**Sicherheitspolitische Informationsveranstaltung am 03.Februar 2017**

# Cyber-Sicherheit in der Bundeswehr

Am 03.02.2017 wurde die Veranstaltungsreihe 2017 der Kameradschaft der Fernmelder Koblenz/Lahnstein mit der Quartalsveranstaltung I/2017 im Haus der Begegnung - Soldatenheim Koblenz, Horchheimer eröffnet.

Nach der **Begrüßung der 28 Teilnehmer um 19:00 Uhr durch Herrn Oberst a.D. Siegel** und Vorstellung des **Referenten,**

**Herrn Oberst Dipl.Inform. Gerd Weiß,**
**Leiter Geschäftsbereich IT-Sicherheit / Cyber Defence und**
**stv-Leiter IT-Zentrum Bw EUSKIRCHEN**

**eröffnete O Weiß** seinen Vortrag mit einer kurzen Vorstellung seiner Person und seinen **Werdegang in der Bundeswehr**.

| | | |
|---|---|---|
| 1978 – 1983 | Offiziersausbildung und Informatikstudium , | München u.a. |
| 1983 – 1989 | ZgFhr 2./FmBtl 310 und KpChef 4./FmBtl 330, | Koblenz |
| 1989 – 1992 | IT-Projektoffizier im NATO HQ AFCENT, | Brunsum, NL |
| 1992 – 1994 | Hörsaaleiter an der Fernmeldeschule | Feldafing |
| 1994 – 1995 | KpChef 1./FmRgt 920 | Kastellaun, |
| 1995 – 1998 | Dezernent Gruppe Weiterentwicklung FM, | Pöcking |
| 1998 – 2002 | Deutscher Austauschoffizier beim U.S.Programm Executive Office (PEO) C3S, | Fort Monmouth, New Jersy, USA |
| 2002 – 2005 | KdrFmBtl 701, 2004 Kdr FmBtl KFOR | Leipzig u. Prizren, KOSOVO |
| 2005 – 2010 | Referent IT-Sicherheit/Cyber Defence, BMVG MII/IT 3, | Bonn |
| 2010 – 2017 | Ltr Gesch.Bereich IT-Sicherheit / Cyber Defence und stv.Ltr. IT-Zentrum Bw, | Euskirchen |
| Ab 01.04.17 | Ltr Cyber Security Operation Center und stv. Kdr Zentrum für Cyber-Sicherheit Bw. | Euskirchen |

---

**Oberst Weiß behandelte in seinem Informationsvortrag nachstehende Themenbereiche,**
**Schwerpunkt Geschäftsbereich 100:**

- **Rückblick auf allgemeine technische Entwicklung** vom Automobil – über Flugzeug – Waffen wie Tank/Panzer u. Atombombe – zum Computer und Internet.
  All diese **Entwicklunge**n wurden im Entwicklungszeitraum mit **skeptischen Gedanken** zur **Notwendigkeit und Nutzungsdauer** in Frage gestellt – sie sind **aber heute nicht mehr aus unserem Leben zu verdrängen.**
  **Ähnlich skeptische Fragen** gab und gibt es auch zum **Kommunikationsmittel „Internet“** mit Nutzung des **„World Wide Web“**.
  **Das Internet gehört inzwischen auch in der Bundeswehr zum meistgenutzten Kommunikationsmittel.**
- **Angriffe im Internet – *Cyberfangriffe:***
  **Cyberangriffe** wurden am **Beispiel** echter Angriffe dargestellt und die Gefahren für die Nutzer und die Netzsicherheit erläutert. Neben Angriffen mit **kriminellem Hintergrund**, die **überwiegend den zivilen/privaten Bereich** betreffen, besteht auch die **Gefahr auf Beeinträchtigung wichtiger Infrastrukturen** –Stromnetze und Stromversorgungseinrichtungen (auch Atomkraftwerke) und andere lebenswichtige Einrichtung- von Staaten und damit **auch auf den militärischen Bereich.**

**Aktuelle Angriffe:** **Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für 2016**

| | |
|---|---|
| 560 Mil. | Bekannte Schadsoftwarevarianten |
| 39.000 | festgestellte Infektionen deutscher IT-Systeme pro Tag |
| 44.000 | infizierte Emails / Monat in Regierungsnetzen |

Größtes Botnetz: Bredrolabs mit 30 Mill. Bots.

