Netzwerkzentrierte Kriegsführung in den Seestreitkräften

Konzepte und Entwicklungen

Stefan Schumacher

www.sicherheitsforschung-magdeburg.de
Magdeburger Institut für Sicherheitsforschung

MRK Seeland
02.05.2014



Über Mich

- 20+ Jahre Hacker, einige Jahre NetBSD-Entwickler
- Berater für Unternehmenssicherheit `www.Kaishakunin.com`
- Direktor des Magdeburger Instituts für Sicherheitsforschung
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`
- Lehrbeauftragter OvGU
- W23 JgBtl 371 KRK



Informationstechnologie und Sicherheitspolitik

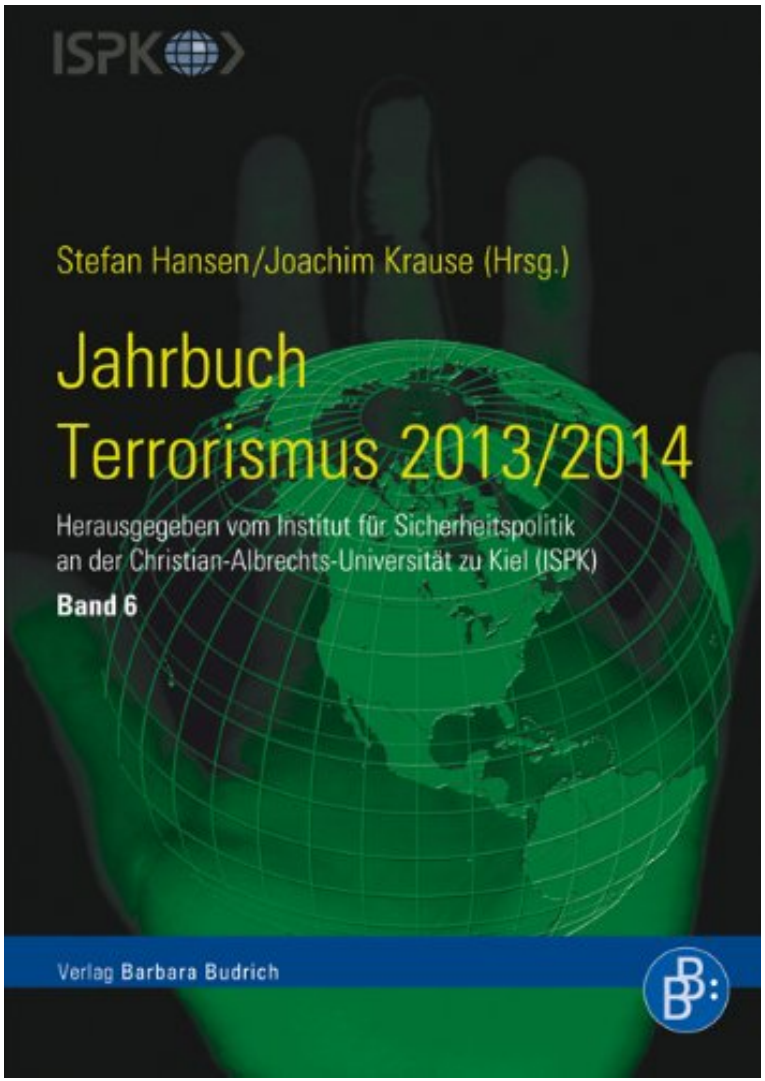
Sambleben, J. und Schumacher, S. (Herausgeber)



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

Jahrbuch Terrorismus 2013/2014

Hansen, S. und Krause, J. (Herausgeber)



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

Inhaltsverzeichnis

1. Grundlagen
2. AEGIS
3. Network Centric Warfare
4. Schluss



Inhaltsverzeichnis

1. Grundlagen
2. AEGIS
3. Network Centric Warfare
4. Schluss



NCW/NetOpFü

- Network Centric Warfare
- Vernetzte Operationsführung
- Einflüsse der Wirtschaftsinformatik in die Kriegsführung
- technisches Konzept umsetzbar durch IT und deren Miniaturisierung
- aber: Frage der Führungsphilosophie

