Interdisziplinäres Kolloquium am 11. November 2010:

Auf dem Weg zur Automatisierung und Digitalisierung des Krieges

Tagungsbericht von Dr. Roman Schmidt-Radefeldt

Nach den Grußworten des Präsidenten der Bundesakademie, Generalleutnant a.D. Lahl, dem Vorsitzenden der Deutschen Wehrrechtsgesellschaft, Dr. Weingärtner, und dem Geschäftsführer der Molinari-Stiftung, Herrn Christian Singer, wurde die Tagung mit einer Keynote von Elizabeth Quintana vom Royal United Service Institute for Defence and Security Studies, London zum Thema "Wandel des Krieges im High-Tech-Zeitalters" eröffnet. Frau Quintana charakterisierte den künftigen Konfliktschauplatz als zunehmend überfüllt, ungeordnet (etwa mit Blick auf die Unterscheidung zwischen den verschiedenen Akteuren) umkämpft, miteinander verbunden aber auch durch gewisse rechtliche Standards eingehegt.

Quintana skizzierte sodann die technologischen "Megatrends" bei bewaffneten Konflikten und stellte diese in den Zusammenhang ethischer Anforderungen. Abschließend erörterte sie die Frage, inwieweit Cyber und unbemannte Waffensysteme, welche die Reichweite menschlicher Einflussmöglichkeiten erweiterten und den Menschen gleichzeitig aus dem Zentrum des Kriegsschauplatzes verbannten, auch die Wahrnehmung bzw. die Begrifflichkeit des Krieges ändern würden. Unter Berufung auf wichtige Stimmen in der aktuellen amerikanischen Diskussion (Peter Singer, Ron Arkin) hielt Quintana es für denkbar, dass die Werkzeuge des Krieges immer auch den militärischen Ethos und die Art der Kriegsführung beeinflussen würden. Gleichwohl sei aber letztlich nicht die Technologie entscheidend, sondern die Art und Weise ihres Einsatzes.

In dem anschließenden Panel befassten sich zwei Vorträge mit dem Einsatz unbemannter Waffensysteme am Beispiel von Drohnen.

Dr. Niklas Schörnig von der Hessischen Stiftung Friedens- und Konfliktforschung Frankfurt machte den Auftakt mit einem politik- und sozialwissenschaftlichen Referat über "Die Automatisierung des Krieges - eine kritische Bestandsaufnahme". Schörnig beobachtete in diesem Zusammenhang einen weltweiten militärischen Trend zur Automatisierung; nicht nur im Hinblick auf eine rasante Nachfrage der Staaten nach unbemannten robotischen Systemen, sondern auch bei der Automatisierung von Prozeduren und Entscheidungsprozessen.

Betroffen seien dabei vor allem die Fernsteuerung und Fernüberwachung, während Automatisierungstendenzen im Bereich des eigentlichen Waffeneinsatzes bislang noch nicht realisiert, wohl aber diskutiert würden.

Schörnig wies nach, dass gerade westliche Staaten aus militärischen, politischen und gesellschaftlichen Gründen besonders an Entwicklung und Einsatz unbemannter Waffensysteme interessiert seien, wobei neben fiskalischen Einsparungen und einem technisch und kulturell motivierten Prestigedenken vor allem die Erwartungen an eine Minimierung eigener Opfer im Vordergrund stünden.

Gleichzeitig zeigte Schörnig die Schattenseiten der Drohnenrüstung auf, welche langfristig destabilisierende Wirkungen hätten. Zwar sei die Fehlerrate bei Einsätzen unbemannter

Waffensysteme nicht höher als bei bemannten Flugobjekten, doch würden unbemannte Waffensysteme sogar bei "Zivilmächten" allzu schnell als "Allheilmittel" zur Lösung aktueller Probleme angesehen, während die langfristigen Folgen - wie etwa die sich abzeichnende Gewaltspirale bei asymmetrischen Konflikten, die sinkenden Hemmschwellen in der militärischen Auseinandersetzung oder die Unterminierung der US-Counter Insurgency-Strategie, "hearts and minds" zu gewinnen - unterbewertet blieben. Drohneneinsätze erschienen insoweit in der Wahrnehmung der afghanischen Taliban als eine besonders arrogante Form der Kriegführung.

Da unbemannte Waffensysteme praktisch von keinem Rüstungskontrollvertrag erfasst würden, plädierte Schörnig in seinem Vortrag für eine kontrollierte Rüstung im Sinne einer politischen Selbstbeschränkung.

Im nachfolgenden Vortrag widmete sich der Völkerrechtsprofessor Thilo Marauhn von der Universität Gießen, der an einem beim Technikfolgenabschätzungsbüro des Deutschen Bundestages angebundenen Forschungsprojekt über die "völkerrechtliche Einhegung unbemannter militärischer Luftsysteme" beteiligt ist, den humanitär-völkerrechtlichen Fragen des Kampfdrohneneinsatzes. Dabei konzentrierte er sich auf eine völkerrechtliche Bewertung der Bewaffnung von Kampfdrohnen, auf die besondere Bedeutung des Unterscheidungsgebotes im Sinne von Artikel 51 des 1. Zusatzprotokolls zu den Genfer Konventionen sowie auf den Status von Bedienungspersonal und Basisstation.

Im Hinblick auf die spezifischen völkerrechtlichen Waffenverbote machte Marauhn deutlich, dass es sich bei Drohnen nicht um Waffen im Sinne des Völkerrechts handelt, sondern um Luftfahrzeuge mit Trägersystemen, deren Bewaffnung an den generellen Verbotsvorschriften (z.B. für chemische oder biologische Waffen) zu messen sei und keine "drohnenspezifischen" Probleme aufwerfe. Mit Blick auf das völkerrechtliche Unterscheidungsgebot warf Marauhn die Frage auf, ob ein vollautomatisiertes Waffensystem - ergo: künstliche Intelligenz - auch darauf reagieren könne, wenn sich im Zielgebiet einer Kampfdrohne eine neue Konstellation hinsichtlich der Zivilbevölkerung oder dem Status ziviler Objekte ergeben sollte. Die Fragen der Korrektur und Anpassung von Veränderungen im Zielgebiet nach dem Start von Drohnen sei bislang nur unzureichend problematisiert worden. Das Humanitäre Völkerrecht stelle hier zwar keine unerfüllbaren Anforderungen, doch würde die zunehmende Ausdifferenzierung und Spezifizierung der Steuerungssysteme dazu führen, dass die an den Staat gestellten Anforderungen im Bereich des "targeting" entsprechend seinen militär-technologischen Fähigkeiten zunähmen. Dies setze nicht nur ein hohes Maß an Aufklärung voraus, sondern verlange auch eine kontinuierliche Fortsetzung von Aufklärungsmaßnahmen. Für den Einsatz von automatisierten Waffensystemen bedeute dies, dass künstliche Intelligenz wegen der besonderen Bedeutung rechtlicher Wertungen mit menschlicher Verantwortung rückgekoppelt werden müsse. Dies setze möglichst weitreichende Möglichkeiten des Bedieners voraus, um in den Einsatzverlauf von Kampfdrohnen intervenieren zu können. Einer völligen Automatisierung von Waffensystemen, welche ohne jegliche Steuerung selbstständig Kriegshandlungen durchführen könnten, stand Marauhn indes ablehnend gegenüber.

In diesem Zusammenhang untersuchte Marauhn die völkerrechtliche Verantwortung für die Kriegsführung, die indes weder beim zuständigen Einsatzoffizier (Bediener) noch beim Programmierer hinreichend begründet werden könne.

Die räumlich-geographische Trennung des Bedienungspersonals und der Basisstation von der Drohne im Einsatz erlaubten indes keine isolierte rechtliche Betrachtungsweise - beides sei vielmehr als

Einheit zu sehen: So seien folglich Basisstation und Bedienungspersonal legitime militärische Ziele im bewaffneten Konflikt; das Bedienungspersonal - sofern es sich um Zivilpersonen (im Zuge der Privatisierung) handele - würde dabei unmittelbar an den Feindseligkeiten teilnehmen.

Abschließend skizzierte Marauhn den Reformbedarf mit Blick auf spezifische Regelungen für den Einsatz unbemannter Waffensysteme. Dieser sei jedoch im gegenwärtigen Stadium der Automatisierung mit dem herkömmlichen völkerrechtlichen Instrumentarium zu bewältigen. Allenfalls beim Einsatz vollständig autonomer Systeme, bei denen es keine Interventionsmöglichkeiten des Steuerers gäbe, müsse über ein rechtliches Einsatzverbot nachgedacht werden.

In der anschließenden lebhaften Diskussion ging es um die Spezifika von automatisierten Waffensystemen, wobei Konsens darüber bestand, dass Drohnen lediglich einen Entwicklungsschritt bei den Distanzwaffen abbilden, aber keine wirkliche "Revolution in Military Affairs" darstellen. Die Frage, wann die insoweit rechtlich zulässige Grenze der Automatisierung erreicht sei, wurde im Zusammenhang mit der konkreten Entscheidung über den Waffeneinsatz gesehen und diskutiert. Bei der Frage nach der menschlichen Verantwortung für und der Rückkopplung von automatisierten Entscheidungsprozessen wurde deutlich, dass sich rechtliche Wertungen nicht in Computersoftware programmieren lassen. Diskutiert (aber verworfen) wurde sodann die These, ob es mit Blick auf die staatliche Fürsorge für seine Streitkräfte und die Minimierung der Opferzahlen eine Verpflichtung zur technischen Hochrüstung geben könne.

Das zweite Panel befasste sich am Nachmittag mit dem Cyber Space als Kriegsschauplatz. Den Auftakt machte Brigadegeneral a.D. Friedrich-Wilhelm Kriesel, ehemaliger Kommandeur des Kommandos Strategische Aufklärung, mit einer Problemanalyse der "Kriegsführung im virtuellen Raum". Er vertrat die These, der Cyber Space sei bereits der entscheidende Ort für Kampfhandlungen - die hochtechnisierten Gesellschaften hätten dies nur noch nicht realisiert, obwohl sie die primär Gefährdeten seien. Der Krieg im Internet würde von zwei Antipoden geführt - der technischen Supermacht und dem (mittellosen) "underdog". Gleichwohl spiele der Cyber Space im militärischen Bereich keine ausschlaggebende Rolle, da militärische Ziele wie z.B. die Besetzung eines Territoriums weiterhin in der "nicht-virtuellen" Welt stattfänden. Vielmehr sei Cyber-Verteidigung eine gesamtstaatliche Aufgabe, der sich Deutschland nicht zuletzt aufgrund von "überzogenen" datenschutzrechtliche Anforderungen nicht offensiv genug stelle.

In der Diskussion wurde indes bezweifelt, ob der Datenschutz in diesem Zusammenhang eine echte Hürde darstelle, da er ohnehin nur die Identifikation von kleinkriminellen Hackern ermögliche, während Cyberangriffe auf operative militärische Systeme zunehmend durch Gruppen von hochspezialisierten Experten durchgeführt würden.