**Bundeswehr 2016**

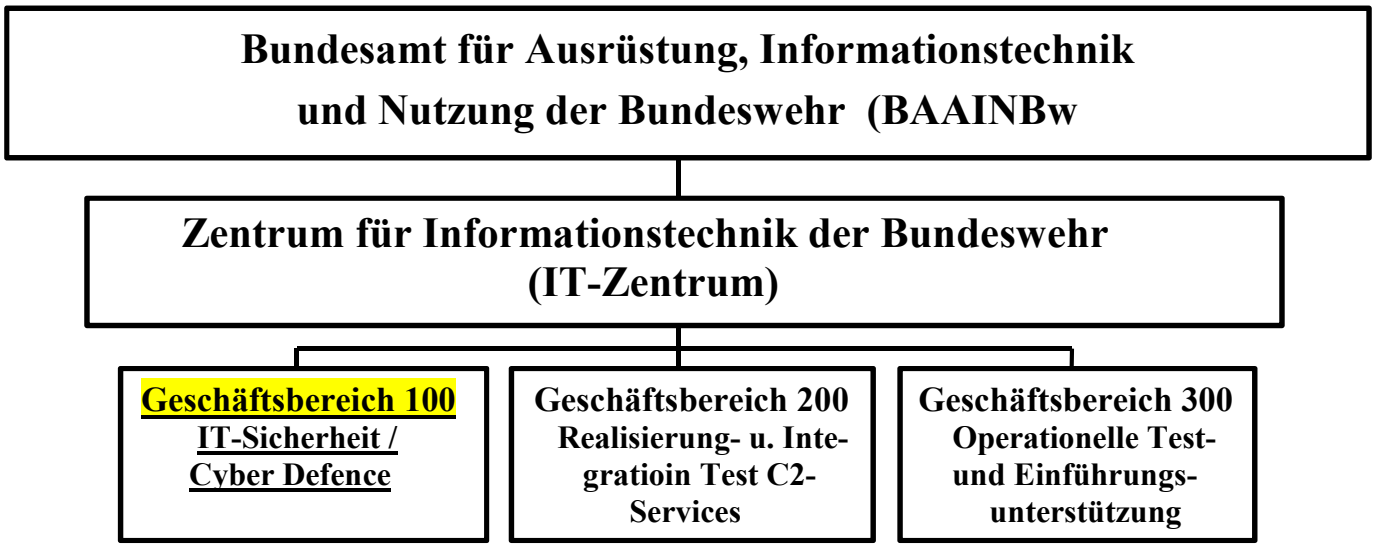
9 Mill. Cyberangriffe / gefährliche Zugriffsversuche, davon 21.000 in Einsatzländern
**4.600 Schadprogramme auf Bw-Rechnern beseitigt.**

**Fazit:** **Don‘t click !** Bei Cyber Angriffen ist der **Nutzer** in der Regel der **„Türöffner“.**
***Deswegen keine Email-Anhänge unbekannter Absender öffnen!***
**Wichtig:** **Sensibilisierung der Nutzer**