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 Grundlagen

2 AEGIS

3 Network Centric Warfare

4 Schluss



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

USS Ticonderoga 1983



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 Leitstand 1987



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

Inhaltsverzeichnis

1 Grundlagen

2 AEGIS

3 Network Centric Warfare

4 Schluss



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

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

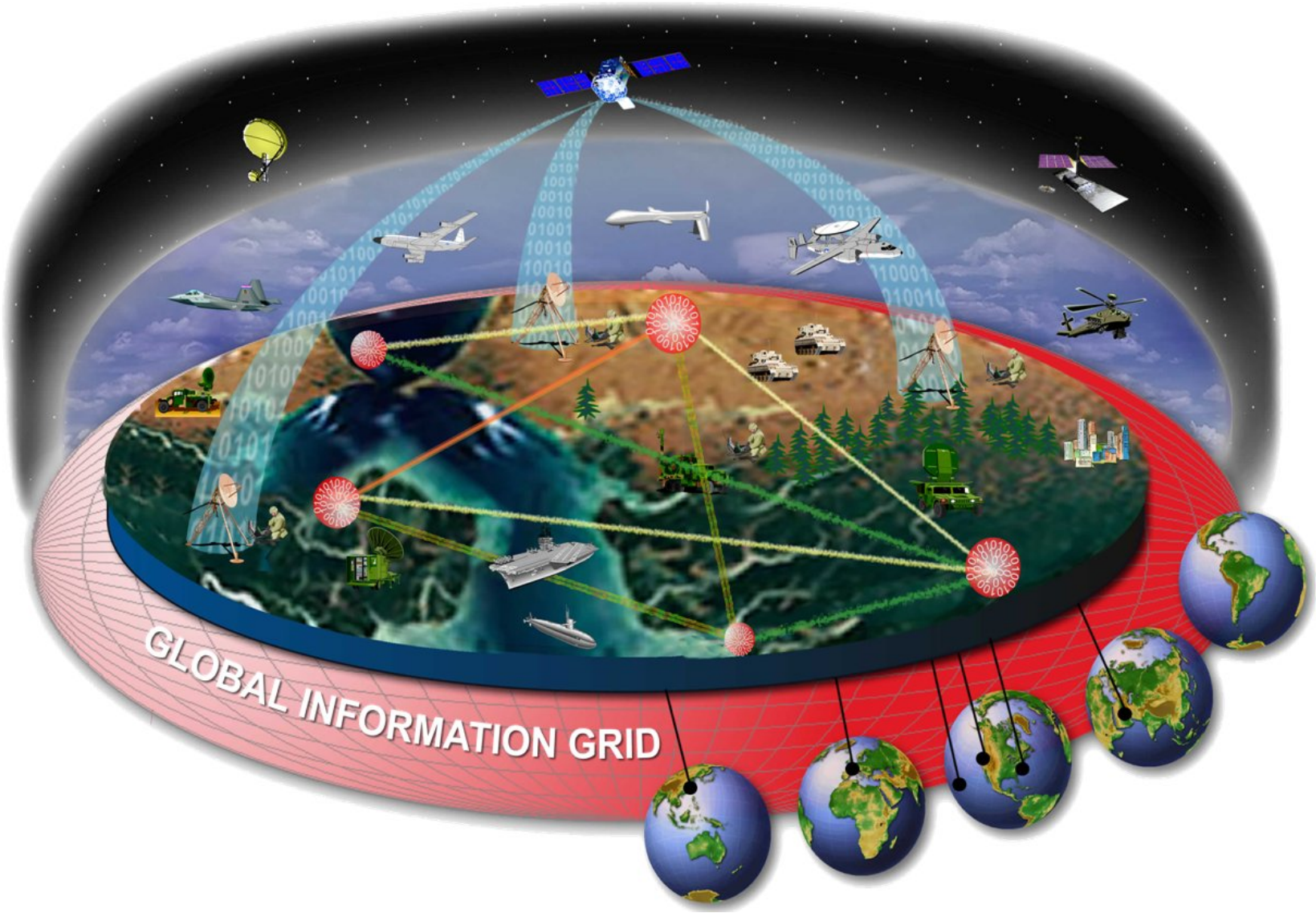
Network Centric Warfare

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
- Raketenabwehrbasen in Rumänien und Polen



