Der neue Cyber-Bereich der Bundeswehr
Pläne, Strukturen, Fähigkeiten und offene Fragen

Thomas Reinhold - reinhold@ifsh.de - cyber-peace.org

Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Warum das Thema /1

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Q: bundeswehr.de

Warum das Thema /2

- Tagesbefehl vom 26.04.2016
- Abschlußbericht des Aufbaustabes "Cyber und Informationsraum CIR"
  - BMVg: Abteilung "Cyber/IT" (CIT) im BMVg seit 10.2016
  - BW: Organisationsbereich "Cyber & Informationsraum (CIR)" ab 04.2017

Warum das Thema /3

- Weißbuch der Bundeswehr 2016
  - Verteidigung im Cyberspace essentieller Bestandteil der Sicherheit Deutschlands
  - Entwicklung und des Trainings defensiver und offensiver "Hochwertfähigkeiten"
  - "*Die Befähigung zum bundeswehrgemeinsamen Wirken in allen Dimensionen (..) ist der übergeordnete Maßstab [und eine] Wirkungsüberlegenheit muss über alle Intensitätsstufen hinweg erzielt werden können*"
- Cyber-Sicherheitsstrategie der Bundesregierung
  - Cyber-Sicherheit ist "*wesentlicher Baustein strategischer Konzepte und ressortübergreifender Vorhaben der Bundesregierung"* und *"Innere und äußere Sicherheit im Cyber-Raum nicht mehr trennscharf voneinander abzugrenzen*"

- NATO-Gipfel 2016 in Warschau
  - Cyberverteidigung ist Bestandteil der Bündnis-Planungen
  - Cyberangriffe können nach Art. 5 die Beistandspflicht auslösen

Ein wenig historischer Kontext /1

- Bisheriger "Cyber"-Sachstand: ~ 13.700 Dienstposten bei der BW
- Streitkräftebasis (SKB)
  - Führungsunterstützungskommando (FüUstgKdoBw)
  - Betriebszentrum "IT-Systeme der Bundeswehr"
  - Militärischer Abschirmdienst
  - Kommando Strategische Aufklärung mit den Bataillonen für elektronische Kampfführung und der Abteilung Computer Netzwerk Operationen (CNO)

Ein wenig historischer Kontext /2

- Heer / Marine / Luftwaffe
  - Systemzentren für den IT-Betrieb
  - IT-Personal für Aufbau/Betrieb der Gefechtsstände
- Abteilung Ausrüstung, Informationstechnik und Nutzung (AIN) beim BMVg
  - CERTBw
  - Bundesamt für Ausrüstung, Informationstechnik und Nutzung (BAAINBw)
  - WTD 81 Wehrtechnische Dienststelle für Informationstechnologie und Elektronik

Der Aufbaubericht

- Von der Leyen: "*Wir haben sehr viel Expertise in der Bundeswehr, müssen diese aber vernünftiger bündeln, sichtbarer machen und schlagkräftiger aufstellen [der neue militärische Organisationsbereich soll aufgestellt werden] um die notwendige Expertise und Möglichkeiten zu entwickeln*“

- Seit November 2015 in Arbeit
- Federführung
  - Katrin Suder, Rüstungsstaatssekretärin
  - Generalleutnant Markus Kneip, stellv.Generalinspekteurs der Bundeswehr
  - Gundbert Scherf, Beauftragter für Strategische Steuerung Rüstung
- Umstrukturierungen im BMVg und bei der Bundeswehr bis 2021

Neue Strukturen und Personalien: BMVg

- Abteilung Ausrüstung, Informationstechnik und Nutzung => Abteilung A
- Neue Abteilung Cyber/ IT (CIT)
  - Chief Information Officer (CIO) ThyssenKrupp-Manager Klaus-Hardy Mühleck
  - CIO als "point of contact" für Abstimmung im Rahmen von Allianzen
  - anfänglich 130 Dienstposten, davon 95 umgewidmente Dienstposten
- Kernziele:
  - Effektivierung von IT Projekten, deren Planung, Beantragung, Budgetierung
  - Agiles Management bei Beschaffung, Entwicklung und Forschung
- BWI GmbH
  - Seit 2016 100%ige Bundesgesellschaft
  - Zentraler IT-Dienstleister der Bundeswehr

Neue Strukturen und Personalien: Bundeswehr /1

- Neuer Organisationsbereich Cyber und Informationsraum (CIR)
  - zum Start 13.700 bestehende Dienstposten, 290 DP neue , max 20.000 DP
  - Leitung: Generalmajor Ludwig Leinhos
  - Organisationsbereich gleichrangig zu Heer/Marine/Luftwaffe/Sanitätsdienst

- Kompetenzbündelung
  - Führungsunterstützungskommando (FüUstgKdoBw)
  - Kommando Strategische Aufklärung (KdoStratAufkl)
  - Zentrum für Operative Kommunikation der Bundeswehr (ZOpKomBw)
  - CNO wird zum Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw)
  - IT-Zentrum der Bundeswehr (IT-ZentrumBw)
  - Berufsqualifizierende Aus-, Fort- und Weiterbildung

=> Großteil bereits bei Streitkräftebasis zentralisiert

Neue Strukturen und Personalien: Bundeswehr /2

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- DP-Zuwachs zum 1.4.2017 bei:
- KdoCIR: 230
- Zentrum Cyber-Sichheit Bw: 40
- Zentrum Cyber-Operationen: 20

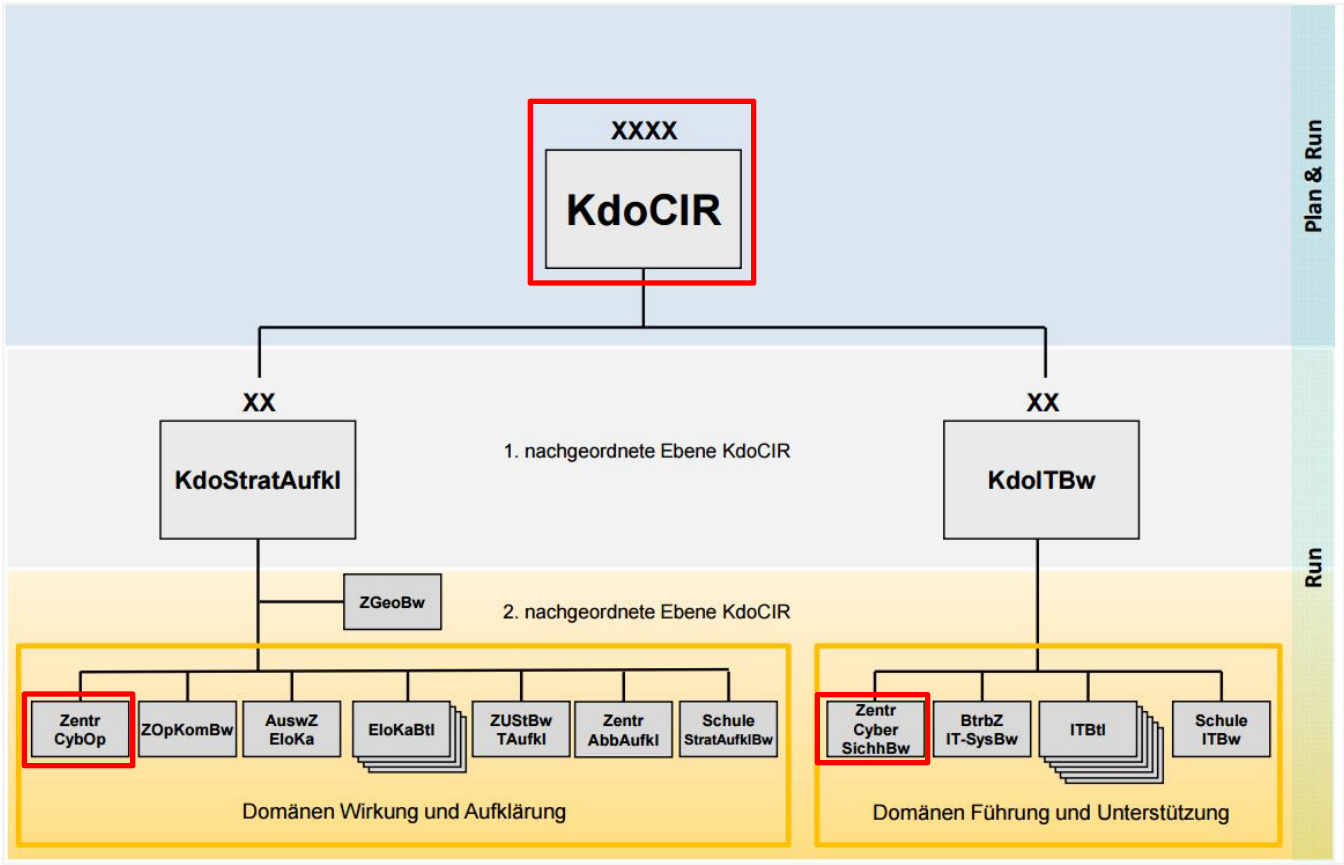


Abbildung 5: Startaufstellung Organisationsbereich Cyber- und Informationsraum 2017

Alte und neue Fähigkeiten

- Zusammenführung bestehender Ressourcen der
  - ELOKA
  - CNO
  - Strategische Aufklärung
  - MAD
  - Lagebild & Kommunikation
  - IT-Sicherung

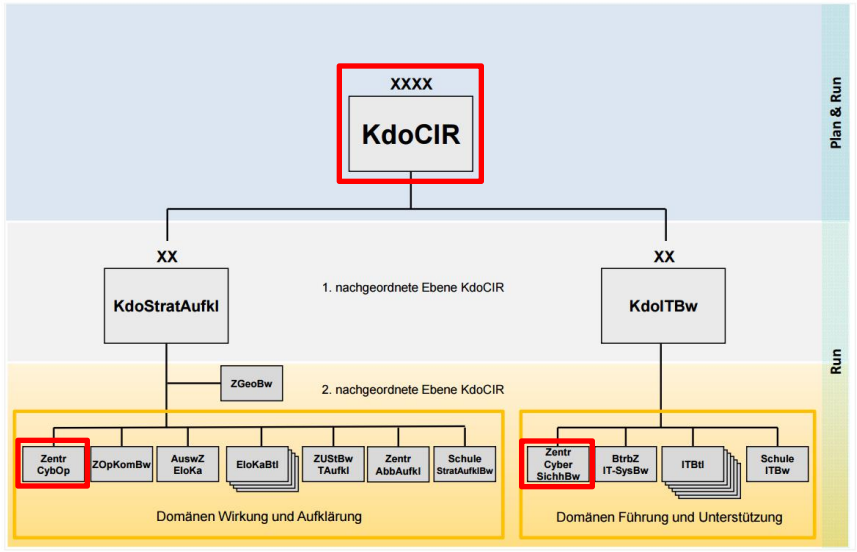


Abbildung 5: Startaufstellung Organisationsbereich Cyber- und Informationsraum 2017

Alte und neue Fähigkeiten

- Zusammenführung bestehender Ressourcen der
  - ELOKA
  - CNO
  - Strategische Aufklärung
  - MAD
  - Lagebild & Kommunikation
  - IT-Sicherung
- Ausbau der Ressourcen von
  - Computer Netzwerk Operationen
    - Stärkung der vorhanden CNO-Fähigkeiten
    - Red-Teaming als Beitrag zum Schutz (Selbst-Angriff, Penetration-Tests)
  - IT-System-Schutz

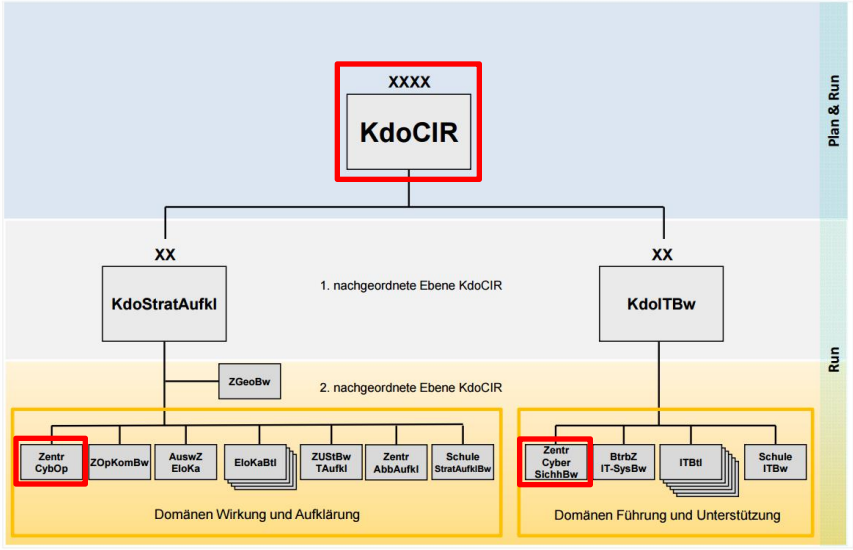
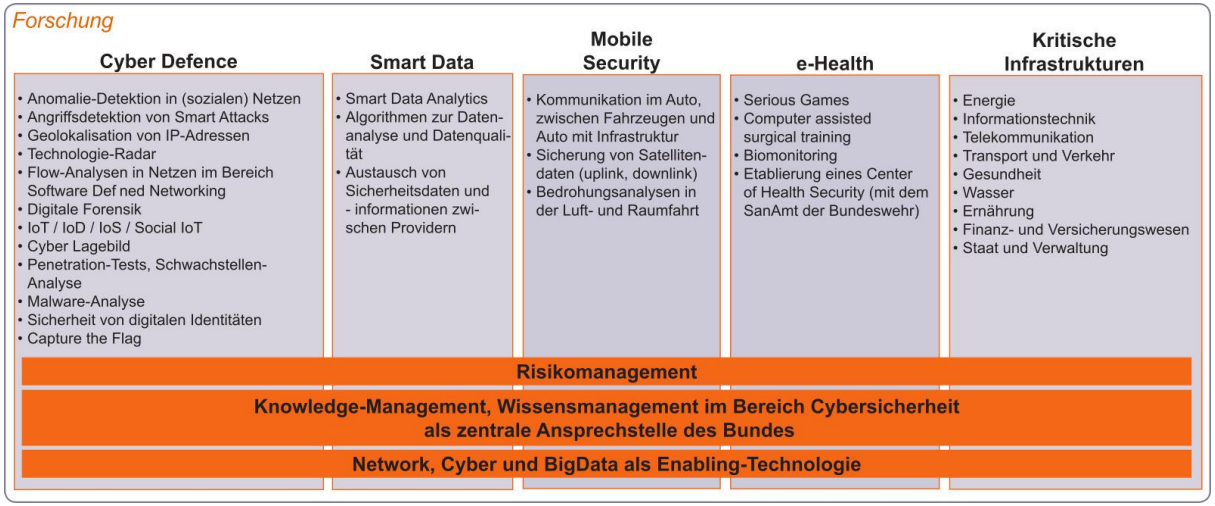


Abbildung 5: Startaufstellung Organisationsbereich Cyber- und Informationsraum 2017

Elektronische Kampfführung (ELOKA)
Computer Network Operations (CNO)

Neue Strukturen und Personalien / Forschung

- Bundeswehrhochschule in München
  - "*zentrale, wissenschaftliche Aus-, Fort und Weiterbildungsstätte (..) für Tätigkeiten im Bereich der Cyber-Verteidigung und Cyber-Sicherheit*"
  - Studiengang "Cyber-Sicherheit" ab 2018 bis zu 70 AbsolventInnen/Jahr
- Forschungszentrum Cyber Defence (CODE) 2013 gegründet
  - Aufbau eines 7000 m² großen Hochsicherheitsgebäude zur Cyber-Forschung
  - 11 neue W3-Professuren sowie 67 Mitarbeiter vom BMVg finanziert
  - 200 weitere Mitarbeiter aus Drittmitteln finanziert



Offene Fragen und Probleme /1

- Cyberverteidigung auch im Inneren
  - "*Das klassische Denken ist das versäulte Denken innerhalb der Ressortgrenzen. Und das ganze Thema Cyberpolitik zeigt es klassisch, dass zum Beispiel die Trennung von äußerer und innerer Sicherheit im Cyberraum obsolet ist. Es gibt keine äußere oder innere Grenze im Cyberraum mehr.*"
  - Cyber & hybride Konflikte
- CNO-Einheit und offensive Planungen
  - Welches strategisches Ziel
  - Welche "Rules of Engagement" und Grenzen des Einsatzes
  - Welche völkerrechtlichen Grundlagen

Offene Fragen und Probleme /2

- Prinzipielle Probleme bei Aktivitäten im Cyberspace
  - Die realistische Einsatzfähigkeit erfordert eine aktive Vorfeldanalyse
  - Jeder Fremdzugriff auf IT ist eine Manipulation
- Maßnahmen einer effektiven Cyberverteidigung
  - Hackback
  - Abschreckung
- Entwicklung "effektiver Wirkmittel" für den Cyberspace
  - Die Nähe von CODE & ZITiS
  - Kooperationen mit nat./internationalen Geheimdiensten
  - Offensiver Charakter von Penetration-Tests (Red-Teaming)

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Cyberwehr
Wir. Dienen. Neuland.

Q: Chaos Computer Club ccc.de