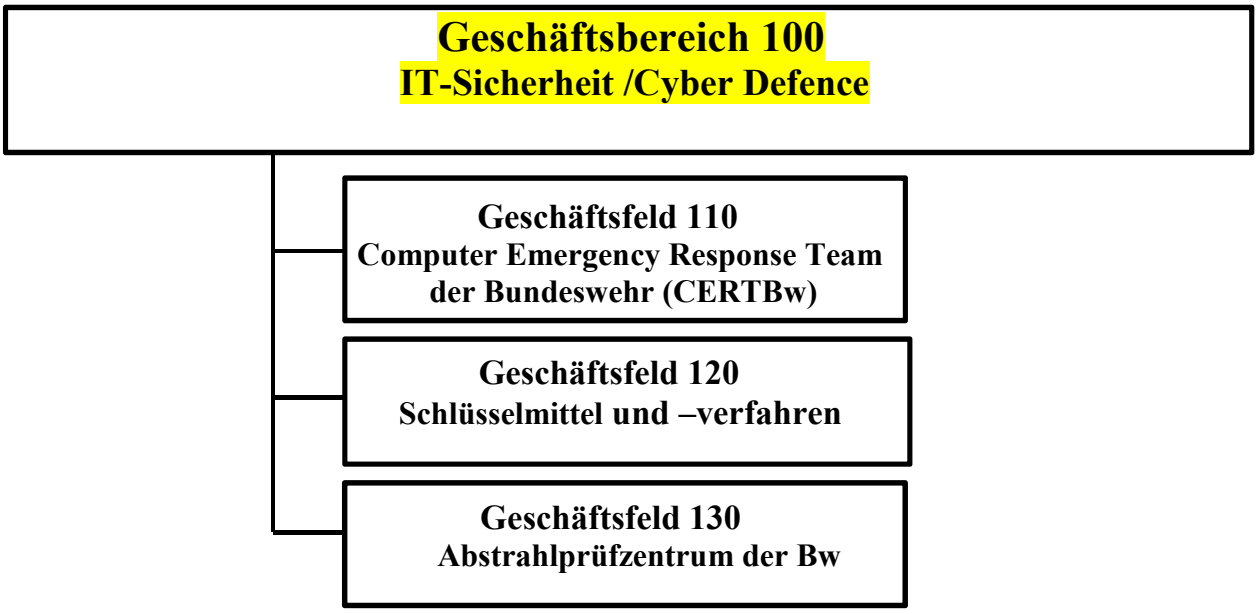
- **IT-Sicherheit / Cyber-Sicherheit / Cyber Defence**
  **Die Bundeswehr** hat als eine der **ersten Armeen die Notwendigkeit** zur Absicherung von IT-Systemen erkannt und **ab 2002 beim IT-Zentrum der Bundeswehr** (Euskirchen) unter anderem **das Computer Emergency Response Team der Bundeswehr (CERTBw) aufgestellt.**

**IT-Zentrum der Bundeswehr**
**Aufgabe: Sicherstellung der Führungsfähigkeit der Bundeswehr**

**Unterstellung und Gliederung**




- **IT-Sicherheit / Cyber Defence (Geschäftsberereich 100)**



- **Ein wichtiger Bereich ist das Computer Emergency Response Team (CERTBw)**

**Das CERTBw** als **„Feuerwehr des Cyberraums“** ist zuständig für sämtliche Computer der **Bundeswehr**. **Aufgaben:**

- Zentrale **IT-Sicherheitsüberwachung** im IT-System Bw (**auch in den Auslandsdienststellen der Bw im Einsatz**)
- Durchführung von **Schwachstellenprüfungen** an IT-Systemen
- Unterstützung bei **Akkreditierung** von IT-System Bw
- Aktuelle **Hinweise auf Schwachstellen** (CERTBw Advisory)
- Festlegen von **Maßnahmen zur Schadensbegrenzung** und –beseitigung
- **Computerforensische Untersuchung** von IT-Sicherheitsvorfällen

**Enge Zusammenarbeit** besteht zu Diensten
**CERT BWI, CERT Bund, BSI (Bundesamt Sicherheit Informationstechnik), CERT-Verbund, BKA, Bundespolizei, Frauenhofer FKIE, Universität der Bw**
und **Internationalen CERT-Diensten z.B. (NATO, US EUCOM, US-Defence Ministerium, Österreich, Schweiz, England, ENISA(European Agency).**

**Durch Ministerin-Entscheidung** in Befehlen vom 17.09.2015, 26.04.2016 und dem **Tagesbefehl vom 05.10.2016** wurde eine **neue Organisation der IT-Sicherheit** angeordnet.

*Die Bundesministerin* *Berlin, 5. Oktober 2016*

***Tagesbefehl***
Soldatinnen und Soldaten,
zivile Mitarbeiterinnen und Mitarbeiter**!**

*Als offene Gesellschaft und global vernetzte Volkswirtschaft stehen wir von vielschichtigen sicherheitspolitischen Herausforderungen. Gefahren, Konflikte und Krisen entwickeln sich dynamischer, sie treten parallel auf, wirken auf unterschiedlichen Ebenen und beeinflussen sich wechselseitig. In dieser Situation haben wir den Cyber-und Informationsraum als eine Dimension identifiziert, der wachsende Bedeutung zukommt. Um eine verantwortungsvolle gesamtstaatliche Gesamtvorsorge zu gewährleisten, muss auch der Geschäftsbereich des Bundesministeriums der Verteidigung seine Kompetenzen und Fähigkeiten langfristig auf die neuen Herausforderungen hin ausrichten.*

*Der Cyber- und Informationsraum hat sich bei unseren Partnern und Verbündeten längst zu einem*
*Strategischen Handlungsraum entwickelt: seit dem Gipfel von Warschau gilt er offiziell als Militärischer Operationsraum der NATO. Für die Bundeswehr heißt das: Sie muss Schritt halten mit dieser Entwicklung. Sie muss das Thema initiativ besetzen und damit gestalten. Sie muss muss die mit der Digitalisierung verbundenen Chancen nutzen, aber auch frühzeitig die Risiken erkennen – und den Gefahren wirkungsvoll begegnen können. Zudem muss die Bundeswehr in der Lage sein, sich auf kürzer werdende technische Innovationszyklen in der Informations- und Kommunikationstechnik einzustellen.*

*Mit meiner Entscheidung vom 26.April 2016 hatte ich den erweiterten Aufbaustab „“Cyber und Informationsraum“ (CIR) unter der Führung von Generalmajor Leinhos angewiesen. Die notwendigen organisatorischen Veränderungen im Ministerium und im nachgeordneten Bereich vorzubereiten.*

*Mit dem heutigen Tag ist ein erster Meilenstein dieser Arbeit erreicht. Wir richten im Ministerium – an den Standorten Bonn und Berlin – die neue Abteilung Cyber/IT (CIT) ein. Mit deren Führung habe ich Herrn Klaus-Hardy Mühleck betraut. Er verantwortet in dieser Funktion künftig die Bereiche Cyber-/IT-Governance und IT-Services/Informationssicherheit sowie die zukünftige strategisch inhaltliche Ausrichtung der Bundeswehr Informationstechnik GmbH (BWI). Zugleich nimmt der Abteilungsleiter die Aufgaben des „Chief Information Officer“ für unser Ressort wahr.*

*In der neuen Abteilung bündeln wir alle IT- und cyber-relevanten Aufgaben und Fähigkeiten zu ein er zentralen Stelle im Ministerium. Dazu werden bestimmte Dienstposten verschoben, aus dem*

*Aufbaustab, aber auch aus anderen Referaten; so das sich Unterstellungen ändern. Das wiederum hat zur Folge, dass die bisherige Abteilung Ausrüstung, Informationstechnik und Nutzung (AIN) nach der Ausgliederung des IT-Anteils nun umbenannt wird in Abteilung Ausrüstung (A)*

*Mit dieser organisatorischen Weiterentwicklung beginnen wir, auf der Ebene des BMVg die entscheidenden Weichen zu stellen für eine stärker IT-getriebene Modernisierung sowie die Aufwertung des Cyber- und Informationsraumes zu ein er eigenen militärischen Dimension. Und wir bauen damit ganz konkret unseren Beitrag für eine umfassende Sicherheitsarchitektur in Deutschland aus.*

*Für das außerordentliche Engagement, mit dem alle Beteiligten diese wichtigen Schritte in die Zukunft gestaltet und vorangetrieben haben, möchte ich mich von Herzen bedanken. Ich wünsche Herrn Mühleck und seinen Mitarbeiterinnen und Mitarbeitern viel Erfolg für die herausfordernde Arbeit. Und ich bin mir sicher, dass wir auch die nächsten Etappen auf diesem Weg gemeinsam meistern werden.*