Im zweiten Panelvortrag beleuchtete Dietmar Thelen von CASSIDIAN (EADS) das Thema "Cyber Security und IT-Waffentechnik im Spannungsfeld von Rüstungsindustrie und Sicherheitspolitik". Eingangs skizzierte Thelen den Cyber Space als fünftes militärisches Operationsgebiet und gab einen Überblick über die Entwicklung von Cyber-Attacken im Bereich der NATO, über die Akteure des Cyber Crime, deren Methoden und Motivation sowie über die staatlichen Maßnahmen auf diesem Gebiet. In einem Zeitraum von 1985 bis heute hätten die Cyber-"Tools" an Komplexität und Bedrohungspotential zugenommen - angefangen von einfachen Viren, Würmern und Trojanern bis hin zu Botnets, DDoS-Attacken der "Stuxnet-Klasse", deren Neuheit darin liege, dass sie nicht nur Netzwerke, sondern auch Steuerungssysteme von Industrieanlagen u.a. befallen würden.

Anhand ihrer spezifischen Charakteristika erläuterte Thelen, was IT-Attacken durch sogenannte Malware und Viren diese zu "Waffen" im herkömmlichen technischen Sinne machen würden. Angesichts des dual-use-Charakters bestünden vielfältige Probleme bei der Definition, der Transparenz und Verifikation von IT-Waffen, für die es bislang weder eine gültige Einsatzdoktrin noch greifbare Rüstungskontrollmechanismen gebe. In diesem Zusammenhang betonte Thelen auch die Eigendynamik und den Überraschungsfaktor von Cyber Attacken, deren Wirkung auf der umfänglichen Abhängigkeit westlicher Gesellschaften von Informationstechnologien basiere.

Das Problem der Attribution, d.h. die technisch nicht leistbare Rückverfolgbarkeit und damit die fehlende (kausale) Zurechenbarkeit von Cyber Attacken gegenüber einer bestimmten staatlichen oder privaten Entität erschwere jede glaubhafte Abschreckung und Rückschlagfähigkeit. Lösungsansätze zur Gewährleistung von Cyber Security sah Thelen neben dem technologischen Bereich (Infrastruktur, sichere Betriebsmodi, Kryptogeräte, Firewalls etc.) sowohl im politischen als auch im gesellschaftspolitischen Bereich.

Der Völkerrechtsprofessor Heintschel von Heinegg, der sich als einer der ersten mit der Problematik Cyber War befasst hat und derzeit in einem internationalen Expertengremium an einem Handbuch zu Cyber Attacken arbeitet, ergänzte das zweite Panel mit seinem Vortrag zum Thema "Cyber War - eine völkerrechtliche Standortbestimmung". Dabei versuchte er mit der Vorstellung des Cyber Space als eines metaphysischen, nachgerade unregulierbaren Raumes aufzuräumen und die Begrifflichkeiten und Elemente des Cyber War in der "nicht-virtuellen" Realität zu verorten.

Heintschel von Heinegg unterschied in diesem Zusammenhang zwischen Cyber-Attacken im technischen Sinn und dem "Angriffsbegriff" im völkerrechtlichen Sinn (z.B. in Artikel 49 des 1. Zusatzprotokolls zu den Genfer Konventionen). So müssten - um die Schwelle eines "bewaffneten Angriffs" im Sinne von Artikel 51 UN-Charta zu erreichen - die Wirkungen von IT-Viren den Wirkungen konventioneller Waffen gleichkommen, was immer auch physische Zerstörung und Gewaltanwendung voraussetze. In diesem Zusammenhang warnte v. Heinegg davor, den durch vielfältige Staatenpraxis und Gerichtsurteile ausdifferenzierten und rechtlich eingehegten "Gewaltbegriff" im Völkerrecht allein mit Blick auf die (unbestreitbar) zunehmende Verwundbarkeit hochtechnisierter Gesellschaften im IT-Sektor zu erweitern und für jegliche Formen von IT-Beeinträchtigungen (Neutralisierung bzw. "Lahmlegen" von Netzwerken, Kommunikations- oder Steuerungssystemen) zu öffnen. So sei der Stuxnet-Angriff auf das iranische Atomprogramm, auch wenn er aufgrund seiner Komplexität nur mittels staatlicher Involvierung geleistet werden konnte, kein bewaffneter Angriff im Sinne von Artikel 51 UN-Charta, der eine Selbstverteidigung mit militärischen Mitteln legitimieren würde; ebenso wenig wie die Cyber Attacken gegen Estland (2007) und Georgien (2008) mangels entsprechender Wirkungen den Bündnisfall im Sinne von Artikel 5 NATO-Vertrag ausgelöst hätten.

