Bundesakademie
für Sicherheitspolitik

Arbeitspapier Sicherheitspolitik, Nr. 23/2017

Autonome oder halbautonome Waffensysteme: Eine neue terroristische Bedrohung?

von Wolfgang Rudischhauser

Autonome Waffensysteme, wie sie derzeit durch Streitkräfte und Privatunternehmen entwickelt werden, sowie der Vorschlag, diese zu ächten, werden derzeit vielfach in den Medien und Sicherheitskreisen diskutiert. Dabei stellen bereits existierende halbautonome oder ferngelenkte Systeme, wie etwa „Drohnen“ und unbemannte Bodenfahrzeuge, die bereits durch Terrororganisationen wie den Islamischen Staat in verschiedenen Konfliktgebieten genutzt werden, eine viel konkretere Bedrohung dar. Der Zugriff auf solche Technologien wird von Tag zu Tag einfacher, und ihre kommerzielle Nutzung wird sich in naher Zukunft exponentiell ausweiten. Der Gefahr, dass sie terroristisch missbraucht werden, sollte deshalb dringend mehr Beachtung geschenkt werden – insbesondere, da sie zur Verbreitung chemischen, biologischen oder radioaktiven Materials verwendet werden könnten, um mehr Aufmerksamkeit zu erzeugen. Wir müssen darauf vorbereitet sein, dass Terroristen in naher Zukunft nicht nur Messer, improvisierte Sprengsätze oder Lastwagen nutzen werden, um Furcht zu verbreiten, sondern, dass sie zunehmend auf fortgeschrittenere Technologien zugreifen werden.

In einem kürzlich erschienenen Aufruf, der von knapp einhundert Experten für Künstliche Intelligenz (KI) und Führungskräften von Hochtechnologieunternehmen verfasst und unterzeichnet wurde - darunter der Tesla-Gründer Elon Musk und der Google-Forscher Mustafa Suleyman – wird vor den Gefahren autonomer Waffensysteme (sogenannter „Killerroboter“) gewarnt. Die Autoren drängen darauf, solche Systeme im Rahmen der Kriegswaffenkonvention der Vereinten Nationen zu ächten, da sie ihrer Ansicht nach Kriege in der Zukunft dramatisch verändern würden. Seit geraumer Zeit wird eine intensive ethische Debatte darüber geführt, ob solche Waffen nach den Vorschriften des Humanitären Völkerrechts legal sein können. Einige Experten warnen zudem vor der Gefahr, dass solche Systeme die asymmetrische Kriegsführung zwischen Staaten und insbesondere für nichtstaatliche Akteure (wie zum Beispiel Terroristen) vereinfachen könnten. Werden sich diese Systeme zu einer neuen terroristischen Bedrohung entwickeln?

Derzeit werden Terrorangriffe, wie in Barcelona, Brüssel, London, Nizza oder Berlin mit frei zugänglichen Waffen begangen wie etwa Messern, improvisierten Sprengsätzen oder sogar Lastwagen, die in Menschenmengen gesteuert werden. Während diese Anschläge mit aller Deutlichkeit zu verurteilen sind, da sie zahlreiche unschuldige Menschen verletzt oder getötet haben, sollten wir den Blick zugleich darüber hinaus auch auf technisch weiterentwickelte Mittel richten, die eine noch verheerendere Wirkung haben könnten – von den psychologischen Auswirkungen ganz zu schweigen. Es gilt, neue Arten von Waffensystemen wie Drohnen und unbemannte Fahrzeuge zu betrachten, unabhängig, ob diese nur ferngesteuert oder autonom sind, die potentiell sowohl im Rahmen hybrider Kriegführung als auch bei Terroranschlägen verwendet werden könnten.

 | ISSN 2366-0805

Drohnen oder unbemannte Luftfahrzeuge, oft *UAV* (Unmanned Aerial Vehicles) genannt, werden bereits heute nicht nur durch Staaten, sondern zunehmend auch durch nichtstaatliche Akteure, wie die Terrororganisation IS vielerorts eingesetzt.[1] Sie dienen Überwachungszwecken, aber auch dazu, zu töten. Der IS hat angeblich sogar bereits UAVs eingesetzt, um chemische Waffen und andere toxische Stoffe zu verbreiten, wenn auch einschlägige Beweise hierfür bislang vage bleiben. Das Pentagon hat kürzlich ein 700-Millionen-Dollar-Programm aufgelegt, um geeignete Mittel zur Abwehr dieser neuen Bedrohung zu identifizieren – Berichten zufolge mit bislang gemischten Resultaten.[2] Obwohl auch Szenarien hybrider Kriegführung auf disruptiven und chaoserzeugenden Methoden aufbauen, konzentriert sich dieses Papier allein auf die terroristische Gefahr.

Müssen wir eine völlig neue Bedrohung unserer Sicherheit ins Auge fassen? In welchem Ausmaß werden nichtstaatliche Gruppen Zugang zu neuen Waffensystemen, einschließlich autonomer Technologien haben? Wären sie versucht, diese bei Anschlägen zu verwenden, und – falls ja – bei welchen Anschlagsszenarien wären solche Technologien für den Angreifer von Vorteil? Welche entscheidenden technologischen Entwicklungen müssten Sicherheitsbehörden genauer im Blick behalten?

Low Tech oder High Tech: die verschiedenen Implikationen unbemannter Systeme

Die vollständige Autonomie neuer Waffensysteme ist noch immer mehr Vision denn Realität. Unter Experten gibt es eine intensive Debatte darüber, ob völlig autonome Systeme sich bereits in einer erfolgversprechenden Entwicklung befinden – unabhängig davon, ob beim Militär oder in der Industrie. Einige Experten empfehlen, dass vollständig autonome Systeme niemals entwickelt werden sollten, da stets Menschen die letzte Kontrolle haben sollten. Sie berufen sich auf das Humanitäre Völkerrecht und auf andere grundlegende Rechtsprinzipien. Im Falle sehr weit fortgeschrittener Systeme und auf KI basierender Autonomie könnte die Ächtung oder die Beschränkung ihrer Entwicklung tatsächlich eine Lösung sein. Es ist deshalb wichtig, zwischen völliger Autonomie, die eine autonome Entscheidungsfindung beinhaltet, und „Automatisierung“ oder Halbautonomie, wie sie bereits in UAVs Anwendung findet, zu unterscheiden. Es gilt besonders die letztgenannten Technologien zu beobachten, da bei diesen eine Ächtung aufgrund ihrer breiten Verfügbarkeit und kommerziellen Nutzung keine Option mehr darstellt.

Einige der Technologien in unbemannten Systemen und autonomen Trägermitteln sind wenig fortgeschrittener Natur. Das schließt kleine Elektromotoren, einfache Sensoren wie Kameras, akustische, Wärme- und Drucksensoren, Mikroelektronik und Prozessoren, Leichtbaumaterial (wie Kohlefaser), Kommunikationssysteme und Software für automatisierte Systeme ein. All diese Materialien sind auch nichtstaatlichen Akteuren oder Terroristen zugänglich. Kleine Drohnen, sogenannte „Marke Eigenbau“-Geräte oder „Hobbydrohnen“ können im Elektrosupermarkt an der Ecke erworben werden, und sogar unsere Kinder können sie steuern.

Diese Technologien werden permanent weiterentwickelt, günstiger und in zunehmendem Maße verfügbar, entweder im offenen Internet oder im „Darknet“. Es ist nahezu unmöglich, sie zu kontrollieren, da es sich oft um zivile Technik „von der Stange“ und mit nahezu unendlichen Nutzungsmöglichkeiten handelt. Solche frei verfügbaren Komponenten reichen, um eine einfache kleine Drohne herzustellen, die dann zu einer Waffe umgebaut und ferngesteuert oder mit einem vorher definierten Ziel automatisiert eingesetzt werden kann. Die Verluste an Menschenleben durch den Einsatz einer solchen Drohne wären wohl eher niedrig, solange sie nicht mit chemischen, biologischen, radioaktiven oder hochwirksamen Sprengstoffen (CBRe[3]) kombiniert werden, was wiederum zusätzliche technische Hürden mit sich bringen würde. Dennoch könnte eine solche Kleindrohne ausreichen um große Panik auslösen, wenn sie etwa bei großen öffentlichen Veranstaltung wie Rockkonzerten oder in einem Fußballstadion eingesetzt würde. Sich gegen solche Drohnen zu verteidigen ist aufgrund der kleinen Größe schwierig, insbesondere wenn mehrere davon in größerer

[1] Yayla, Ahmet (2017): The Potential Threats Posed By ISIS's Use Of Weaponized Air Drones And How To Fight Back, in: Huffington Post, https://www.huffingtonpost.com/entry/the-potential-threats-posed-by-isiss-use-of-weaponized_us_58b654b3e4b0e5fdf6197894
[2] The New York Times (2017): Pentagon tests tech to combat ISIS Drones (26. September), S. 1.
[3] CBRe bezeichnet *chemical, biological, radiological material or high impact explosives.*

Zahl gleichzeitig eingesetzt würden. Zu den derzeit, auch durch das Pentagon erprobten Gegenmaßnahmen gehört es die Funkverbindung zu stören oder die Sensorik zu täuschen. Auch konventionellere Mittel wie Schusswaffen könnten gegen Drohnen eingesetzt werden. Dies birgt allerdings die Gefahr schwerer Kollateralschäden. Einige Staaten denken deshalb sogar darüber nach, Raubvögel wie Adler oder Bussarde einzusetzen, um kleine Drohnen ohne weiteren Schaden zu neutralisieren, was allerdings gegen eine größere Zahl kleinerer, gleichsam im „Schwarm" eingesetzter Drohnen kein wirkungsvolles Mittel wäre.

Zugleich gewinnen Technologien an Bedeutung, die eher am Ende des hochtechnologischen Spektrums rangieren. Dazu zählen Systeme, die tatsächlich dazu befähigt sind, Entscheidungen autonom zu treffen – darunter insbesondere die autonome Zielauffassung. Ebenso zählen dazu ausgereiftere, stärkere und dynamischere Antriebssysteme, widerstandsfähigere Materialien wie Titan und Luftfahrtaluminium sowie hochentwickelte Sensoren (Nachtsicht, Wärmebild, RADAR, Laserentfernungsmesser). Zu dem hochtechnologischen Spektrum gehören zudem Techniken zur Zerstäubung chemischer und biologischer Stoffe, Autopilotsoftware für schwerere und komplexere Flugwerke und größere Nutzlasten, Hochleistungsbatterien mit geringerem Gewicht sowie kleine Hochleistungsprozessoren. Ausgereifte Schwarmtechnologie ist glücklicherweise, wenngleich sie durch Militär und Unternehmen entwickelt wird, derzeit für nichtstaatliche Akteure (noch) nicht verfügbar. Der zusätzliche Nutzen den UAV-Schwärme für terroristische Zwecke bringen würden, sowohl mit Blick auf die Kosten, als auch auf den Aufwand, sollte nicht zu hoch eingeschätzt werden.

Probleme und Hürden, die einem terroristischen Gebrauch entgegenstehen

Die Nutzlast erschwinglicher UAVs auf dem kommerziellen Markt ist noch immer viel zu gering, um größere Mengen Sprengstoff oder CBRe-Material zu transportieren. Ferner müssten Stoffe, die gefährlich genug sind, um in kleiner Dosierung größeren Menschenmengen zu schaden (wie bestimmte chemische oder biologische Gifte), sehr weitflächig zerstäubt/verteilt werden, um ihre Wirkung zu entfalten. Angesichts der Tatsache, dass Unternehmen wie Amazon aber bereits auf größere „Lieferdrohnen" setzen und damit experimentieren, kann sich das allerdings schnell ändern. Die Beschaffung oder auch die das Umdirigiren solcher Drohnen zu missbräuchlichen Zwecken (wie etwa ihre „Entführung" durch terroristische oder andere nichtstaatliche Gruppierungen) entwickelt sich zu einem immer realistischeren Bedrohungspotential.

Wie bereits dargestellt, und obwohl sich die Technologien sowohl im Hinblick auf Künstliche Intelligenz (autonome Entscheidungsfindung) wie auch auf die Hardware rapide weiterentwickeln, sind vollständig autonome UAVs sogar in den am weitesten fortgeschrittenen Streitkräften noch nicht eingeführt worden. Auch die nötige Software zu ihrer Steuerung ist noch nicht frei verfügbar. Viele andere Systeme, bei denen Autonomie eine Rolle spielt, wie etwa „Google Cars" oder „Fliegende Taxis", befinden sich noch in einer experimentellen Phase und sind teuer. Diese Technologien entwickeln sich jedoch sehr schnell, und viele der Systeme werden bald günstiger und zunehmend für zivile und private Nutzer verfügbar werden. Derzeit werden sie noch durch eine geringe Anzahl von Herstellern und Händlern entwickelt und produziert. Dies macht es potentiell einfacher sie zu kontrollieren und ihre Verbreitung nachzuverfolgen. Hier kommt auf die Industrie und die Forschung eine besondere Verantwortung zu. Die westlichen Staaten haben in diesem Wettbewerb auch noch einen Vorsprung, der es möglich macht, Standards zur Kontrolle dieser Technologien zu setzen.

Es kann aber dennoch nicht ausgeschlossen werden, dass finanzstarke und gut organisierte terroristische Gruppierungen mit großen Ausbildungskapazitäten und wissenschaftlicher Expertise wie der IS schon heute oder in naher Zukunft Zugang zu solchen Technologien bekommt. Sie könnten eine fortgeschrittene Drohne oder andere Trägermittel entweder selbst entwickeln oder anderweitig beschaffen, um sie im Rahmen eines automatisierten oder durch Menschen ferngesteuerten Angriff gegen gut geschützte Ziele einzusetzen, wie etwa Kraftwerke, Wasserwerke und andere kritische Infrastruktur oder gegen militärische Liegenschaften. Deshalb lohnt es sich, zu diskutieren, wie die Verbreitung solcher Systeme am effektivsten kontrolliert werden kann – besser bevor als nachdem sie breiter eingeführt worden sind.

Wie würden diese Technologien das terroristische Risikokalkül beeinflussen?

Wie die jüngsten Terrorfälle gezeigt haben, spielt technologischer Fortschritt im Denken terroristischer Gruppierungen derzeit keine große Rolle. Auch ob größere oder technisch fortgeschrittenere Drohnen oder autonome Fahrzeuge, sei es in der Luft, zu Wasser oder zu Land, Terroristen wirklich substantielle Vorteile gegenüber einfacheren ferngesteuerten Mitteln bringen würden – sieht man von größerer Geschwindigkeit, Nutzlast und Genauigkeit ab, ist noch weitaus unsicherer. Der Herstellungsprozess solch komplexerer Systeme ließe sich wesentlich schwieriger geheim halten und fiele deutlich kostenintensiver aus. Die mögliche Verwendung hinge demnach einerseits von den Fähigkeiten und Finanzmitteln der Gruppierung ab und andererseits davon, ob größere Nutzlast, Autonomie und schwieriger erreichbare Ziele den zusätzlichen Aufwand rechtfertigen würden. Vorausgesetzt, dass vollständig autonome Technologie einmal breiter verfügbar wird, stellt sich als wichtigste Frage, unter welchen Bedingungen die Beschaffung eines wirklich autonomen Systems sich für eine nichtstaatliche oder eine terroristische Gruppe lohnen würde und wann in der Zukunft sich das derzeitige Kosten-Nutzen-Kalkül einer solchen Gruppierung ändern könnte.

Autonomie (oder zumindest Halbautonomie) birgt eine Reihe von Vorteilen für Terroristen, da sie deren eigene Verluste reduziert. Man stelle sich für einen Moment vor, dass anstelle eines Lastwagens ein unbemanntes Bodenfahrzeug in einem der Angriffe in Nizza, Berlin oder Barcelona verwendet worden wäre. Das Fahrzeug wäre nicht nur mangels eines Fahrers an Bord wesentlich schwieriger zu stoppen gewesen; auch hätte kein Angreifer sein Leben riskieren müssen, und die Identifizierung eines Täters oder einer Tätergruppe wäre wesentlich schwieriger gewesen. Ebenso bräuchten UAVs, die zu Terroranschlägen verwendet werden, um Sprengsätze zu verbringen oder bestimmte CBRe-Stoffe zu verbreiten nicht völlig autonom zu sein, während sie zugleich immer noch den Täter davon entbinden würden, direkt mitbetroffen zu sein. Die Waffenwirkung automatisiert auszulösen und durch autonome Navigation ein Ziel zu erreichen – Technologien, die bereits zum Beispiel in Marschflugkörpern Anwendung finden – würden ausreichen. Ein UAV müsste für solche Manöver keine autonome Entscheidungsfindung beherrschen. Ein solches Szenario ist demnach wahrscheinlich viel realistischer.

„Standard"-UAVs sind günstig und stützen sich auf solide entwickelte und erprobte Technologie. Es ist sogar möglich, dass eine Drohne schlichtweg durch Terroristen ferngesteuert würde, wobei allerdings die Gefahr der Entdeckung (oder der Störung des GPS-Systems) in diesem Fall wesentlich höher wäre. Wenngleich es für manche Gruppen einfach zu sein scheint, in großem Umfang Freiwillige zu finden, die bereit sind, ihr eigenes Leben in Terroranschlägen zu verlieren (wie das Beispiel radikalisierter IS-Unterstützer zeigt), dürften kleinere oder stärker zentralistisch organisierte Gruppen einem anderen Kalkül unterliegen. Da unbemannte oder zumindest halbautonome Personen- und Lastwagen aller Voraussicht nach in den nächsten fünf bis zehn Jahren marktreif sein werden, könnte auch aus diesen ein neues Bedrohungspotential erwachsen.

Künftige Risiken: Offene Fragen und Klärungsbedarf

Wie bereits ausgeführt, sind viele der Technologien die für vollständig autonome oder halbautonome Waffensysteme entwickelt und benötigt werden noch nicht frei verfügbar oder für terroristische Gruppierungen zumindest schwer zu beschaffen. Jedoch könnten neue Systeme wie Drohnen oder unbemannte Bodenfahrzeuge, die bereits verfügbar sind oder es bald sein werden, für Terroranschläge verwendet werden. Deshalb gilt es, gerade diese Technologien genauer in den Blick zu nehmen, um aus ihnen erwachsende künftige Risiken besser einschätzen zu können. Auch müssen Fragen terroristischer Kosten-Nutzen-Kalkulation sowie die Möglichkeit, die Verbreitung der einschlägigen Technologien besser zu kontrollieren, diskutiert werden. Zu diesen Fragen zählen:

- In welchen terroristischen Szenarien würde der Gebrauch eines UAVs oder eines unbemannten Bodenfahrzeugs Attentätern einen Vorteil gewähren? Welchen zusätzlichen Einsatzwert brächten hier autonome Systeme?

- Würde eine zunehmende Autonomie von Systemen die Identifizierung und Zuschreibung zu einer terroristischen Gruppierung erschweren?

- Welche kritischen technologischen Entwicklungen müssen beobachtet werden, insbesondere im Hinblick auf UAVs? Wie kann das Installieren von Autonomiesoftware in ansonsten nichtautonomen Systemen beschränkt werden? Wie können autonome Flug-/Fahrzeuge bereits bei der Herstellung besser gegen Missbrauch geschützt werden?

- Woher könnten Terroristen sich autonome Systeme beschaffen? Was kann getan werden, um zu verhindern, dass nichtstaatliche Akteure selbst autonome Systeme entwickeln, sobald die nötige Technologie „demokratisiert" worden ist?

- Was wären mögliche Gegenmaßnahmen, um autonome Flug-/Fahrzeuge zu stoppen? Wie können diese (insbesondere in einem urbanen Umfeld) eingesetzt werden? Gibt es verlässliche Stör-/Abschalt-/Täuschungstechnologien, um sie zu stoppen und wem sollten sie zugänglich gemacht werden?

- Wie groß ist der Unterschied zwischen Hochtechnologie und einfacher Technologie mit Blick auf das Bedrohungspotential und die Verbreitungsgefahr? Erfordern sie verschiedene Kontrollmaßnahmen?

- Sollte der Schwerpunkt der Kontrollen eher auf einfache oder vornehmlich auf hochentwickelte Technologien gelegt werden? Welche bergen die größeren Gefahren?

- Sollten die Anstrengungen darauf konzentriert werden, Technologien im Zusammenhang mit unbemannten Systemen und Autonomien zu beobachten, weil sie das Potential haben, die Kriegführung zu verändern? Oder sollten sie eher darauf konzentriert werden, den Missbrauch solcher Technologien für die Verbreitung von CBRe-Stoffen zu verhindern?

Obwohl viele dieser Fragen derzeit offen sind, bleibt das Risiko, dass autonome oder semi-autonome Systeme durch Terroristen benutzt werden, derzeit gering. Der Einsatz von Messern, Schusswaffen, improvisierten Sprengsätzen oder Lastkraftwagen werden auf absehbare Zeit die Hauptmittel für Terroranschläge bleiben, jedenfalls für weniger gut organisierte Gruppen oder radikalisierte Einzeltäter. Es ist dennoch empfehlenswert, sich genauer anzusehen, wie neue Technologien, die derzeit entwickelt werden oder für nichtstaatliche Akteure und Terroristen zugänglich werden könnten, unsere Gefahreneinschätzung in der Zukunft verändern könnten.

Wolfgang Rudischhauser[4] ist Vizepräsident der Bundesakademie für Sicherheitspolitik in Berlin. Der Autor gibt seine persönliche Meinung wieder.

[4] Jean Backhus und Stefan Maetz, meine vormaligen Praktikanten bei der NATO, haben mit ihren Gedanken und Anmerkungen zu diesem Artikel beigetragen. Der Beitrag gibt nichtsdestotrotz ausschließlich die persönliche Meinung des Autors und auch nicht die der Bundesakademie für Sicherheitspolitik wieder.