Cyberwarfare und Kampfdrohnen

Die Bundeswehr auf neuen Wegen

Stefan Schumacher

www.sicherheitsforschung-magdeburg.de

3. Sicherheitspolitisches Tagesseminar Gießen
01.06.2013



Über Mich

- Direktor des Magdeburger Instituts für Sicherheitsforschung
- Geek, Nerd, Hacker seit knapp 20 Jahren
- W23 JgBtl 371 KRK - Marienberger Jäger
- B.A. Bildungswissenschaft und Psychologie, derzeit IVE
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`



Informationstechnologie und Sicherheitspolitik

Sambleben, J. und Schumacher, S. (Herausgeber)



http://www.sicherheitsforschung-magdeburg.de/buecher.html

1 Einführung

2 Drohnen
- Drohnen der Bundeswehr
- Drohnen anderer Streitkräfte

3 Network-Centric Warfare/NetOpFü

4 Sicherheit

5 Moral und Psychologie



Inhaltsverzeichnis

1 Einführung

2 Drohnen

3 Network-Centric Warfare/NetOpFü

4 Sicherheit

5 Moral und Psychologie



Drohnen

- allgemein: ein unbemanntes autonomes oder ferngesteuertes Fahrzeug
- Flugzeug, Landfahrzeug, Schiff, Unterwasservehikel
- Hier: Unbemanntes Luftfahrzeug / Unmanned Aerial Vehicle (UAV)
- riesiges Themengebiet



Klassifizierung

- auf strategischer oder taktischer Ebene
- Gefechtsfeldaufklärung und -überwachung
- Sensoren: optisch (Foto/Film, Infrarot), Radar, SIGINT
- Steuerung: autonom (GPS) oder per Luftfahrzeugführer
- Kampfeinsätze mit verschiedenen Wirkmitteln bspw. Hellfire, JDAMs
- Hauptsächlich taktische Erdkampfunterstützung/Luftnahunterstützung
- Flugdauer, Flughöhe, Größe, Datenübertragung