Global Information Grid



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

Domänen der NCW

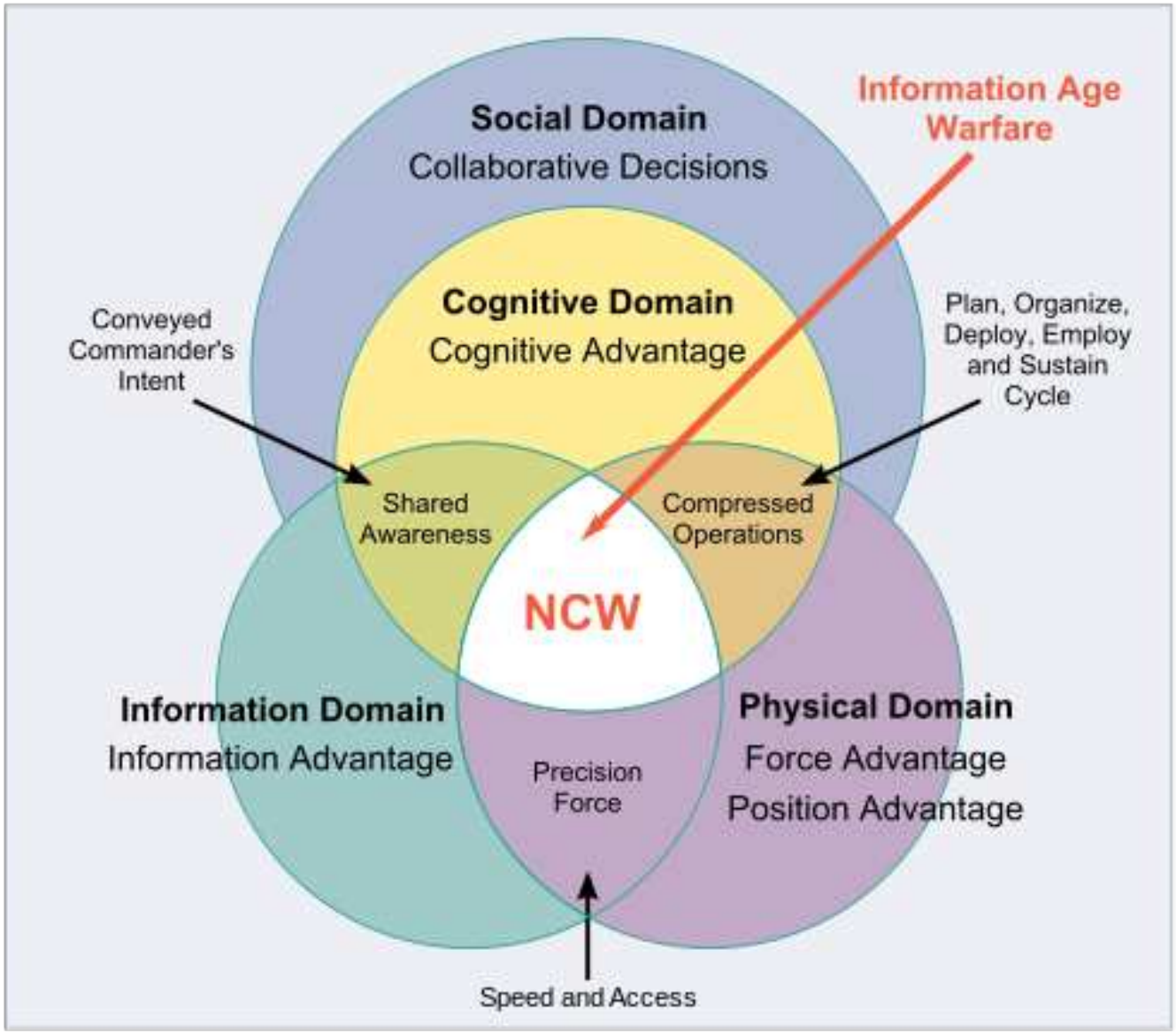


Figure 6: Information Age Warfare ... Domains of Conflict

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
- 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
- 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

