Technische Neuerungen und rechtliche Probleme

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

21.04.2016



über mich



Über Mich

- Bildungswissenschaft/Psychologie
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Geek, Nerd, Hacker seit knapp 20 Jahren
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`



Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
- Lehrerfortbildung
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe
- IT-Sicherheit in KMU
  - empirische Grundlagenforschung
  - didaktische Aufbereitung
  - Schulungen



Schulungs- und Beratungsangebote

- Sicher unterwegs im Internet
- Anonymität und Überwachung im Internet
- Security Awareness Kampagnen konzipieren
- Netzwerke absichern/Penetration Testing
- Die psychologischen Grundlagen des Social Engineerings
- Der digitale Untergrund: zur aktuellen Bedrohungslage im Internet
- Kryptographie - Konzepte, Methoden und Anwendungen
- Strategien im Wirtschaftskrieg
- Selbstschutz in Krisengebieten



Informationstechnologie und Sicherheitspolitik

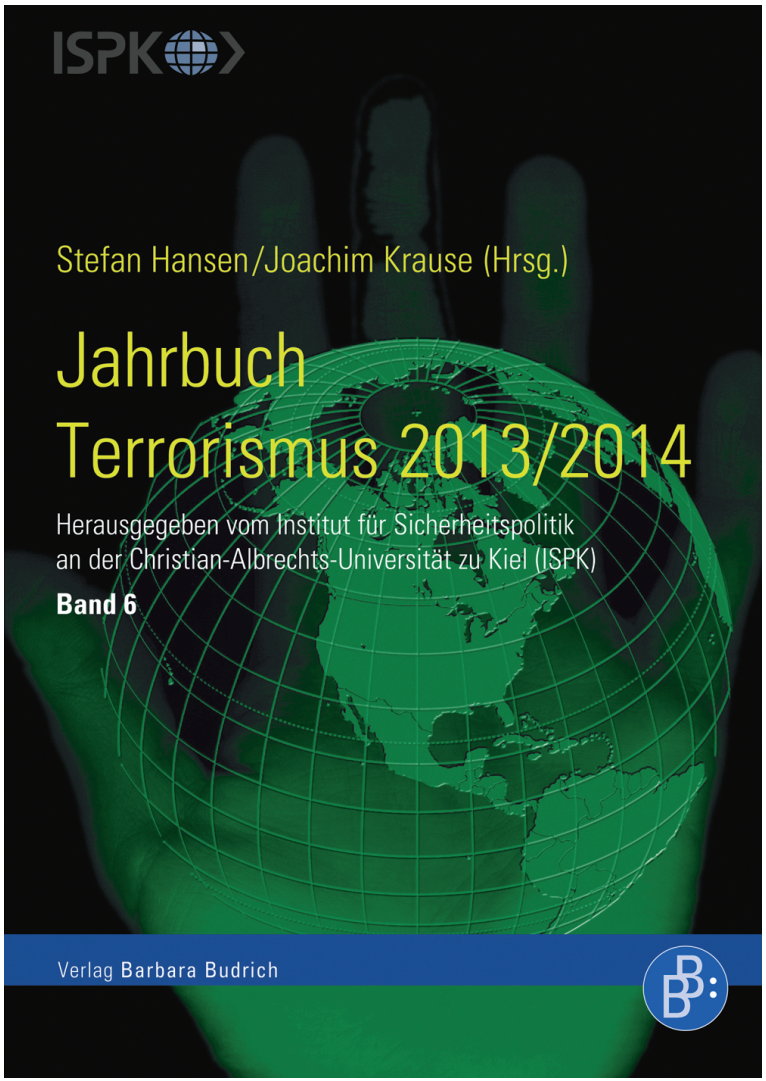
Sambleben, J. und Schumacher, S. (Herausgeber)



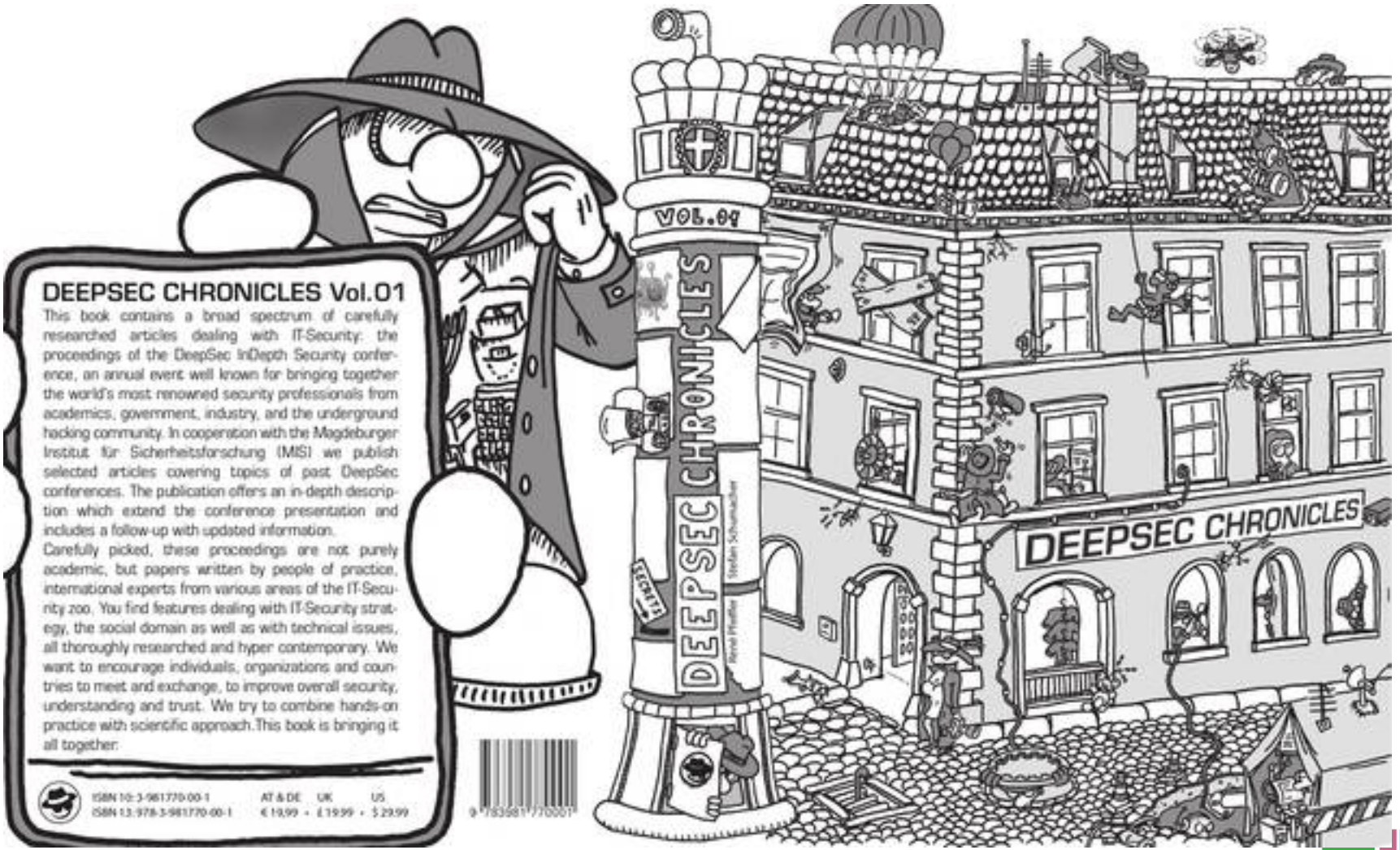
sicherheitsforschung-magdeburg.de/buecher.html

Jahrbuch Terrorismus 2013/2014

Hansen, S. und Krause, J. (Herausgeber, Institut für Sicherheitspolitik Kiel)



Stefan Schumacher:
Cyber-Terrorismus:
Reale Bedrohung oder Mythos?
S. 159 – 180


DEEPSEC CHRONICLES Vol.01
This book contains a broad spectrum of carefully researched articles dealing with IT-Security: the proceedings of the DeepSec InDepth Security conference, an annual event well known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. In cooperation with the Magdeburger Institut für Sicherheitsforschung (MIS) we publish selected articles covering topics of past DeepSec conferences. The publication offers an in-depth description which extend the conference presentation and includes a follow-up with updated information.
Carefully picked, these proceedings are not purely academic, but papers written by people of practice, international experts from various areas of the IT-Security zoo. You find features dealing with IT-Security strategy, the social domain as well as with technical issues, all thoroughly researched and hyper contemporary. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security, understanding and trust. We try to combine hands-on practice with scientific approach. This book is bringing it all together.
ISBN 10: 3-981770-00-1
ISBN 13: 978-3-981770-00-1
AT & DE UK US
€ 19,99 £ 19,99 $ 29,99
Vol.01
DEEPSEC CHRONICLES
DEEPSEC CHRONICLES

- Stefan Schumacher and René Pfeiffer (editors)
- In Depth Security – Proceedings of the DeepSec Conference
- 360 Pages
- Magdeburger Institut für Sicherheitsforschung
- 978-3981770001
- `http://www.amazon.de/Depth-Security-Stefan-Schumacher/dp/3981770005/ref=sr_1_1?ie=UTF8&qid=1448888706`



Inhaltsverzeichnis

1. Einführung
2. AEGIS
3. Drohnen
4. Maritimer Einsatz: AEGIS
5. Network-Centric Warfare/NetOpFü
6. Sicherheit
7. Moral und Psychologie
8. Robotik und Zukunft



Inhaltsverzeichnis

1 Einführung

2 AEGIS

3 Drohnen

4 Maritimer Einsatz: AEGIS

5 Network-Centric Warfare/NetOpFü

6 Sicherheit

7 Moral und Psychologie

8 Robotik und Zukunft



Maritimer Einsatz

- Marine bietet sich zur Erprobung von Technik an
- Platz vorhanden
- erste GPS-Empfänger in Container-Größe
- Miniaturisierung ermöglicht weitere Einsatzszenarien
- Automatisierung im Schiff



HMS Sheffield (D80)



versenkt durch Super Etendards mit Exocet im Falklandkrieg
Rolle der Sheffield: Flugabwehr

Exocet

- Argentinier versenken HMS Sheffield und Frachter Atlantic Conveyor
- Alle von franz. Super Etendard Flugzeugen abgefeuert
- Exocet: Fire and Forget Sea Skimmer, aktiviert Radar erst nach ca. 80% der Strecke
- Britische Marine hatte eklatante Mängel in der Luftabwehr insbesondere im Nahbereich
- 17. Mai 1987: USS Stark (FFG-31) von 2 Exocets einer irakischen Mirage schwer beschädigt



AEGIS

- Aegis oder Aigis: Schild aus Ziegenfell des Zeus, welches Donner und Blitze aussendet
- Airborne Early Warning Ground Environment Integration Segment
- Informations- und Feuerleitsystem
- Antwort auf Flugkörpersättigungsangriffe des Warschauer Vertrages
- massierter Angriff mit Flugkörpern von Schiffen und Hubschraubern aus
- Überlastung der Abwehr des Zieles
- Bessere Koordination erforderlich



AEGIS

- Sensoren, Datenbanken und Feuerleitsystemen
- 4 phasengesteuerte Radargeräte (AN/SPY1)
- passiv phasengesteuertes System mit elektronischer Strahlschwenkung und agilem Strahl
- keine beweglichen Teile
- schneller Wechsel (μs) zwischen anfliegenden Zielen möglich
- Verfolgung und Bekämpfung tausender Ziele gleichzeitig möglich
- Echtzeit-Vernetzung via Link 11 oder Link 16
- Zeit zwischen 1. Ortung und Start der Abfangrakete unter 15s



AEGIS

- vollautomatische Verteidigung oder Generierung von Lagebildern möglich
- Vernetzung mit anderen Schiffen möglich und sinnvoll
- eingesetzt auf Kreuzern der Ticonderoga-Klasse, Zerstörern der Arleigh-Burke-Klasse
- Fernsteuerung technisch machbar
- bspw. in einer Flugzeugträgerkampfgruppe
- im Konzept der Network Centric Warfare



Carrier Strike Group

- 1 Flugzeugträger der Nimitz-Klasse mit je einem Carrier Air Wing
- 2 Lenkwaffenkreuzern der Ticonderoga-Klasse
- 2-3 Lenkwaffenzerstörern der Arleigh-Burke-Klasse: Luft- und U-Bootabwehr zuständig sind
- 2 Jagd-U-Boote der Los-Angeles-, Seawolf- oder Virginia-Klasse: U-Boot- und Ü-Bootabwehr
- Trossschiffe



Freund-Feind-Erkennung

- Iran-Air-Flug 655 Teheran - Dubai
- 03.07.1988: von USS Vincennes abgeschossen
- automatische Anfrange der USS Vincennes identifiziert den Airbus als zivil
- Aegis identifiziert die Airbus als F-14 Tomcat
- Aegis meldet den Airbus im Sinkflug und auf Abfangkurs
- Airbus befindet sich die ganze Zeit über im Steigflug
- Kapitän Rogers schießt 2 SM2 SAM ab
- 290 tote Zivilisten



Freund-Feind-Erkennung

- Aegis arbeitete fehlerhaft
- falsche nachrichtendienstliche Informationen
- fehlerhafte Entscheidungsfindung in der OpZ
- Disziplinare Würdigung?



Freund-Feind-Erkennung

- Aegis arbeitete fehlerhaft
- falsche nachrichtendienstliche Informationen
- fehlerhafte Entscheidungsfindung in der OpZ
- Disziplinare Würdigung?



Freund-Feind-Erkennung

- Aegis arbeitete fehlerhaft
- falsche nachrichtendienstliche Informationen
- fehlerhafte Entscheidungsfindung in der OpZ
- Disziplinare Würdigung?
- George H. W. Bush zeichnet Kapitän Rogers mit dem Legion-of-Merit-Orden „für außerordentliche Pflichterfüllung im Einsatz“ aus
- befördert alle anderen am Abschuss beteiligten Offiziere



Freund-Feind-Erkennung

- Aegis arbeitete fehlerhaft
- falsche nachrichtendienstliche Informationen
- fehlerhafte Entscheidungsfindung in der OpZ
- Disziplinare Würdigung?
- George H. W. Bush zeichnet Kapitän Rogers mit dem Legion-of-Merit-Orden „für außerordentliche Pflichterfüllung im Einsatz“ aus
- befördert alle anderen am Abschuss beteiligten Offiziere



Inhaltsverzeichnis

1 Einführung

2 AEGIS

3 Drohnen

4 Maritimer Einsatz: AEGIS

5 Network-Centric Warfare/NetOpFü

6 Sicherheit

7 Moral und Psychologie

8 Robotik und Zukunft



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



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



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 AEGIS

3 Drohnen

4 Maritimer Einsatz: AEGIS

5 Network-Centric Warfare/NetOpFü

6 Sicherheit

7 Moral und Psychologie

8 Robotik und Zukunft



Maritimer Einsatz

- Marine bietet sich zur Erprobung an
- Platz vorhanden
- erste GPS-Empfänger in Container-Größe
- Miniaturisierung ermöglicht weitere Einsatzszenarien
- Automatisierung im Schiff



Inhaltsverzeichnis

1 Einführung

2 AEGIS

3 Drohnen

4 Maritimer Einsatz: AEGIS

5 Network-Centric Warfare/NetOpFü

6 Sicherheit

7 Moral und Psychologie

8 Robotik und Zukunft



Geschichte

- Feldherrenhügel, Trommler und Pfeifer
- mongolische Meldereiter
- Signalfeuer, Telegraphenmasten, Telegraphenleitungen
- getrennt marschieren - vereint schlagen
- Fernmelder, Elektronische Kampfführung im WK1
- Enigma im WK2
- Funker auf jedem deutschen Panzer $\rightsquigarrow$ taktische Überlegenheit
- Konzept der verbundenen Waffen
- Kybernetik in der UdSSR und USA diskutiert $\rightsquigarrow$ Regelkreis



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



Gefecht der verbundenen Waffen

Bestandteile

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

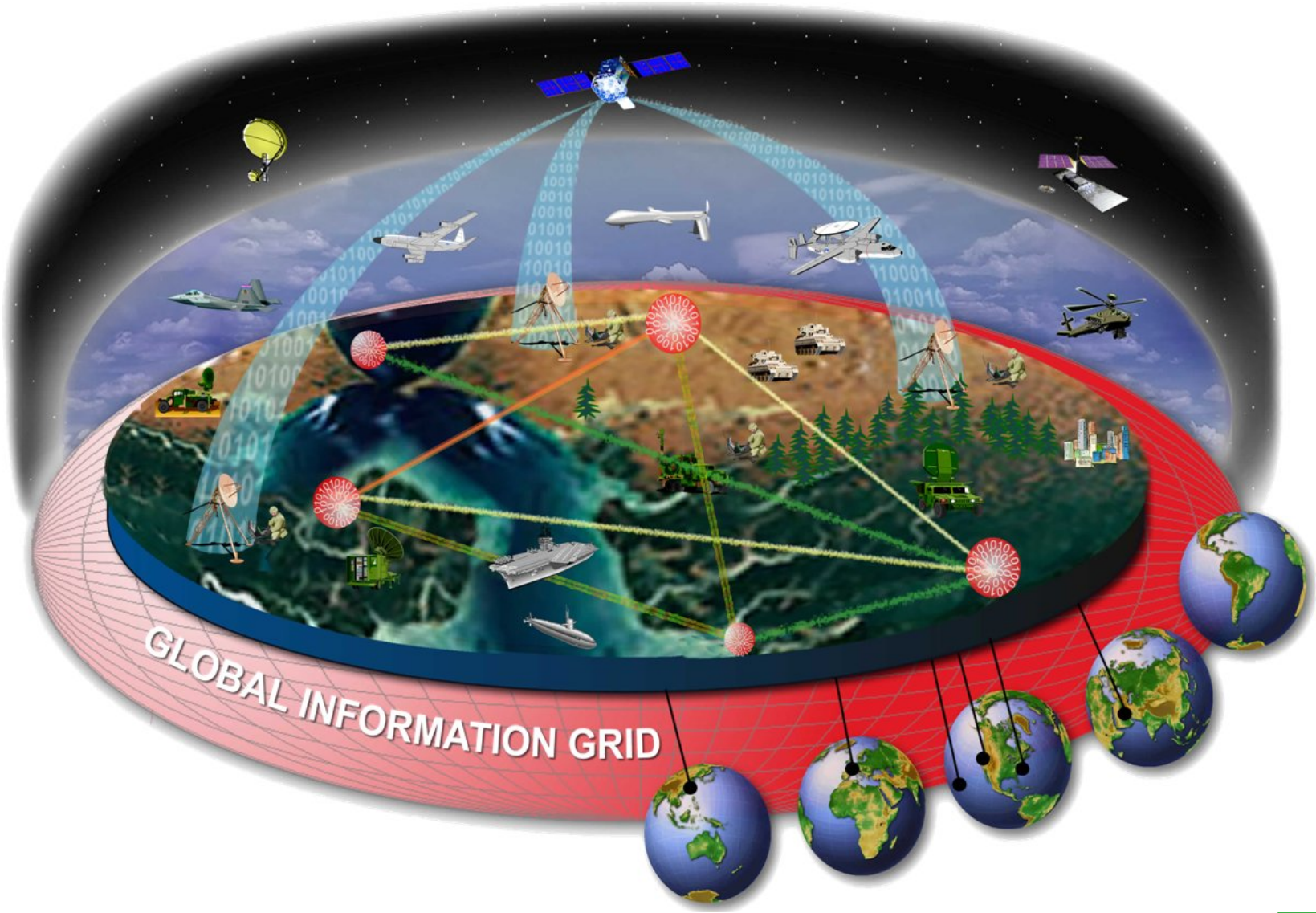


Network Centric Warfare

- 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



Global Information Grid



Network Centric Warfare

Kerngedanken

- Erfassung von Daten über Sensoren
- Sammlung der Daten in Datenbanken
- Algorithmisierte Aufbereitung der Daten (Statistik, Stochastik etc.)
- Identifizierung von Probleme
- Automatisierte Lösung von Problemen
- Propagierung der Lösung im System
- Ausführung



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



Idee

- Geheimdienst klärt Zielperson per SIGINT auf (Satellitentelefon)
- Fernspäher klären Ziel hinter den feindlichen Linien auf
- senden Koordinaten an OpZ
- Zerstörer bekämpft Ziel mit BGM-109 Tomahawk
- Luftwaffe schickt Überwachungsdrohne ins Zielgebiet
- die Zielpersonen selbständig verfolgt und bekämpft
- Fallschirmjäger verfolgen Zielperson, bekommen Informationen der Drohne in Echtzeit auf HUD



Network Centric Warfare

Probleme?

- Abhängigkeit von der IT
- 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?



Inhaltsverzeichnis

1 Einführung

2 AEGIS

3 Drohnen

4 Maritimer Einsatz: AEGIS

5 Network-Centric Warfare/NetOpFü

6 Sicherheit

7 Moral und Psychologie

8 Robotik und Zukunft



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

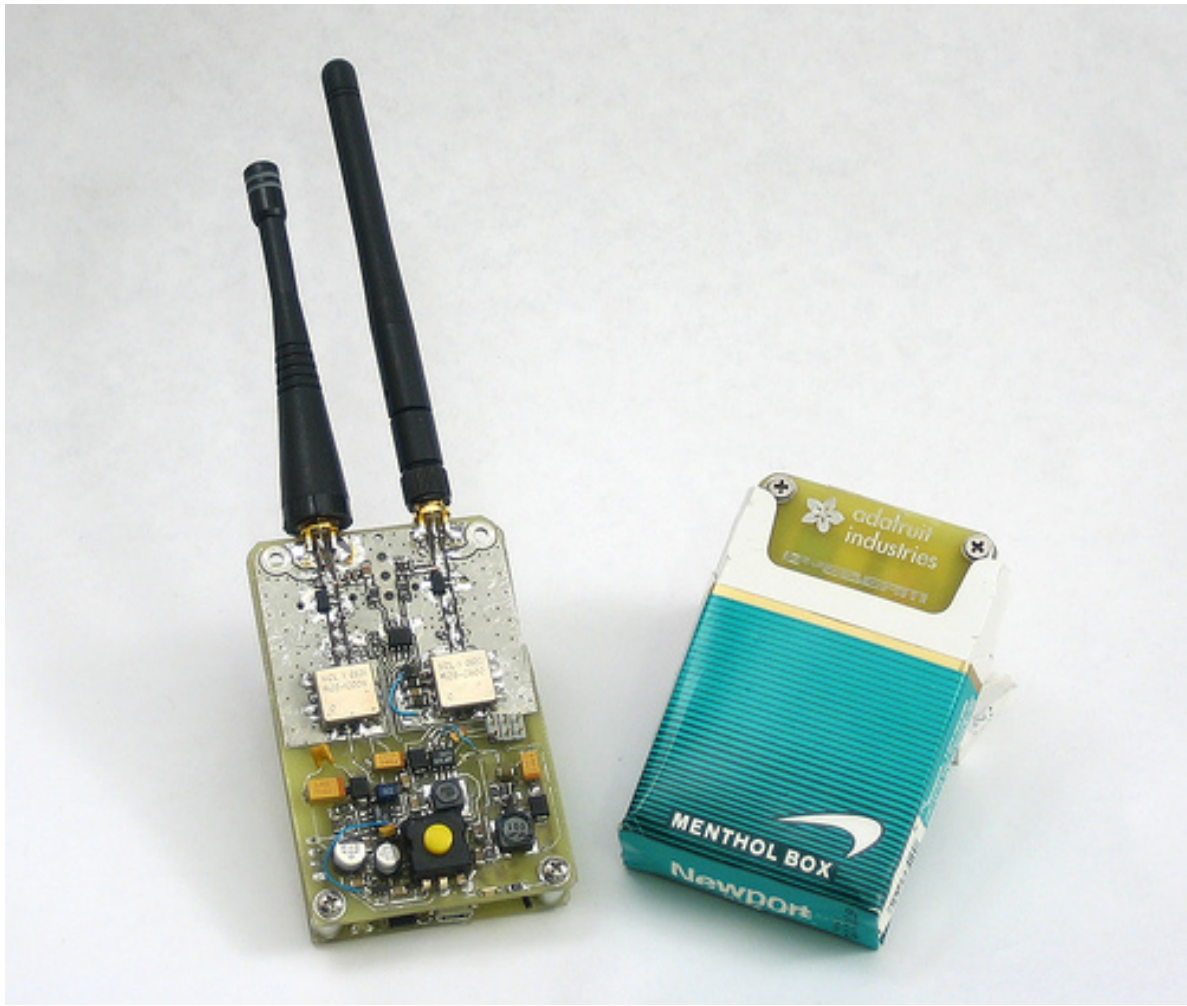


Navigational Satellite Timing and Ranging - Global Positioning System

- 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 ...)



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 AEGIS

3 Drohnen

4 Maritimer Einsatz: AEGIS

5 Network-Centric Warfare/NetOpFü

6 Sicherheit

7 Moral und Psychologie

8 Robotik und Zukunft



Moral?

Turing-Maschine

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

- Q := endliche Zustandsmenge
- Σ := Eingabealphabet
- Γ := endliches Bandalphabet mit $\Sigma \subset \Gamma$
- $\delta : (Q \setminus \{q_f\}) \times \Gamma \mapsto Q \times \Gamma \times \{L, 0, R\}$:= partielle Überführungsfunktion
- $q_0 \in Q$:= Anfangszustand
- $\square \in \Gamma \setminus \Sigma$:= leeres Feld
- $q_f \in Q$:= 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



Inhaltsverzeichnis

1 Einführung

2 AEGIS

3 Drohnen

4 Maritimer Einsatz: AEGIS

5 Network-Centric Warfare/NetOpFü

6 Sicherheit

7 Moral und Psychologie

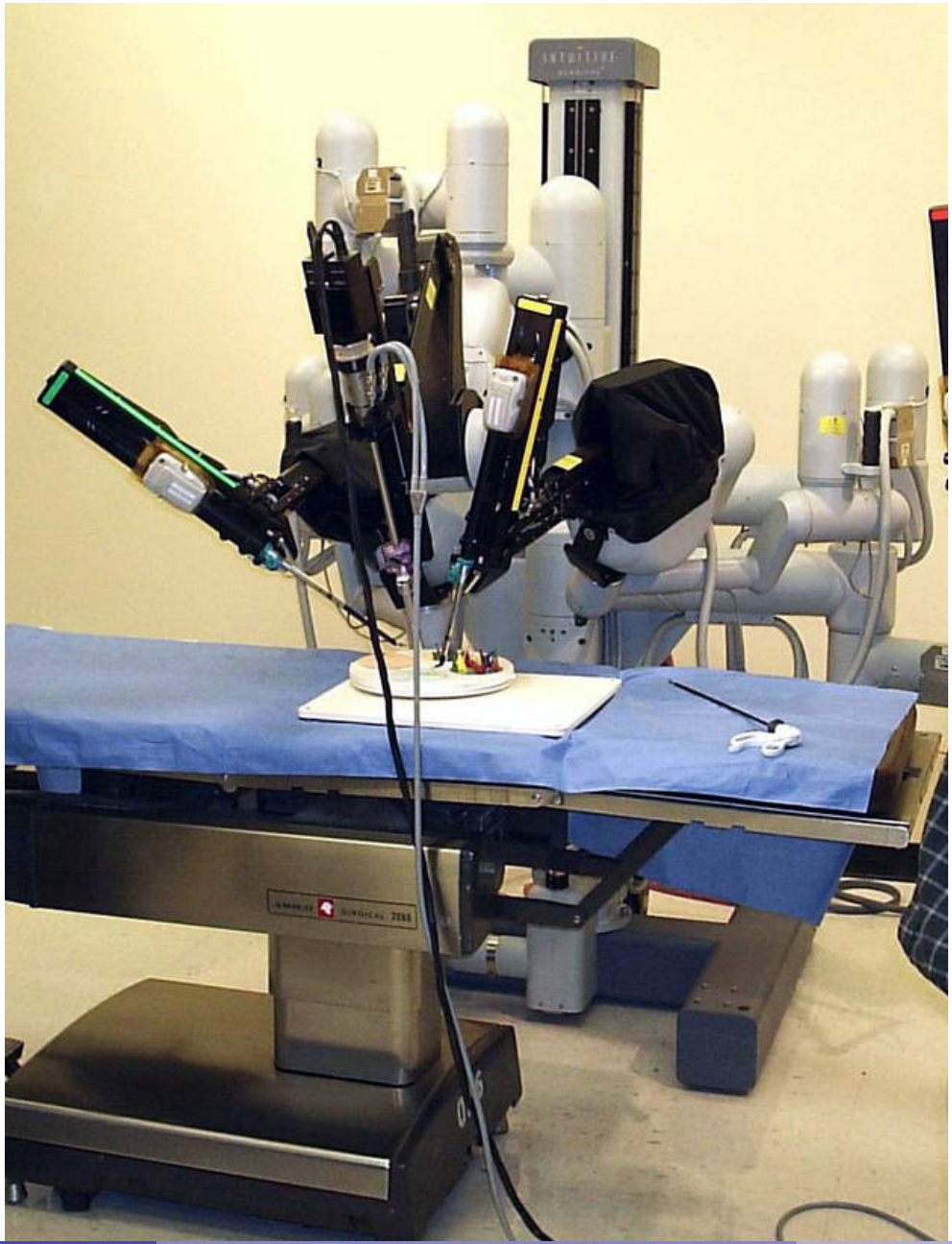
8 Robotik und Zukunft



Zukunft


ENTERBAY
HD
MASTERPIECE
T-800
(BATTLE DAMAGED EDITION)
T2
TERMINATOR 2
JUDGMENT DAY
www.enterbay.com

Chirurgischer Roboter



Lights Out Factory

- Produktionsphilosophie
- 1955: Philip K. Dick – Autofac
- keine menschlische Interaktion mehr notwendig
- vollautomatisierte Produktionsanlage
- Computer steuern, überwachen und reparieren ggf. die Anlagen



Lights out Factory

- FANUC Japan betreibt LOF seit 2001
- Roboter bauen 50 Roboter pro 50h-Schicht
- Keine Überwachung nötig für 30 Tage
- »Licht und Heizung aus«
- Philips baut elektrische Rasierer mit 128 Robotern, nur 9 Angestellte in der QA

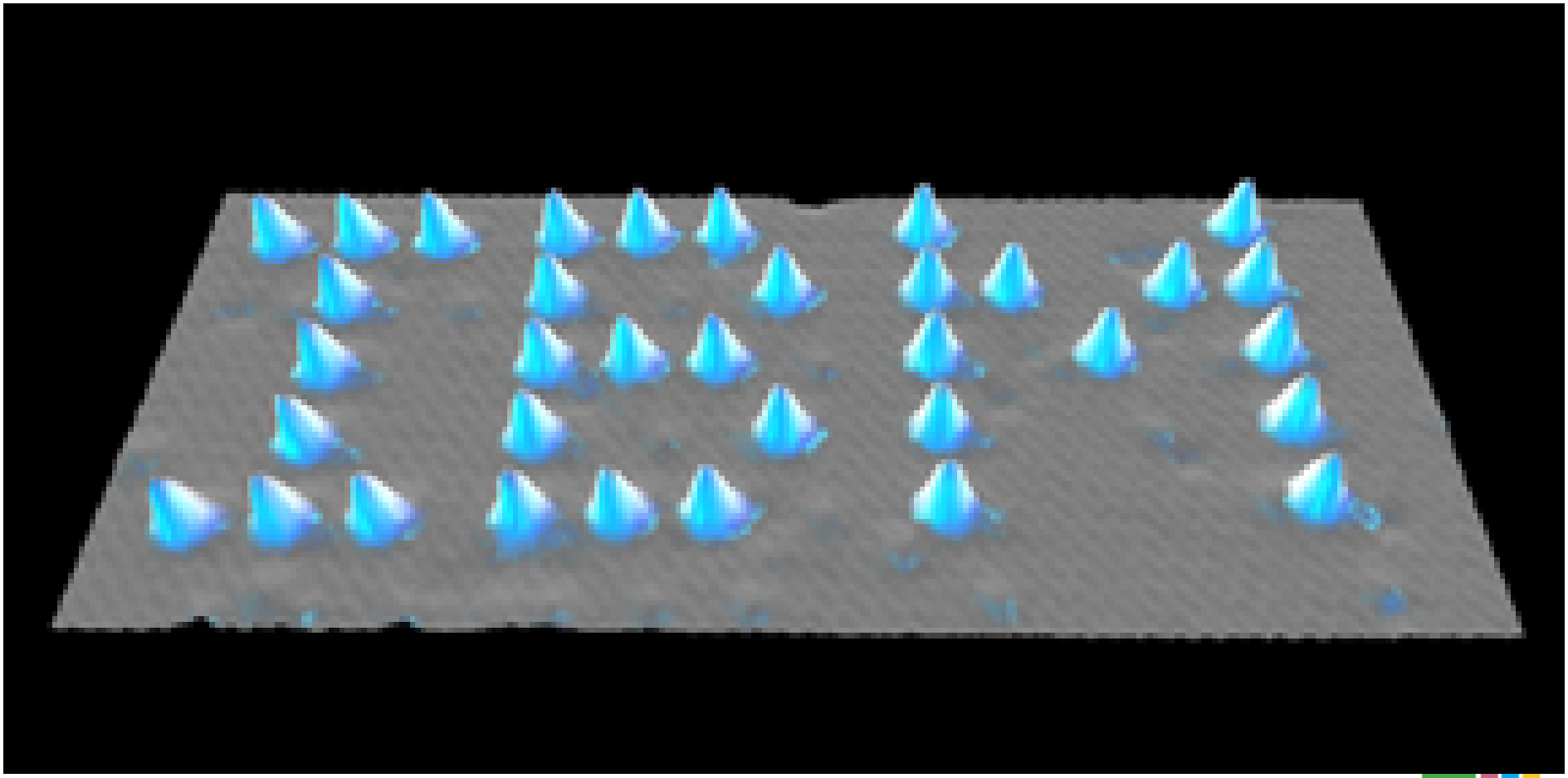


Nanotechnologie

- Einzel-Atom bis zu einer Strukturgröße von 100 Nanometern (nm)
- Nanometer = 1 Milliardstel Meter ($10^{-9}m$).
- gegenwärtige Mikroprozessoren in 22nm-Technologie
- Nanoelektronik und Nanobots
- können u.a. in Zellen eindringen und Krebs verursachen
- Idee: Nanobots reparieren u.a. elektronische und mechanische Bauteile



IBM – 35 Xenon-Atome



Inhaltsverzeichnis

1. Einführung
2. AEGIS
3. Drohnen
4. Maritimer Einsatz: AEGIS
5. Network-Centric Warfare/NetOpFü
6. Sicherheit
7. Moral und Psychologie
8. Robotik und Zukunft



Algorithmen

- Algorithmisierung des Krieges notwendig
- Algorithmen haben Grenzen – Turingberechenbarkeit
- Nebel des Krieges?
- IT-Systeme als Angriffsziel?
- Kontrolle über Systeme behalten?
- Freund-Feind-Erkennung?



rechtliche Fragen

- Befehlsnotstand
- Kombatantenstatus
- Rules of Engagement - Algorithmisierbarkeit
- Utilitarismus?



- sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- 9475 1687 4218 026F 6ACF 89EE 8B63 6058 D015 B8EF



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher
- ZRTP: 0xKaishakunin@ostel.co