Inhaltsverzeichnis

1 Einführung

2 Drohnen

3 Network-Centric Warfare/NetOpFü

4 Sicherheit

5 Moral und Psychologie



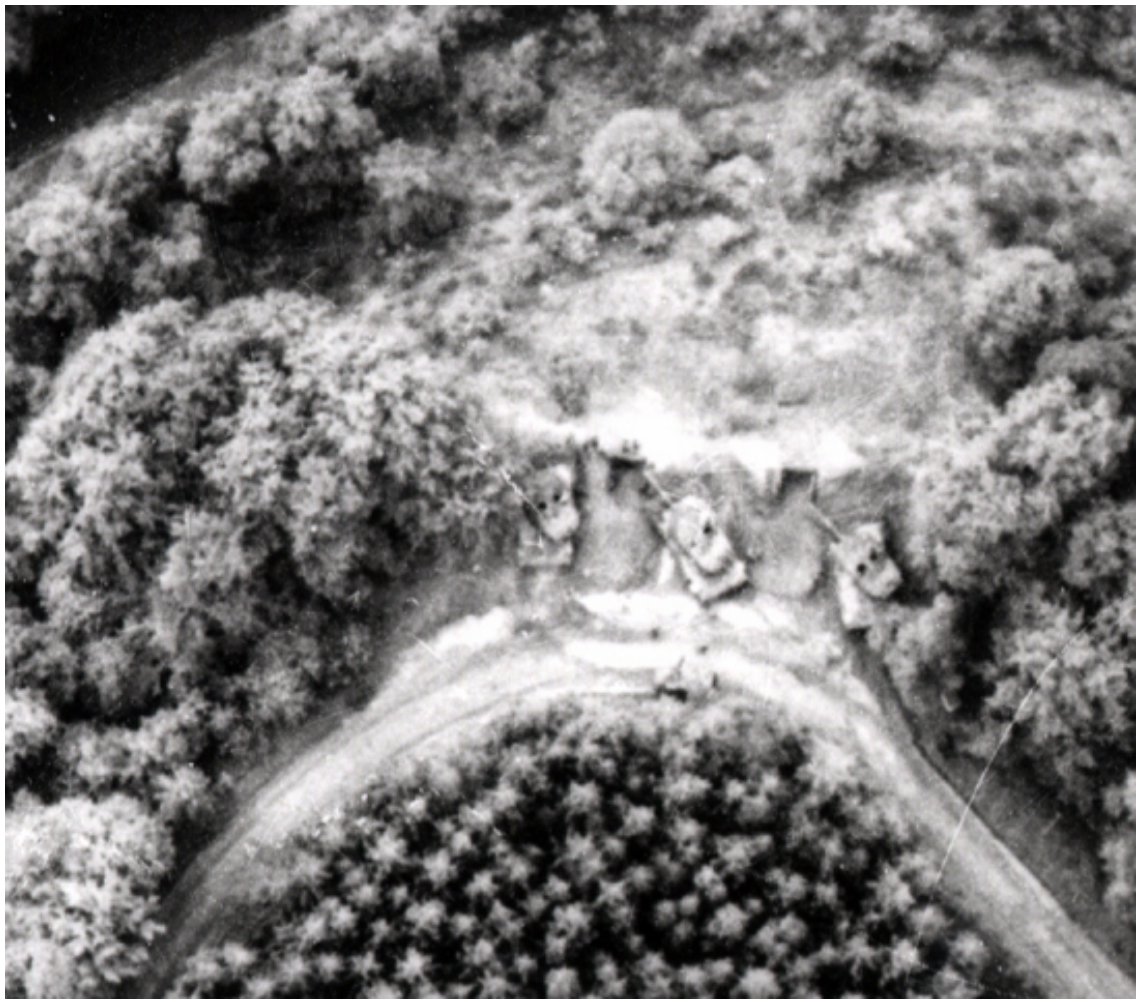
Canadair CL-289

- Systemdefiniton: 1972; Indienststellung 1990; Einführung Bw: 1991
- Bw eine der ersten Streitkräfte weltweit mit Drohnenkapazität
- Drohnenlehrbatterie 300 zum 01.01.1979 aufgestellt
- 740 km/h, 30 Minuten/400km, Eindringtiefe 170km, Länge 3,7m, Spannweite 1,3m, Leergewicht 130kg, Optische Kamera, IR Liner, Funkübertragung bis 70km, Steuerung per GPS
- 18 Drohnen, 376 Aufklärungsflüge S/I/KFOR, 5 Verluste
- letzter Flug 18.03.2009

Canadair CL-289



Canadair CL-289



Quelle: www.dlb300.de

LUNA: Luftgestützte Unbemannte Nahaufklärungs-Ausstattung

- März 2000: Einsatz im Kosovo, 2003 Indienststellung
- Spannweite: 4,17 m, 40kg, 70 km/h, 8h Flugdauer, 100km Datalink
- 4 Farbvideokameras
- optional: Nahinfrafrot- und Wärmebildkamera



LUNA: Luftgestützte Unbemannte Nahaufklärungs-Ausstattung



LUNA: Luftgestützte Unbemannte Nahaufklärungs-Ausstattung



EMT Aladin: abbildende luftgestützte Aufklärungsdrohne im Nächstbereich

- Übergabe: Oktober 2005 an PzTrpSchule Munster
- 3,2kg; 1,5m Spannweite; 30 Minuten; 5 km Reichweite
- Aufklärung im Umkreis von 65km
- Programmierung der Route vor dem Start, Duplex-Mikrowellenverbindung zur Kurskorrektur, Downlink für Daten



EMT Aladin



KZO - Kleinfluggerät Zielortung

- Erstflug 1998, Indienststellung 2005
- Artillerie und Heeresaufklärer
- amtlich zugelassenes unbemanntes Luftfahrzeug
- Spannweite 3,42 m; 168 kg; 120-216km/h; 33PS Propeller
- Einsatzdauer 3,5 - 6h; 100km ohne Störer/65km mit
- Störerschutz durch Frequency Hopping Spread Spectrum und Direct Sequence Spread Spectrum