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

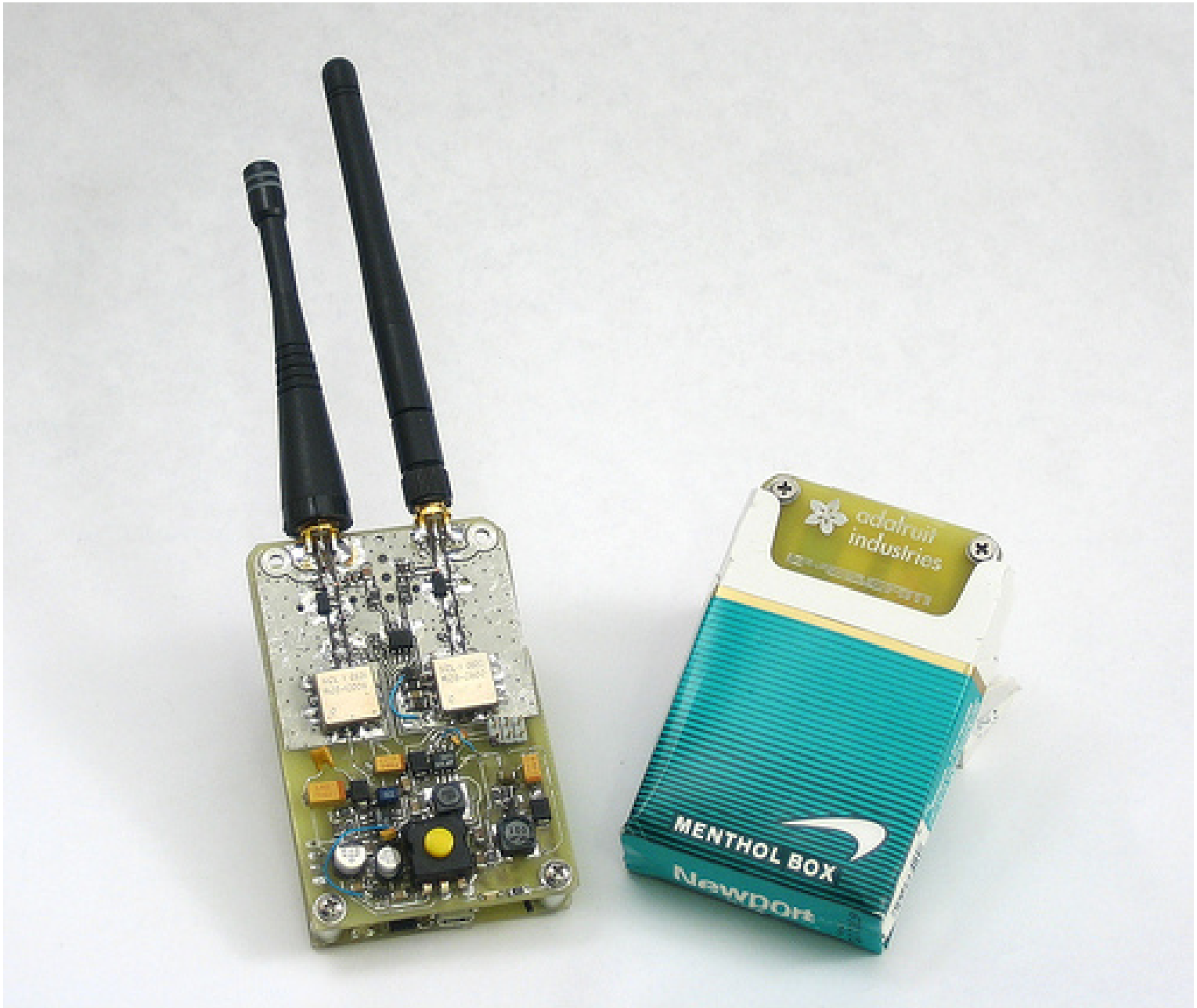


Navigational Satellite Timing and Ranging - Global Positioning System

- 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



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 Grundlagen

2 AEGIS

3 Network Centric Warfare

4 Schluss



Termine

- 07.05. Bremervörde: Vom Cyber-Kriege
- 09.50. Mannheim: Vom Cyber-Kriege
- 14.05. Gold Coast/Australia: Security in a Post NSA world
- Juni: E-Businesslotsen Halle u.a. Industrie 4.0

Kontakt

- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher