

Rüdiger Stix

## Zwischen Packesel und Killerroboter

### Teil 1: Drohnen, unbemannte Plattformen zu Luft, zu Land und auf See

Woran denken wir, wenn wir von Drohnen hören? Meist entfalten sich vor uns Bilder von eigenwilligen Fluggeräten, von selbstlenkenden, unbemannten Kampfflugzeugen in Afghanistan – oder in Action-Thrillern und in Science-Fiction-Filmen. Sprachlich leitet sich der Begriff Drohne aus dem niederdeutschen „drone“, lautmalerisch zu ‚Dröhnen‘, bzw. aus dem indogermanischen „dhren“, also „brummen“, ab und steht nicht nur für die männliche Honigbiene, Hummel, Wespe oder Hornisse, sondern auch für unbemannte Luftfahrzeuge und für (Spielzeug-)Flugmodelle, ja im weiteren Sinn für jedes unbemannte Fahrzeug, auch zu Land oder zu Wasser.

Der Übergang zu Robotern ist fließend. Selbstlenkende Geräte können auch krabbelnd, kriechend und vielleicht sogar auf sechs bis acht Beinen stapfend unterwegs sein. Selbststeuernde Plattformen können den Körpern von Pferden nachgebaut sein, oder dem Vorbild von Raupen, von Spinnen, und natürlich von allem, was im Wasser gleitet. Findigen Ingenieuren sind dabei keine Grenze gesetzt, und so werden uns künftig insektengroße Selbstflieger aus Bio-Materialien genauso beschäftigen wie riesige Hyperschallflugkörper an der Grenze der Stratosphäre. Es gibt noch keine international verbindliche Definition, was denn nun als Drohne zu gelten hat und was als sonstiger Roboter. Allerdings gibt es zwei, drei Zugänge im populären Umgang, und auch in den verwendeten rechtlichen Rahmen, die uns eine gewisse Ordnung in der Evolution von Drohnen ermöglichen.

Wenn wir unser Augenmerk primär den militärischen Drohnen, also (potentiell) bewaffneten autonomen Plattformen, zuwenden, sollten wir nicht vergessen, dass wir fast alle unsere fernen Reiseziele in „Drohnen“ erreichen, in (semi)autonomen Plattformen, wie etwa in den üblichen und ganz gewöhnlichen Passagierjets, sobald diese auf Autopilot geschaltet sind – was wohl die überwiegende Zeit der Fall sein dürfte, auch wenn die Piloten wahrscheinlich an Bord und hoffentlich auch in der Nähe des Cockpits sind.

Es ist dabei auch gar nicht so unwahrscheinlich, dass wir bei unseren Ferien- oder Geschäftsreisen im Flug die Bahnen von anderen Fluggeräten kreuzen, die ebenfalls autonom fliegen, und es kann sein, dass die eine oder andere Maschine ihren Piloten einige tausend Kilometer entfernt am Boden sitzen hat – in einem militärischen Einsatzzentrum.

#### Sprunghafter Anstieg autonomer militärischer Plattformen

Lassen wir dabei mit heutigem Stand Revue passieren, wie die sprunghaft angestiegene und weiter steigende Zahl semiautonomer und autonomer militärischer Plattformen behandelt wird, so kann man derzeit zusammenfassend sagen: Auch bewaffnete autonome Plattformen bewegen sich als Plattform, also als Verkehrsmittel, gemäß den entsprechenden Regeln der jeweiligen Verkehrsträger. Dies heißt, in der Luft nach den Regeln der internationalen Zivilluftfahrt, also der ICAO (International Civil Aviation Organization), bzw. nach den Nor-

men der Militärluftfahrt, wobei in Österreich der Luftraum bis zur Höhe von 30 Metern über dem Boden für Spielzeuge freigegeben ist (was Modellflugzeuge und kleine Drohnen begünstigt).

Auf dem Boden bewegen sich unsere autonomen Plattformen gemäß den nationalen Bestimmungen zum Straßenverkehr, wenn sie auf den Straßen fahren oder laufen, bzw. gemäß den Regeln zur Nutzung von Gelände abseits der öffentlichen Verkehrsflächen, falls sich unsere Landdrohnen im Gelände tummeln sollten. In Österreich geben den Rahmen die Bestimmungen der StVO (Straßenverkehrsordnung), des Forstgesetzes oder des MBG (Militärbefugnisgesetzes) vor. Auf hoher See wird's dann etwas unbestimmter. Schwimmende und tauchende Drohnen bewegen sich gemäß der Regeln des Seerechtsübereinkommens, meistens im Status eines Staatsschiffes bzw. eines Kriegsschiffes. Alle aufgezählten Beispiele der autonomen Plattformen zu Lande (also auf der Straße), in der Luft, oder zur See (wenn sie den Status eines Schiffes oder Kriegsschiffes beanspruchen, und nicht als Treibgut oder Bergegut betrachtet werden wollen), haben eines gemeinsam: Sie befinden sich zumindest theoretisch jederzeit unter menschlicher Kontrolle, auch wenn die Piloten, die Fahrer oder die Skipper sehr weit entfernt in ihren Kontrollzentren sitzen.

Falls die Kontrolle ausgeschaltet wird und die bewaffnete Drohne autonom agiert, ist sie eine Waffe – ähnlich wie andere schon lange bekannte selbstlenkende Waffen, von den frühen Marschflugkörpern (Cruise Missiles) in den Zeiten der V1 („Vergeltungswaffe“) über Roboter-Panzer bis zu selbstlenkenden Torpedos.

Theoretisch ist es auch denkbar, dass es in absehbarer Zeit weitgehende Rüstungskontrollbeschränkungen und Verbote gegen autonome Waffen gibt: Wir sehen dabei insbesondere die Initiative „Campaign to stop killer robots“ der US-amerikanischen Nichtregierungsorganisation „Human Rights Watch (HRW), die von vielen internationalen Aktivisten gestützt wird.

Dies wird zwar technologisch fortgeschrittene Staaten vermutlich nicht sonderlich behindern in der Entwicklung von autonomen Plattformen. Diese werden dann offiziell erst im Bedarfsfall, gegebenenfalls in einem formalen Krieg, mit Waffen ausgestattet werden – oder eben in aller rechtlich gebotenen Form unter der geforderten Fernaufsicht, also überwacht, „in the loop“ kontrolliert bleiben – bis zum eigentlichen Einsatz.

Bemerkenswert ist dabei, dass die gesamte Entwicklung von autonomen Waffenträgern, also von Militärrobotern, juristisch betrachtet ins humanitäre Völkerrecht, also ins Kriegsvölkerrecht, ausgelagert wurde.

Das Spektrum der modernen Drohnen reicht also von riesigen, strategischen unbemannten Flugzeugen bis in den fliegengroßen Bereich der Mikrodrohnen – und selbstverständlich gibt es fliegende Paket-Zulieferer von Amazon oder High-Tech-Rollstühle, die auch schon autonom fahren können. Dennoch dominiert die Militärtechnik.

## Österreichische Spitzentechnologie

Dabei sind trotz der Dominanz der USA in der Luft- und Weltraumtechnologie sowie in den Science-Fiction-Filmen auf dem Gebiet der Drohnentechnologie auch Europa und insbesondere Österreich ganz vorne mit dabei, in Teilbereichen sogar weltweit führend. Zwar kennen viele aus den einschlägigen Actionfilmen und aus den Nachrichten von den Kriegsschauplätzen dieser Welt amerikanische Drohnen in spektakulären Aufnahmen, doch ist wohl nur wenigen bewusst, dass diese amerikanischen Drohnen in der Regel mit österreichischer Technologie der Fa. Rotax, eines Motorenherstellers in Gunskirchen in Oberösterreich, fliegen. Sogar ein weltweit führendes eigenständiges Drohnensystem ist österreichisch. So sind die Schiebel-Helikopterdrohnen (Firmensitz: Wien-Margarethen) sowohl zu Land als auch zur See eingesetzt. Wahrscheinlich sind die Schiebel-Marinedrohnen sogar derzeit die weltbesten unbemannten Hubschrauber für den Einsatz auf hoher See.

Jeder von uns kennt wohl auch die Diskussion darüber, wie bewaffnete Drohnen über tausende Kilometer Entfernung zum Einsatz kommen. So ist es durchaus üblich, dass die Piloten

jener Kampfdrohnen, die etwa im Jemen oder in Afghanistan Einsätze fliegen, irgendwo in einem Luftwaffenstützpunkt der USA sitzen.

## „gespamt“ und „gespooft“

Selbstverständlich wissen wir auch, dass eine Drohne, egal ob sie routinemäßig Aufklärung fliegt oder in einem Kampfeinsatz unterwegs ist, auch ihre Verbindung zu ihrem „Piloten“ und zum Kontrollzentrum verlieren kann. Genau genommen ist dies nicht nur eine theoretische Möglichkeit, sozusagen eine Art unangenehmes und selten vorkommendes technisches Versehen, sondern es ist vielmehr eine Situation, mit dem bei jedem Drohneneinsatz zu rechnen ist – zumindest wenn er sich gegen einen technisch versierten Gegner richtet. Der Pilot jeder Drohne muss also damit rechnen, dass sie „gespamt“ (mit unerwünschten Informationen gefüttert) oder „gespooft“ (getäuscht) wird, also in deutsche Worte gefasst, dass die Funkverbindung durch Störsender unterbrochen wird, oder dass sie Fehlinformationen gesendet bekommt, typischerweise meist Informationen über ihre Orientierung, beispielsweise falsche Satellitendaten...

Umgelegt auf eine nichtmilitärische Situation würde „spoofen“ bedeuten, dass uns unser Navi im Auto plötzlich nicht auf der Bundesstraße oder auf der Autobahn sieht, sondern im daneben liegenden Fluss. Dabei scheint es dringend empfehlenswert, im Zweifel auf die eigene Wahrnehmung zu achten und nicht dem Navi zu glauben ...

Selbstverständlich ist es über die elektronische Kampfführung durch „Jammen“ (Stören) oder „Spoofen“ (Täuschen) hinaus auch üblich, dass man zumindest versucht, sich in das Leitsystem gegnerischer Drohnen hinein zu hacken. Wiederum umgelegt auf zivile Anwendungen müssen wir damit rechnen, dass mit entsprechender krimineller Energie Hackerangriffe auch auf Steuerungssysteme möglich sind, wenn etwa ein Schadensfall provoziert werden soll, indem man autonome Steuerungen von Lkws oder von Hochseeyachten hackt, oder Energie-Versorgungs-Netzwerke lahmlegt oder im Fall von Spitälern auf Patientenversorgungssysteme zugreift, wenn nicht gar auf zukünftig automatisierte Leistungen im Operationsaal.

Wir erkennen dabei auch deutlich, dass der Übergang zur reinen Netzkriegsführung, dem „Cyberwar“, sehr fließend ist, und dass durch den Einsatz von Hackern und von Schad-Software so ein Gerät, womöglich sogar autonom selbstlernend, wie eine fast körperlose Waffe im Netz agiert, quasi als „Cyber“-Drohne ...

Im Normalfall hat daher jeder verantwortungsbewusste Drohnenbetreiber für den Fall eines Cyber-Angriffes auf die Steuerungssysteme vorgesorgt: Die Drohne fliegt dann entweder Warteschleifen, oder, wenn sich der Kontakt zur Kontrollbasis nicht mehr gesichert herstellen lässt, wieder „nach Hause“.

Damit wäre die Sache auch erledigt, wenn es sich um eine Paket-Drohne handelt, oder um eine Luxus-Yacht, die damit dem Versuch entgeht, auf ein Riff gesteuert zu zerschellen wie in früheren Zeiten, in denen unglückliche Seefahrer den irreführenden Leuchtfeuern von Strandpiraten gefolgt sind. Aber wir können wohl nicht einfach abschalten und nach Hause fliegen, wenn ein heikler Rettungs- oder Kampfauftrag betroffen ist.

Wahrscheinlich können wir uns leicht hineinversetzen in einen Rot-Kreuz-Beobachter, der beispielsweise in Afghanistan in den Hinterhalt von Talibankriegern gerät, und dessen einzige Rettung darin besteht, dass ihm eine Drohne Feuerschutz gibt, damit er sich zurückziehen kann.

Wir können uns daher auch sehr plastisch vorstellen, dass dieser Rot-Kreuz-Beobachter wenig Freude hat, wenn die Drohne plötzlich aufhört, ihm Feuerschutz zu geben, und aus Sicherheitsgründen gemächlich nach Hause fliegt, weil sie „gespamt“ oder „gespooft“ worden ist und daher aufgrund der formellen Bestimmungen der (Luft-)Verkehrssicherheit nicht mehr autonom alleine weiter unterwegs sein dürfte. Selbstverständlich wissen das auch alle – zumindest industrialisierten – Streitkräfte, die Drohnen einsetzen, und sie haben wohl si-

cher für diesen Fall vorgesorgt. Die Drohne wird daher in einem Kampfeinsatz vermutlich auf ein automatisiertes System umschalten und ihren Kampfauftrag autonom fortsetzen.

Entwickler von Software für autonome Plattformen verfolgen daher mit Interesse, wie Streitkräfte, insbesondere die wohl weltweit dominierenden US-Militärs, auf diesem Gebiet Vorsorge getroffen haben, und welche rechtlichen Lösungsansätze entwickelt werden.

Das Pentagon (US-Verteidigungsministerium) hat daher bereits im November 2012 eine Direktive in Kraft gesetzt, die als die DOD-Direktive 3000.09 noch heute als Standard gilt, und die festhält:

„Autonomous and semi autonomous Weapon Systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgement over the use of force“.

Man sieht schon an der Formulierung die Vorsichtigkeit, die sich natürlich auch auf die Entwicklung von voll autonomen Systemen bezieht, wobei die DOD-Direktive 3000.09 festhält, dass sie, also das Department of Defense (DOD), derartige Entwicklungen sehr eng überwachen werden.

Gleichzeitig verlangt das Pentagon eine angemessene Sorgfalt in der Anwendung des humanitären Völkerrechtes (Kriegsvölkerrecht), sowie der international anwendbaren Verträge, der Sicherheitsbestimmungen der betroffenen Waffensysteme und die anwendbaren Regeln des Einsatzes (ROE/Rules of Engagement).

Daraus ist erkennbar, dass sowohl das Pentagon, als wohl alle anderen Staaten auch, die autonome Waffenplattformen als Drohnen einsetzen, diese unter die Regeln des humanitären Völkerrechtes stellen – was bedeutet, dass autonome bewaffnete Plattformen juristisch betrachtet im Zweifelsfall dann eben schlicht als Waffen gelten und den Konfliktregeln unterliegen, nach denen Waffen legal eingesetzt werden können.

## Initiativen zur internationalen Ächtung

Auf dieser Ebene spielt sich die Diskussion auch von Seiten der Kritiker ab, konzentriert durch die schon zitierte Human-Rights-Watch-Organisation. Auch sie hat schon im November 2012 eine Initiative eingeleitet, um durch international bindende Verträge zu erreichen, dass autonome Waffenträger international geächtet bzw. generell verboten werden sollten („Loosing Humanity: The case against killer robots“).

Vorbild dieser Initiative sind die bereits existierenden internationalen Verbote von Landminen o.ä., die durchaus eine gewisse humanitäre Wirkung entfalten (und zu Lasten der schlechter entwickelten Staaten gehen, da die Industriestaaten bekanntlich über andere Möglichkeiten mit elektronisch steuerbaren Sprenganlagen verfügen). Aber wahrscheinlich ist diese Debatte nur eine Sackgasse oder eine juristische Haarspalterei – denn jede autonome Waffe müsste ja jetzt schon im Fokus dieser internationalen Debatten sein, wenn es nur um die Frage geht, ob denn eine menschliche Kontrolle über die Drohne als autonome Plattform, oder eben auch über die schon lange im Einsatz befindlichen autonomen Waffen, gesichert ist.

Das überzeugendste Argument dieser Debatte ist jedoch eine andere Sorge, die ausgerechnet das US Militär dem Vernehmen nach auch offiziell sehr ernst nimmt: Können sich in absehbarer Zeit autonome Systeme dank künstlicher Intelligenz mit unseren Plattformen und Waffen selbstständig machen – ganz egal, ob diese künstliche Intelligenz so etwas wie ein Bewusstsein schon entwickelt hat, oder ob sie „nur“ ein blind außer Kontrolle geratenes selbstlernendes Programm ist ...?

Wir sprechen also von einem filmreifen Szenario wie etwa vom Bordcomputer HAL 900, der in Stanley Kubricks „2001 – Odyssee im Weltraum“ die Besatzung seines Raumschiffes (fast) komplett tötet, um die Mission zu schützen, oder vom „Sky-Net“, welches in den Terminator-Filmen die Menschheit ausrotten will – und hierzu sagt sogar der stellvertretende Joint Chief of Staffs der USA, General Selva, dass dies inzwischen denkmöglich sei ...

Dabei ist seine Begründung verblüffend, aber nachvollziehbar: Bisher waren alle High-Tec-Programme der USA, von der Entwicklung der Nuklearwaffen im Manhattan-Projekt bis zum Griff nach dem Weltraum durch die Raumfahrtbehörde NASA, allesamt Regierungsprojekte, wobei allerdings die technologische Basis der Industrie dabei mitgezogen wurde. Bei der künstlichen Intelligenz sei dies inzwischen anders. Ungeachtet der zweifellos beeindruckenden Ballung an Ressourcen von künstlicher Intelligenz in Regierungsbehörden, nicht zuletzt im Geheimdienst NSA, der „National Security Agency“, so liegen doch die bei weitem überwiegenden Kapazitäten der künstlichen Intelligenz nicht bei der Regierung, sondern in der Industrie – also vereinfacht gesagt, nicht im Pentagon, sondern allen voran bei Apple, bei Google, Microsoft oder bei Facebook ... und natürlich auch mit etwas Abstand in Russland, in China, Indien, Japan sowie in den Industrien Europas.

Lesen Sie demnächst in **Teil 2**:  
Wie intelligent ist künstliche Intelligenz?