KZO - Kleinfluggerät Zielortung



IAI Heron

- Anfang 2010 Leasing von 3 Heron 1 für Bw AG 51 »Immelmann«
- Middle Altitude, Long Endurance
- 16,6 m Spannweite; 1.150 kg; 24 h Flugzeit; 111 - 213km/h
- autonomer Flug über GPS, vollautomatische Starts und Landungen
- Luftfahrzeugführer kann 400 km entfernt sein
- Datenlink über Funk (Sicht) oder Satellit
- Luftfahrzeugführer muss ständig in Kontakt mit Flugsicherung stehen
- direkte Unterstützung der Bodentruppem mit Live-Bildern
- Keine Überschneidung zum RECCE-Tornado



IAI Heron



Weitere Systeme

- Tauchroboter (gesteuert oder autonom)
- AEGIS auf Schiffen
- autonome Autos (Google Challenge)
- Roboter z.B. Kampfmittelbeseitigung, Aufklärung im MOUT



Northrop Grumman RQ-4E Euro Hawk

- Spannweite: 35,42 m; Leergewicht 5t; 36 Stunden, ca. 5500km Radius/24h; Dienstgipfelhöhe 19.811 m
- Aufgabe: SIGINT
- Geplanter Ersatz für BR 1150 M



Northrop Grumman RQ-4E Euro Hawk



General Atomics MQ-9 Reaper

- Indienststellung 2007; Spannweite 20,12 m; Leergewicht 2223 kg; Marschgeschwindigkeit 276km/h bzw. 313km/h; Einsatzradius 3065 km, Flugdauer 30h
- Bis zu 1361 kg Waffenlast
- SAM AGM Hellfire (Panzerabwehrrakete); JDAM (Lasergelenkte Bomben)
- u.a. in Pakistan für Targeted Killing eingesetzt



General Atomics MQ-9 Reaper



Machatz 1

- israelische Heron-Variante
- Daten liegen nicht offen, Bewaffnung existiert vermutlich
- Operation Gegossenes Blei: Machatz-1, Elbit Hermes 450, AH-64 Apache und Kampfflugzeuge im Verbund dem Heereskommando unterstellt
- Ziel: besseres Lagebild und schnellere Luftschläge



Honeywell RQ-16 T-Hawk

- 8,4 kg; 40 Minuten Flugdauer
- u.a. im Irak zur Suche nach Sprengfallen eingesetzt
- eine Drohne in Fukushima zur Aufklärung eingesetzt



Honeywell RQ-16 T-Hawk



Inhaltsverzeichnis

1 Einführung

2 Drohnen

3 Network-Centric Warfare/NetOpFü

4 Sicherheit

5 Moral und Psychologie



Gefecht der verbundenen Waffen

Entstehung

- Gefecht der verbundenen Waffen
- Führung von Vorn $\rightsquigarrow$ Führungsmittel
  (Rommel vor Tobruk)
- seit 2007 Operation verbundener Kräfte
  Erweiterter Sicherheitsbegriff
- Zusammenwirken mechanisierter Truppengattung zur Steigerung des Gefechtswertes
- Erste HDV im 1. Weltkrieg, von Guderian weiterentwickelt
- Koordination von Feuer und Bewegung der eigenen Kräfte
- Informations- und Feuerüberlegenheit sowie Bewegungsfähigkeit erzwingen und erhöhen

Gefecht der verbundenen Waffen

Entstehung

- neue technische Möglichkeiten im IT-Bereich
- ideal: Aufklärungssysteme speisen Daten direkt in Waffensysteme ein
- Bsp: VB (JFST) oder KZO funkt GPS-Koordinaten an PzH2000



Gefecht der verbundenen Waffen

Entstehung



Gefecht der verbundenen Waffen

Bestandteile

- Feuer
- Bewegung
- Sperren
- Elektronischer Kampf
- Kräfte
- Raum
- Zeit
- Information