Freilich müssten völkerrechtswidrige Handlungen unterhalb der Schwelle eines "bewaffneten Angriffs" (sog. "measures short of war") nicht einfach hingenommen werden. So sei eine Bandbreite an proportionalen Gegenmaßnahmen unterhalb der Selbstverteidigungsschwelle gegeben, die ihre (wenn auch gewohnheitsrechtlich nur teilweise verfestigten) Schranken in den Regeln über die Staatenverantwortlichkeit fänden.

Ähnlich wie sein Vorredner problematisierte Heintschel von Heinegg die Frage der Zurechnungsfähigkeit und plädierte dafür, dass die Staaten ihre Fähigkeiten im Sinne einer "Cyber

Forensik" verbessern müssten. Es bestünde aber eine widerlegbare Vermutung, dass Cyber Attacken von Staaten herrühren oder zumindest durch diesen nicht wirksam unterbunden worden seien.

In der anschließenden Diskussion wurden vor allem die Grauzonenbereiche unterhalb der bewaffneten Angriffsschwelle weiter ausgeleuchtet, wobei die Unterschiede zwischen einer Bombe und einem Trojaner im Hinblick auf deren Wirkungen auf die Steuerungssysteme existenznotwendiger Anlagen lebhaft diskutiert wurden.

Im Anschluss an die Panels kommentierte Dr. Reinhard Müller von der Frankfurter Allgemeinen Zeitung die "Herausforderungen des High-Tech-Krieges für die deutsche Sicherheitspolitik."

Er gab zu bedenken, dass es sich beim sogannten Cyber War um einen "plakativen" Begriff ähnlich dem des "Kriegs gegen die Drogen" handeln könnte. Gleichwohl stelle die Cyber Problematik das deutsche Recht auf den Prüfstand. Müller forderte eine Initiative der Bundesregierung zur konzertierten Aktion in Sachen Cyber Security, um die besten IT-Fachleute zu rekrutieren, betrachtete die mangelnde Kooperation zwischen Staat und IT-Privatwirtschaft, und er warf die Frage nach der (fehlenden) Vorbereitung auf einen möglichen totalen Zusammenbruch der Infrastruktur nach einer Cyber-Attacke auf.

Die interdisziplinäre Fachtagung über die "Automatisierung und Digitalisierung des Krieges" habe - wie der Präsident der Bundesakademie für Sicherheitspolitik in seinem Fazit hervorhob - geradezu visionäre Zukunftsthemen aufgegriffen, die tiefgreifende Fragen an die Vorstellung vom Krieg und an das Verhältnis von Mensch und Maschine stellten. Die Ergebnisse der Tagung hätten einmal mehr gezeigt, wie wichtig die Verständigung über die gemeinsamen Begrifflichkeiten (wie der "Angriff" im technischen und rechtlichen Sinne) geworden ist. Es sei deutlich geworden, dass erst die Anwendung von Technik und nicht die Technik selbst eine sicherheitspolitische Relevanz entfalte. Der Mensch bleibe daher bis auf weiteres der unverzichtbare Entscheidungsträger in automatisierten und digitalisierten Einsatzabläufen. Cyber Security sei gerade ein Paradebeispiel für vernetzte Sicherheit im Sinne einer gesamtstaatlichen Herausforderung, bei der die Grenzen zwischen innerer und äußerer Sicherheit längst überschritten seien. Für die Praxis gehe es heute darum, den Prozess zunehmender Automatisierung und Digitalisierung der Kriegsführung rechtlich einzuhegen und im Sinne ethischer Postulate und sicherheitspolitischer Interessen zu gestalten.