stellt dabei auch einen Versuch dar, dem Ziel einer „Europäischen Armee" von der technologischen und rüstungsindustriellen Basis her näher zu kommen. Eine schnelle und integrierende Modernisierung der IKT der europäischen Streitkräfte könnte der EU tatsächlich mit einem Schlag ein ganz anderes militärisches Gewicht geben – wenn sie denn möglich wäre. Die USA jedoch sind nach über 20 Jahren massiver hierauf ausgerichteter Rüstungsanstrengungen noch weit vom Ideal einer alle Teilstreitkräfte übergreifenden, von der taktischen bis zur strategischen Ebene reichenden netzwerkzentrierten Kriegführung entfernt. Für die EU sind die Hürden ungleich größer, da es sich (nimmt man PESCO als Referenz) um den Verbund von 25 souveränen Regierungen mit unterschiedlichen politischen und strategischen Kulturen und ebenso viele Armeen mit unterschiedlicher Grundausstattung handelt. Die Implementierung einer European Combat Cloud dürfte also eine Jahrzehnte währende Anstrengung bleiben – die der Rüstungsindustrie auf ebenso lange Zeit umfangreiche Aufträge einbringen dürfte.

• Deutlich erkennbar sind die Bemühungen, **Einfluss auf Regulation, Logistik und Organisationsstrukturen** zu nehmen. Besonders deutlich wird das bei den Anstrengungen, militärischen unbemannten Luftfahrzeugen Zugang zum Luftraum zu verschaffen, indem dessen Organisation und Kontrolle digitalisiert und automatisiert wird. Ähnliches deutet sich mit den Programmen Militärische Mobilität (der Kommission) und Erweiterte Logistik (der EDA) an. Auffällig ist jedenfalls, dass viele Projekte implizit davon ausgehen, dass die Integration unbemannter Fahrzeuge in den zivilen (Luft-)Verkehr auf absehbare Zeit realisiert wird.

• Der **Cyber- und Informationskrieg** wird langfristig und völlig unhinterfragt als Domäne der Kriegführung und militärische Aufgabe definiert. Eine klare Abgrenzung zu zivilen Institutionen ist ebenso wenig erkennbar, wie Bemühungen um internationale Regulierung. Es ist davon auszugehen, dass die zahlreichen Programme zur Europäischen Zusammenarbeit auf der Ebene der militärischen Cyber-Verteidigung bald die Kapazitäten der zivilen Behörden und ihrer Mitgliedsstaaten ausstechen werden. Da im Cyber- und Informationsraum eine Unterscheidung zwischen Kriegs- und Friedenszustand konzeptionell nicht getroffen wird, kommt damit militärischen oder hybriden Organisationen auch eine dauerhafte Aufgabe zu.

Inhalt

4.2. Eine technologiegetriebene, offensive Strategie

Wie an vielen Stellen bereits angesprochen, lassen sich die aktuelle Aufrüstungswelle und das Ziel Strategischer Autonomie nur im Kontext einer offensiven außen- und militärpolitischen Strategie begreifen. Das Ziel ist es, rüstungs- und industriepolitisch von den USA, China und anderen großen Playern unabhängig zu werden und auf globaler Ebene mit diesen konkurrieren zu können. Dazu gehört zumindest für einige Mitgliedsstaaten auch, die Rolle der NATO bei der Verteidigung zugunsten einer im Aufbau befindlichen EU-Armee zurückzudrängen – was allerdings unter den Mitgliedsstaaten bereits umstritten ist. Weniger umstritten ist es, einen konfrontativeren Kurs gegenüber Russland einzunehmen und dies auch mit Drohgebärden und dem Aufbau entsprechender militärischer Fähigkeiten auf Ebene der EU zu untermauern. Dies ist v.a. deshalb relevant, weil Russland eine hybride Kriegführung vorgeworfen wird, welche die EU in einen latenten Kriegszustand versetzt, der als Rechtfertigung für die Aufrüstungsmaßnahmen dienen kann.

Viel weiter geht diese Strategie allerdings nicht. Wie gesagt ist das konkrete Verhältnis zu den USA und der NATO innerhalb der EU äußerst kontrovers. Eine einheitliche Strategie gegenüber China – jenseits der ökonomischen Eindämmung u.a. im Zuge der strategischen Autonomie – ist bislang nicht absehbar. So konsensual das Säbelrasseln gegenüber Russland grundsätzlich ist, so unterschiedlich sind die Erwartungen und die Bereitschaft, hier tatsächlich einen unmittelbaren bewaffneten Konflikt zu riskieren. Kurz gesagt: eine gemeinsame strategische Kultur ist weiterhin in weiter Ferne.

Absehbar allerdings ist, dass sich die CSDP zukünftig verstärkt auf die Vorherrschaft in dem Raum ausrichten wird, welcher von James Rogers als „Grand Area“ definiert wurde. Dies deckt sich auch mit den realistischeren der angepeilten Aufrüstungsprogramme. Unbemannte Systeme und MUM-T kommen v.a. in der unmittelbaren Nachbarschaft der EU, im Mittelmeer, zum Einsatz, wo sie primär zur Bekämpfung der illegalen Migration, zunehmend aber auch zur Überwachung und Durchsetzung von Embargomaßnahmen eingesetzt werden. Bereits jetzt versucht die EU mittels ihrer GSVP durch den Einsatz von Überwachungstechnologie, die Ausbildung und Anleitung lokaler „Sicherheitskräfte“ und eine überschaubare Zahl von Bodentruppen weite Teile des Nordens und Westen Afrikas – den sie als Sahel-Region definiert hat – unter ihre Kontrolle zu bekommen. Das Sterben im Mittelmeer, die katastrophale Lage in Libyen, die Eskalation in der Sahel-Region und zuletzt der Putsch in Mali illustrieren jedoch überdeutlich, dass „Informationsüberlegenheit“ bzw. ein noch so dichtes Lagebild nicht zwingend mehr Kontrolle bedeuten. Ähnliches gilt für das Horn von Afrika, Teile der Arabischen Halbinsel und den Persischen Golf, wo vonseiten europäischer Mitgliedstaaten, oft im NATO-Verbund, tw. eine massive Aufklärungsdichte besteht, ohne dass sie nennenswerte strategische Erfolge geltend machen können. Die massiven Investitionen in die maritime Aufrüstung bestätigen auch einen Drang zu verstärkter Präsenz in der Ostsee, dem Hohen Norden (Arktis) sowie im indischen Ozean bis hin zum südchinesischen Meer. Ob und unter welchen Bedingungen hierbei allerdings die Bereitschaft besteht, letale Waffengewalt anzuwenden und einen kriegerischen Konflikt einzugehen, ist unklar. Die Wahrscheinlichkeit steigt allerdings mit der Globalstrategie der EU und den damit verbundenen Rüstungsprogrammen enorm.

Ob im Falle eines kriegerischen Konfliktes unbemannte Systeme einen taktischen Vorteil bieten, ist ebenfalls keineswegs ausgemacht. Fraglich ist vielmehr, ob sie – wie andere technologische Innovationen – nicht vielmehr das Potential haben, strategische Fehler zu provozieren. So gilt die US-geführte Operation Desert Storm 1991 im Irak, „als ein beeindruckendes Bündel von

High-Tech-Waffen ... es den USA ermöglicht hat, die viertgrößte Armee der Welt erstaunlich schnell und mit geringsten Verlusten zu überwältigen,“[91] bis heute als markanter Beweis für die taktischen Vorteile, die (informations-)technologische Überlegenheit mit sich bringt. Zugleich kann sie jedoch als Einstieg in eine Kriegführung der USA gesehen werden, in der Kriege – zumindest in ihrer Anfangsphase – mit geringen eigenen Verlusten und damit politischen Kosten verbunden waren, letztlich aber, wie in Afghanistan 2001 und wiederum im Irak 2003, in kostspielige und – zumindest gegenüber den Erwartungen – verlustreiche Einsätze von Bodentruppen mündeten. Beide Interventionen lassen sich heute klar als strategische Fehler erkennen und in beiden Interventionen wurde vor dem (weitgehenden) Abzug der US-Truppen der Einsatz unbemannter bewaffneter Drohnen eingeschränkt, weil er sich fatal auf die öffentliche Unterstützung auswirkte,[92] ohne den Bodentruppen offenbar mittelfristig nicht durchsetzungsfähig sind. Die EU Globalstrategie und die in ihrem Kontext eingeführten Rüstungsprogramme scheinen geradezu darauf ausgelegt, die Fehler US-amerikanischer Strategie der vergangenen 20 Jahre in einem strategischen Umfeld zu wiederholen, das ein deutlich höheres Eskalationspotential aufweist.

[91] Norman Davis: An Information-Based Revolution in Military Affairs (1996), U.S. Strategic Institute Strategic Review, Vol. 24, No. 1, www.rand.org.

[92] Siehe: Anthony Cordesman: The Real Revolution in Military Affairs (5.8.2014), CSIS Commentary, www.csis.org.

Inhalt

4.3. Die wirklichen Triebkräfte: Industrie und (Risiko-)Kapital

Die von der EDA herausgegebene Zeitschrift European Defence Matters enthält in ihrer 19. Ausgabe vom Juni 2020 einen kleinen (5 von 44 Seiten) Schwerpunkt zum Thema Künstliche Intelligenz. Er beginnt mit einer Art Eigenbericht der EDA zu ihren Aktivitäten auf diesem Feld und beinhaltet darüber hinaus ein Interview mit Christian Hedelin, Direktor für Strategieentwicklung bei Saab. Der Eigenbericht beginnt nach einem kurzen Anreisser mit einem Zitat von Panagiotis Kikiras, Abteilungsleiter der EDA für Technologie und Innovation: „KI ist in der Rüstung nichts Neues. Seit dem Ende des Zweiten Weltkriegs wurden an sie viele Erwartungen geknüpft: Viele Tendenzen und verrückte Vorhersagen haben viel versprochen und sind dann doch in der Versenkung verschwunden". Auch Hedelin gibt sich wenig aufgeregt: „KI ist bereits in den heutigen Systemen integriert und funktioniert … Traditionell wird KI oft für die Entscheidungsunterstützung eingesetzt … Unsere ersten Schritte auf diesem Gebiet haben wir vor mehr als 25 Jahren unternommen". Die 2004 aufgestellte und mit dem EDF und PESCO massiv aufgewertete EDA beschreibt ihre Tätigkeiten im Bereich KI eher zurückhaltend. Seit Anfang 2019 arbeite man an einer gemeinsamen Definition, Taxonomie und einem Glossar zur KI. Aktuell befände man sich in Rücksprache mit den Mitgliedsstaaten und will bis Ende 2020 einen KI-Aktionsplan vorlegen. Man räumt dabei ein: „die aktuelle Welle bei der KI-Entwicklung ist anders. Voraussetzungen wie massive Rechenleistung und gewaltige Datenbanken mit Informationen in nahezu Echtzeit waren in den 1980er und 1990er Jahren nicht gegeben und verbessern sich ständig". Deshalb habe man „vorgeschlagen, ein Archiv, einen ‚Daten-See' anzulegen, der weniger sensible, anonymisierte operationale Daten aus [militärischen] Fahrzeugen, Luftfahrzeugen usw. umfasst". Als konkreten Anwendungsbereich hierfür sieht man bei der EDA die präventive und vorausblickende Wartung und allgemein im Bezug auf KI autonome Systeme und Systeme zur Entscheidungsunterstützung – allerdings mit Einschränkungen: „Auf der taktischen Ebene bedeutet KI eher die intelligente Automatisierung von Funktionen, wie jene in autonomen Systemen. Aber auf der strategischen Ebene landen wir gleich bei Themen wie (KI-gestützter) Aufklärung und Entscheidungsunterstützung, wo es gleich sehr schwierig wird mit der Kooperation, weil es da Befindlichkeiten von verschiedenen Akteuren gibt". Auch Hedelin von Saab nennt neben der traditionellen Anwendung der „Entscheidungsunterstützung" autonome Systeme und vorausblickende Wartung als mögliche Anwendungsfelder. Er vergisst jedoch nicht zu fordern, „noch mehr Anstrengungen und Investitionen in KI und Maschinelles Lernen zu stecken … Das würde Infrastrukturen für mehr Rechenleistung beinhalten, um Big Data verarbeiten und [künstliche] neuronale Netze trainieren zu können. Die EU könnte in Super-Rechenzentren sowohl für die Industrie, als auch für die Streitkräfte der Mitgliedsstaaten investieren, damit diese unterschiedliche Plattformen ausprobieren können. Es wäre sehr kostspielig für die Unternehmen, diese selbst im großen Maßstab zu entwickeln".[93] Er antwortet dabei auf die Frage: „Was sollte getan werden, damit die Verteidigungsindustrie in der EU ihre führende Position bei KI zukünftig aufrechterhalten kann?".

Der hier wiedergegebene Diskurs zeigt beispielhaft, wie sich die Perspektive der Rüstung vom herrschenden Diskurs über KI unterscheidet, wonach hier ein Wettrüsten im Gange wäre, weil disruptive Innovationen unmittelbar bevorstünden und „Europa" diese Entwicklung verschlafen habe. In Rüstung und Militär, wo man mit entsprechenden Technologien bereits seit Jahrzehnten arbeitet, geht man demgegenüber offenbar eher von einem kontinuierlichen Verlauf technologischer Innovationen aus und sieht Europa eher gut aufgestellt. Dennoch nutzt man natürlich den Hype insofern, als man ihn zum Anlass nimmt, nach mehr öffentlichen Investitionen zu rufen.

[93] *EDA: EDM – European Defence Matters #19 (June 2020), https://eda.europa.eu.*

Woher kommt also der Diskurs um die bevorstehenden Disruptionen und dem damit drohenden Niedergang Europas? Es sind v.a. die Interessenverbände von Industrie und Kapital, sowie die ihnen nahestehenden Politiker*innen.[94] So war es die aktuelle Kommissionspräsidentin Von der Leyen, welche die Integration von Rüstung und Digitalisierung nun auf EU-Ebene mit großer Energie vorantreibt, die dasselbe zuvor in ihrer Funktion als Verteidigungsministerin in Deutschland umgesetzt hat. Hierzu hat sie Katrin Suder als Rüstungsstaatssekretärin ernannt, die zuvor Leiterin der deutschen Niederlassung des Beratungsunternehmens McKinsey war. In ihrer Amtszeit wurden in diesem Zusammenhang zahlreiche Verträge an dieses und andere Beratungsunternehmen mutmaßlich irregulär vergeben, was bis September 2020 Gegenstand eines Untersuchungsausschusses des deutschen Bundestags war.

Wie die Rüstung, so ist auch die Digitalisierung ein Mechanismus der Umverteilung und das Motto „wer nicht digitalisiert, verliert" stellt sicher, dass es die großen Unternehmen und Kapitalgesellschaften sind, die gewinnen. In Zeiten der Austerität und auch der pandemiebedingten Konjunkturprogramme stellt sich die Frage sehr konkret, ob man in die Ausbildung von Pflegekräften, Gesundheitspersonal und Lehrer*innen investiert, oder Gesundheit, Bildung usw. mithilfe von Großindustrie und Beratungsunternehmen digitalisiert und zugleich Milliardenbeträge für die industrielle und industrienahe Forschung und Entwicklung bereitstellt.

Unternehmen wie Roland Berger und McKinsey propagieren gerade im Bereich der KI hierfür die politische Schaffung von „Ökosystemen", in deren Mittelpunkt Start-ups stehen, welche die Ergebnisse (öffentlich finanzierter) Forschung mithilfe von Risikokapital in Anwendungen überführen und kommerzialisieren sollen. Nur so könne es Deutschland und Europa gelingen, gegenüber China und den USA nicht den Anschluss zu verlieren. Von der öffentlichen Hand wird entsprechend gefordert, in industrie- und anwendungsnahe technologische Forschung zu investieren, Forschungs- und Startup-Cluster aufzubauen, Unternehmensgründungen durch finanzielle Förderung und Deregulierung des Arbeits- und Steuerrechts zu erleichtern, Kapitalerträge aus Investitionen in diesen Bereichen von Steuern zu befreien oder gar Gesundheitskassen, Renten- und Pensionsfonds zu verpflichten, selbst in Risikokapital zu investieren.[95] Vieles davon wird von der europäischen und nationalen Gesetzgebung bereits umgesetzt und ist in den Corona-Konjunkturprogrammen enthalten. Es handelt sich dabei um ein gigantisches Umverteilungsprogramm nach dem Motto: Kosten sozialisieren, Gewinne privatisieren. Verkauft wird es der Öffentlichkeit mit der klassischen Standortlogik, die allerdings geopolitisch mit der Angst um eine chinesische oder US-amerikanische Super-KI angereichert ist.

*[94] Was hier auf der europäischen Ebene am Beispiel von EDA und PESCO festgestellt wurde, hat der Autor bereits zuvor für den deutschen Diskurs um disruptive Innovationen herausgearbeitet, wobei hier als weitere Akteure die Managementebene großer Forschungsinstitute und unternehmerische Wissenschaftler*innen in Erscheinung getreten sind. Siehe: Christoph Marischka: KI und Geopolitik - Die unheilige Allianz von Risikokapital, Wissenschaft und Politik (2020), AUSDRUCK Nr. 100, www.imi-online.de.*

[95] Siehe beispielhaft: Roland Berger / Asgard: Artificial Intelligence – A Strategy for European startups, https://asgard.vc.

Ein Beispiel von vielen hierfür ist Fabian Westerheide, nach eigenen Angaben „internationaler Experte für KI-Strategie, Unternehmer und Risiko-Kapitalgeber", der „Regierungsinstitutionen wie die Europäische Kommission, die Europäische Weltraumagentur, das deutsche Parlament, das chinesische Ministerium für Technologie [und] Institutionen wie das Verteidigungs- und das Außenministerium berät". Eines der Themen, zu denen er gerne als Redner auftritt, trägt den Titel „Europas Strategie für das globale KI-Wettrüsten".[96] Medium.com berichtet über die Ansichten Westerheides: „Europa, einst gefangen in einem epischen Wettrüsten zwischen zwei atomaren Supermächten, findet sich nun wieder im Schatten eines Wettlaufs um die Beherrschung Künstlicher Intelligenz, so der deutsche Investor und KI-Experte – der hinzufügt, dass die Einsätze nun für Europa so hoch wären, wie während des Kalten Krieges, wenn nicht gar noch höher … Sowohl die USA als auch China haben große Verteidigungshaushalte und starke Forschungsuniversitäten und -einrichtungen, welche Investitionen in KI-Entwicklung ermöglichen. In den USA werden Milliarden Dollar über Projekte der Rüstungsforschung und entsprechende Wettbewerbe in Unternehmen im Silicon Valley und an anderen Technologiestandorten geleitet – zum Beispiel durch die DARPA [die Forschungsbehörde des Pentagon]".[97] Zwar gibt es mit der „Joint European Disruptive Initiative" (JEDI) eine Organisation, die sich als „die europäische DARPA" bezeichnet, anders als bei der DARPA handelt es sich dabei jedoch v.a. um ein Netzwerk von Risikokapitalgebern – nach eigenen Angaben „vorangetrieben durch 3.700 führende Köpfe in 23 Ländern des europäischen Tech-Ökosystems" – das sich bislang eher erfolglos um öffentliche Finanzierung und Anerkennung bemüht.[98]

Übertreiben gehört hier offensichtlich zum Geschäft, denn mit Erwartungen wird Geld verdient, bzw. umverteilt. Und natürlich springt die Rüstungsindustrie auf diesen Hype auf und natürlich werden dabei auch Technologien entstehen, welche früher oder später auf den Schlachtfeldern zur Anwendung kommen – wenn sich die Europäische Union nicht von der Politik der Aufrüstung und Digitalisierung verabschiedet und stattdessen soziale Lösungen für soziale Probleme sucht. Das würde auch bedeuten, dass weniger Geld für Rüstungsprogramme zur Verfügung stünde und abgerüstet werden müsste. Das würde auch dazu führen, dass sich Europa auf eine defensive Strategie besinnen und die Frage stellen müsste, wie man mit viel einfacheren und billigeren Mitteln tatsächlich Sicherheit herstellen kann. Zum Beispiel durch ein Verbot autonomer und der Offenlegung (und damit nachhaltigen Entschärfung) aller Cyber-Waffen. Nicht gegen China, Russland und die USA, sondern mit ihnen und all jenen Staaten, die in diesem Wettrüsten ohnehin nicht mithalten können.

[96] Siehe: www.fabian-westerheide.de.

[97] Matt Swayne: Investor, AI Expert Says Europe Must Act Now in Global AI Arms Race (11.9.2018), www.medium.com.

[98] Siehe: https://jedi.group/. Gelegentlich wird JEDI als deutsch-französische Initiative bezeichnet und suggeriert, dass die jeweiligen Regierungen involviert wären. Zur Haltung der Bundesregierung zu JEDI siehe jedoch: Deutscher Bundestag: Drucksache 19/5679.

Inhalt

Impressum

Autor: Christoph Marischka

Gestaltung: Thorsten Hädicke

Druck: Der Faltschachtelprofi GmbH, Solingen

Auflage: 250 Exemplare, November 2020

Die Studie steht auf den angegebenen Webseiten zum Download bereit.

Als gedruckte Broschüre kann die Studie zudem per E-Mail unter **bestellungen@oezlem-demirel.de** angefordert werden.

Herausgegeben von:
THE LEFT Fraktion im Europäischen Parlament
73, Rue Belliard
TRI 07V003
B-1000 Brüssel (Belgien)

www.guengl.eu

GUE/NGL THE LEFT IN THE EUROPEAN PARLIAMENT

DIE LINKE. IM EUROPAPARLAMENT

Fotos:
Titel: Milrem Robotics, THeMIS 5th generation UGV, CC BY-SA 4.0
Grafik: Starline, Freepik.com

Inhalt