Network Centric Warfare

- 1970/80er Jahre: EDV verbreitet sich in Unternehmen
- Wirtschaftsinformatik, Managementsysteme, Data Warehousing, ERP, Expertensysteme, Entscheidungsunterstützungssysteme
- US Militär adaptiert Ideen aus der Wirtschaftsinformatik
- Paper: Joint Vision 2010 und Joint Vision 2020
- Aufbau des Global Information Grid:
  Jedem Soldaten und jeder Kampfeinheit soll an jedem Ort, zu jeder Zeit, unter allen Wetterbedingungen jede relevante Information zur Verfügung stehen.
- DoD Architecture Framework: C^4ISTAR Command, Control, Computers, Communications, Information, Intelligence, Surveillance, Target Acquisition, Reconnaissance



Network Centric Warfare

Kerngedanken

1. Erfassung von Daten über Sensoren
2. Sammlung der Daten in Datenbanken
3. Algorithmisierte Aufbereitung der Daten (Statistik, Stochastik etc.)
4. Identifizierung von Probleme
5. Automatisierte Lösung von Problemen
6. Propagierung der Lösung im System
7. Ausführung



Systemanalyse und Programmentwicklung?



Network Centric Warfare

Definition

- Self-synchronization, or doing what needs to be done without traditional orders;
- Improved understanding of higher command's intent;
- Improved understanding of the operational situation at all levels of command
- Increased ability to tap into the collective knowledge of all U.S. (and coalition) forces to reduce the »fog and friction« commonly referred to in descriptions of fighting.



Network Centric Warfare

Vision

- Jedes System wird mit Sensoren, Up- und Downlink ausgerüstet (FWC/IdZ)
- erfasste Daten werden aufbereitet und in Datenbank eingespeist
- stehen dort der OpFü zur Verfügung
- Daten werden automatisch aufbereitet
- Zielkoordinaten etc. weitergeleitet
- Jedes System kann in sekundenschnelle mit neuen Befehlen versorgt werden



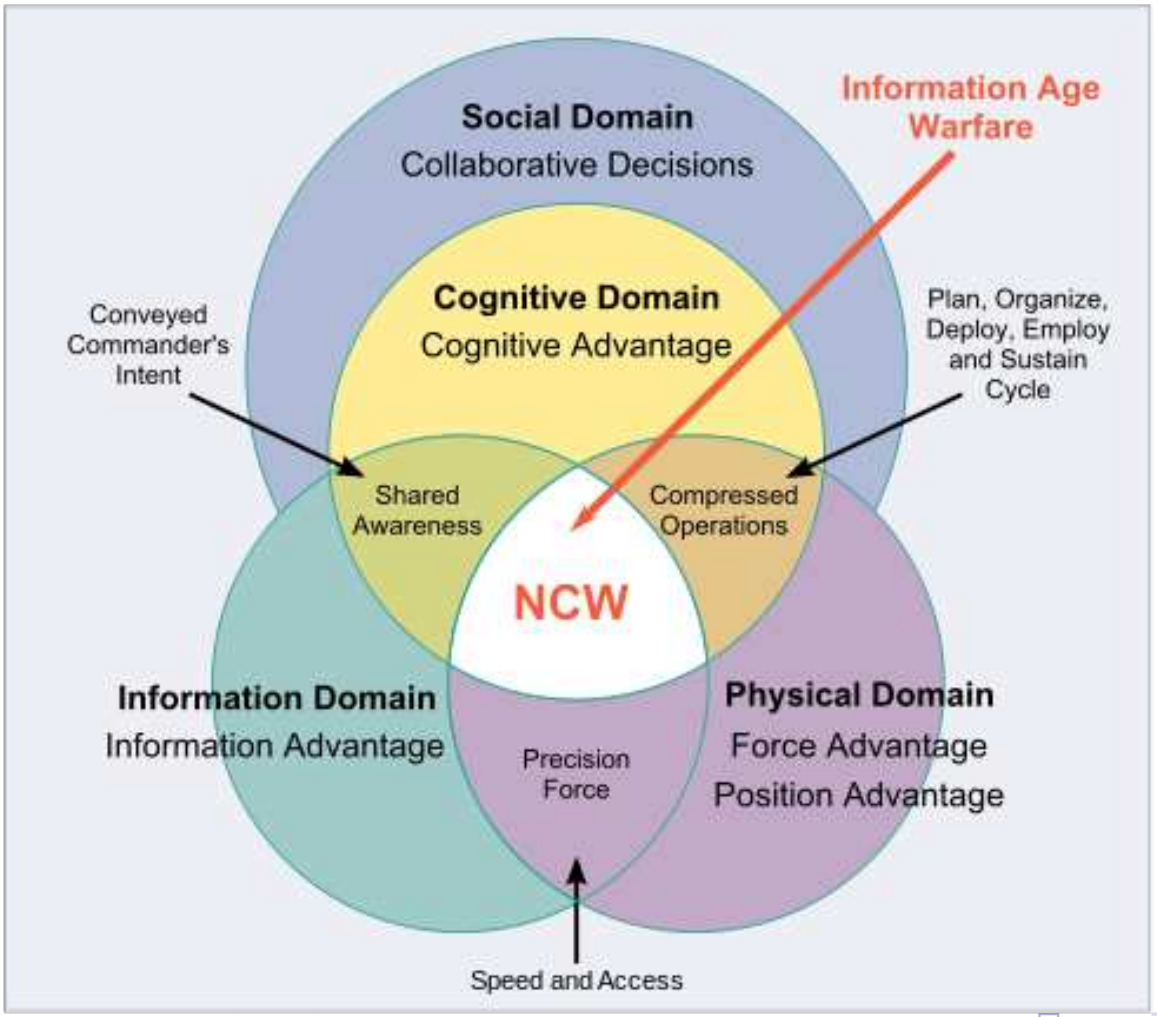
Network Centric Warfare

Probleme?

- Abhängigkeit von der IT (später mehr)
- Was bei Ausfall der IT?
- Können Menschen die Aufgaben noch bewältigen? (Kognitive Last/Theorie der Nebenaufgabe etc.)
- Ertrinken in Datenflut? Wer filtert was wie wohin?
- Will ich das ein StOffz dem OGefr im Häuserkampf aufs HUD quatscht?
- Führen mit Auftrag vs. Führen mit Befehl?



Domänen der NCW



Inhaltsverzeichnis

1 Einführung

2 Drohnen

3 Network-Centric Warfare/NetOpFü

4 Sicherheit

5 Moral und Psychologie



1996 Ariane 5 501



1996 Ariane 5 501

- gesprengt nach 36,7 Sekunden
- Software von Ariane 4 auf Ariane 5 portiert
- 64 Bit Float in 16 Bit signed Int
- Beschleunigung der Ariane 5 ist signifikant höher $\rightsquigarrow$ Overflow
- Test-Simulation vor dem Flug fand das Problem nicht, Nicht-Schutz der Variablen war nicht dokumentiert
- 320 000 000,– Euro teures Feuerwerk



Lockheed Martin RQ-170 Sentinel

Beast of Kandahar



Lockheed Martin RQ-170 Sentinel

Beast of Kandahar

- navigiert selbständig $\rightsquigarrow$ benötigt NAVSTAR GPS oder Trägheitsnavigation
- GPS ist genau aber angreifbar
- Trägheitsnavigation ist problematisch und ungenau über längere Zeiträume (Kopplung)
- Iran behauptet Hack bzw. GPS Jam, USA bestreiten den Einsatz von GPS

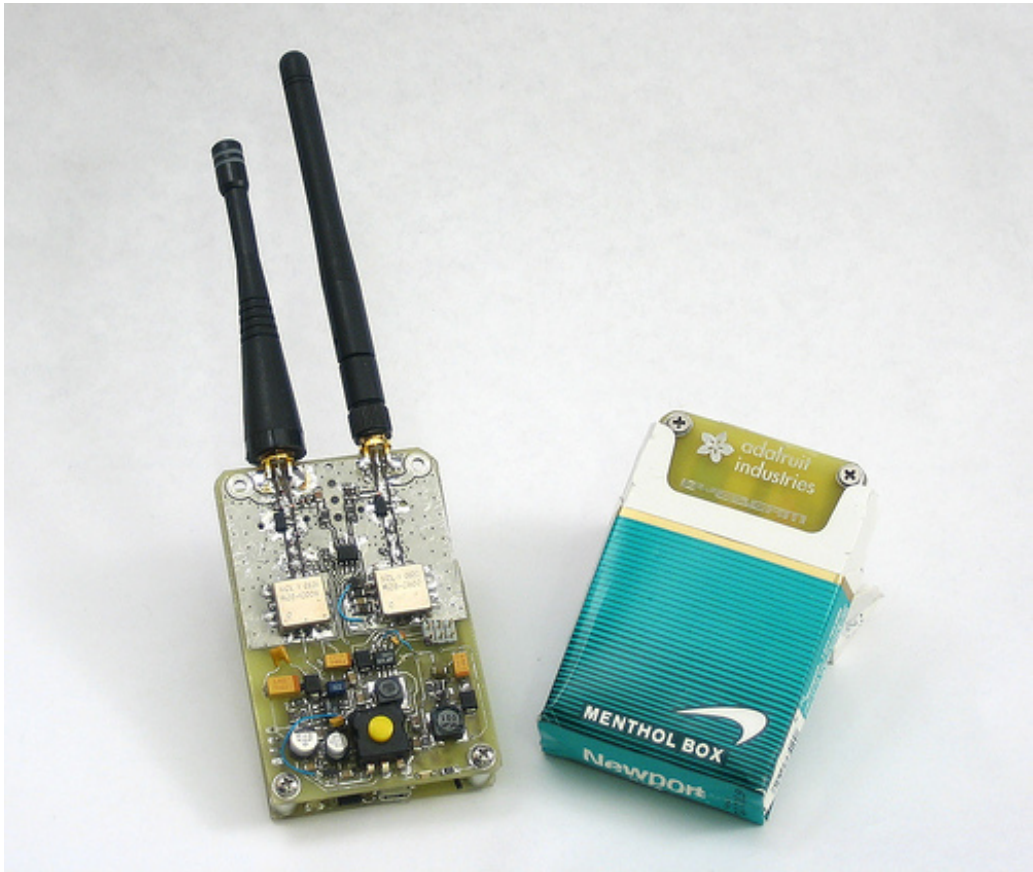


Navigational Satellite Timing and Ranging - Global Positioning System

- min. 24 Satelliten in 20 200 km mittlerer Bahnhöhe
- Positionsbestimmung über Triangulation gegenüber den Satelliten
- öffentliches Signal und verschlüsseltes militärisches Signal mit erhöhter Präzision
- Signalstärke -155 dBW $\rightsquigarrow$ leicht zu jammen
- Richtfunkantenne zum Satelliten
- `http://www.phrack.org/issues.html?issue=60&id=13#article`
- China fälscht/jammed systematisch GPS



WaveBubble - Jammer für Funksignale



0,3 - 1 Watt Sendeleistung, 4h Batteriebetrieb, Bauanleitung im Internet

Cyber-Security betrifft nicht nur Flugzeuge

- Steuerungssysteme können attackiert werden (GPS, Fernsteuerung)
- Funksignale können mitgehört und manipuliert werden $\rightsquigarrow$ Integritätssicherung notwendig (Kryptographie ist komplex)
- 2009: Taliban fangen Videostream mit SkyGrabber ab
- Backdoor im Silizium des FPGA-Chip Actel/Microsemi ProASIC3, u.a. in der Boeing 787 eingesetzt
- französische Mirages im Irak-Krieg 2003 am Boden geblieben
- sowjetische MiG hat südafrikanisches Freund-Feind-Erkennungssystem per Man in the Middle ausgeschaltet



Cyber-Security betrifft nicht nur Flugzeuge

- Fehler in Design-/Simulationssoftware?
- manipulierte Software-Bibliotheken
- Stuxnet hat auf Industriesteuerungen abgezielt (SIMATIC, Frequenzumrichter ...)



Enigma

FM Eloka ist nichts neues ...



Klassisches Old-School-Hacking

- NASA-Hack 1986/87: u.a. franz. Rüstungskonzern Thomson (heute Thales) gehackt
- September 1991: Julian Assange hacked Master-Terminal Nortel Australien
- »Chinesische« Hacker sollen Tech-Konzern Nortel ausgeplündert haben (SpOn)
- Hacker hatten von 2000 an Manager-Passwörter und damit vollen Zugriff
- Nortel wird gegenwärtig liquidiert
- Wie sicher sind Entwicklungsbüros?
- Daten abschnorcheln ist das eine aber Daten ändern? (Integritätsprüfung)



Klassisches Old-School-Hacking

- NASA-Hack 1986/87: u.a. franz. Rüstungskonzern Thomson (heute Thales) gehackt
- September 1991: Julian Assange hacked Master-Terminal Nortel Australien
- »Chinesische« Hacker sollen Tech-Konzern Nortel ausgeplündert haben (SpOn)
- Hacker hatten von 2000 an Manager-Passwörter und damit vollen Zugriff
- Nortel wird gegenwärtig liquidiert
- Wie sicher sind Entwicklungsbüros?
- Daten abschnorcheln ist das eine aber Daten ändern? (Integritätsprüfung)



Inhaltsverzeichnis

1 Einführung

2 Drohnen

3 Network-Centric Warfare/NetOpFü

4 Sicherheit

5 Moral und Psychologie



Moral?

Turing-Maschine

Sei $M = (Q, \Sigma, \Gamma, \delta, q_0, \square, q_f)$ ein formales 7-Tupel mit:

1. Q := endliche Zustandsmenge
2. Σ := Eingabealphabet
3. Γ := endliches Bandalphabet mit $\Sigma \subset \Gamma$
4. $\delta : (Q \setminus \{q_f\}) \times \Gamma \mapsto Q \times \Gamma \times \{L, 0, R\}$:= partielle Überführungsfunktion
5. $q_0 \in Q$:= Anfangszustand
6. $\square \in \Gamma \setminus \Sigma$:= leeres Feld
7. $q_f \in Q$:= akzeptierende Zustand



Moral?

- Computer sind Turing-Maschinen
- Turing-Maschinen führen Algorithmen aus
- Computer können keine Entscheidungen treffen!
- Berechnungsrahmen muss programmiert werden.
- Menschen müssen Entscheidungen treffen oder die Entscheidungen vorher einprogrammieren



Moral - ZMZ?

- militärische Entwicklung treibt zivile Nutzung voran
- Preise sinken, technische Innovationen geschehen
- Nutzung von Drohnen in Krisenszenarien - Aufklärung, Kommunikation
- Mähdrescher die vollautomatisch Felder mähen und per Drohne vor Tieren warnen
- Einsatz in der inneren Sicherheit?



Psychische Faktoren

- kognitive Last bei der Steuerung von Drohnen
- entspricht in der Komplexität her Kampfpiloten
- kürzere, billigere Ausbildung, kaum körperliche Anforderungen
- Ausbildung komplett im Simulator möglich
- fehlende Sensumotorik zur Lage im Raum?



Psychische Faktoren

- Luftfahrzeugführer kann irgendwo auf der Welt sitzen (Satelliten)
- 9-to-5-Job $\rightsquigarrow$ tägliches Framing!
- PTBS/Krise/Traumatisierung ebenso möglich
- Enthemmung/Amok ebenso möglich
- leichteres Töten nicht zwingend wahrscheinlich
- mehrere Faktoren u.a. Persönlichkeitseigenschaften, Betreuung, Ausbildung
- siehe »Killerspiele und Gewalt«



Fazit

- Drohnen eröffnen neue taktische und strategische Fähigkeiten
- Einbettung in ein Gesamtkonzept erforderlich (NCW/NetOpFü)
- Komplexität steigt drastisch
- Ausbildungshöhe der Soldaten steigt (IdZ)
- Angreifbarkeit und Fehleranfälligkeit steigt
- Cyber-Attacken möglich



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- youtube.de/Sicherheitsforschung