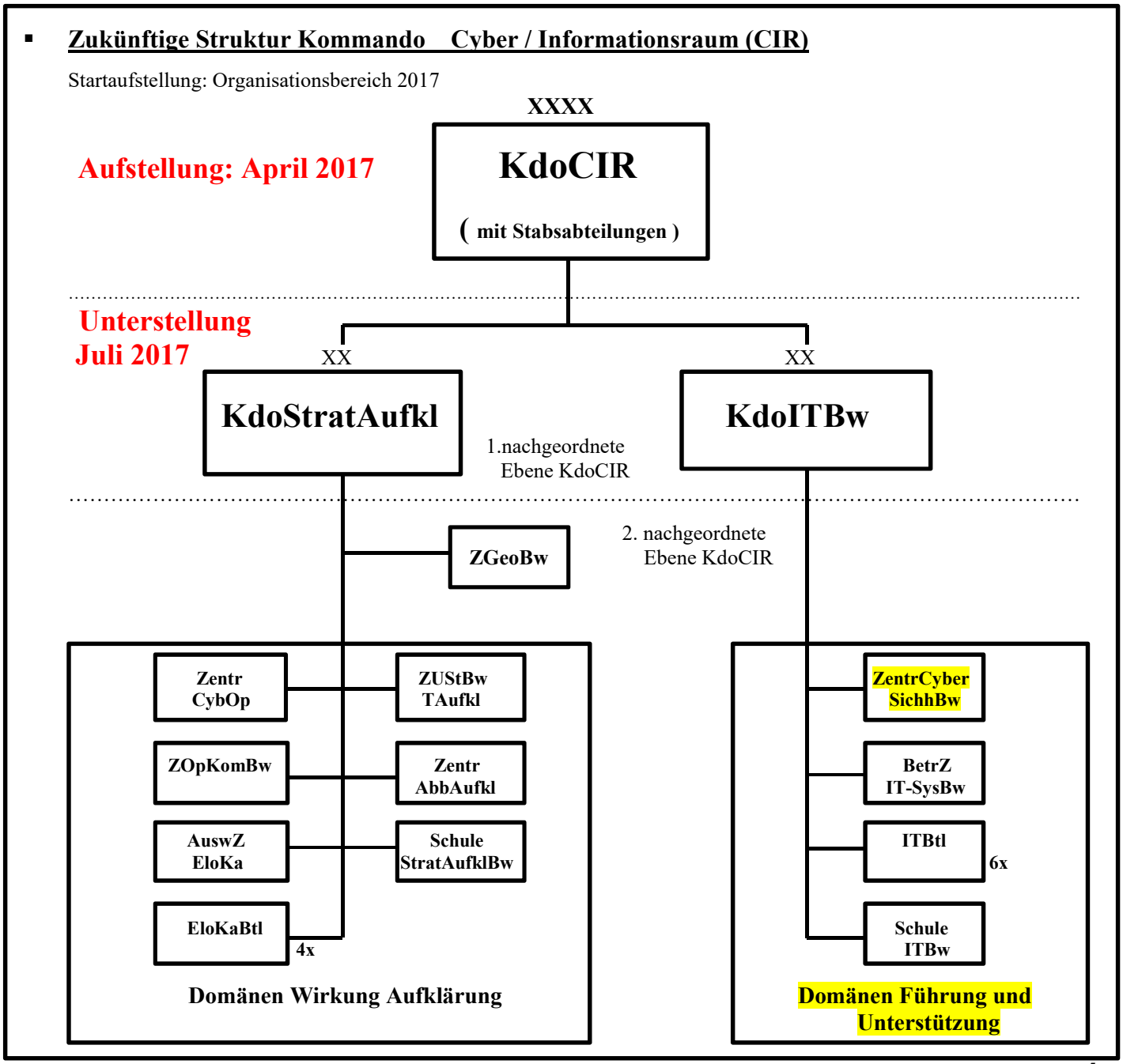
*Dr. Ursula von der Leyen*
*Bundesministerin der Verteidigung*

*(Dieser Tagesbefehl wurde vom Schriftführer KdFm Koblenz/Lahnstein aus dem Magazin für den Fernmeldering e.V. , F-Flagge, 43. Jahrgang / Nr. 4 – 2016 übernommen)*

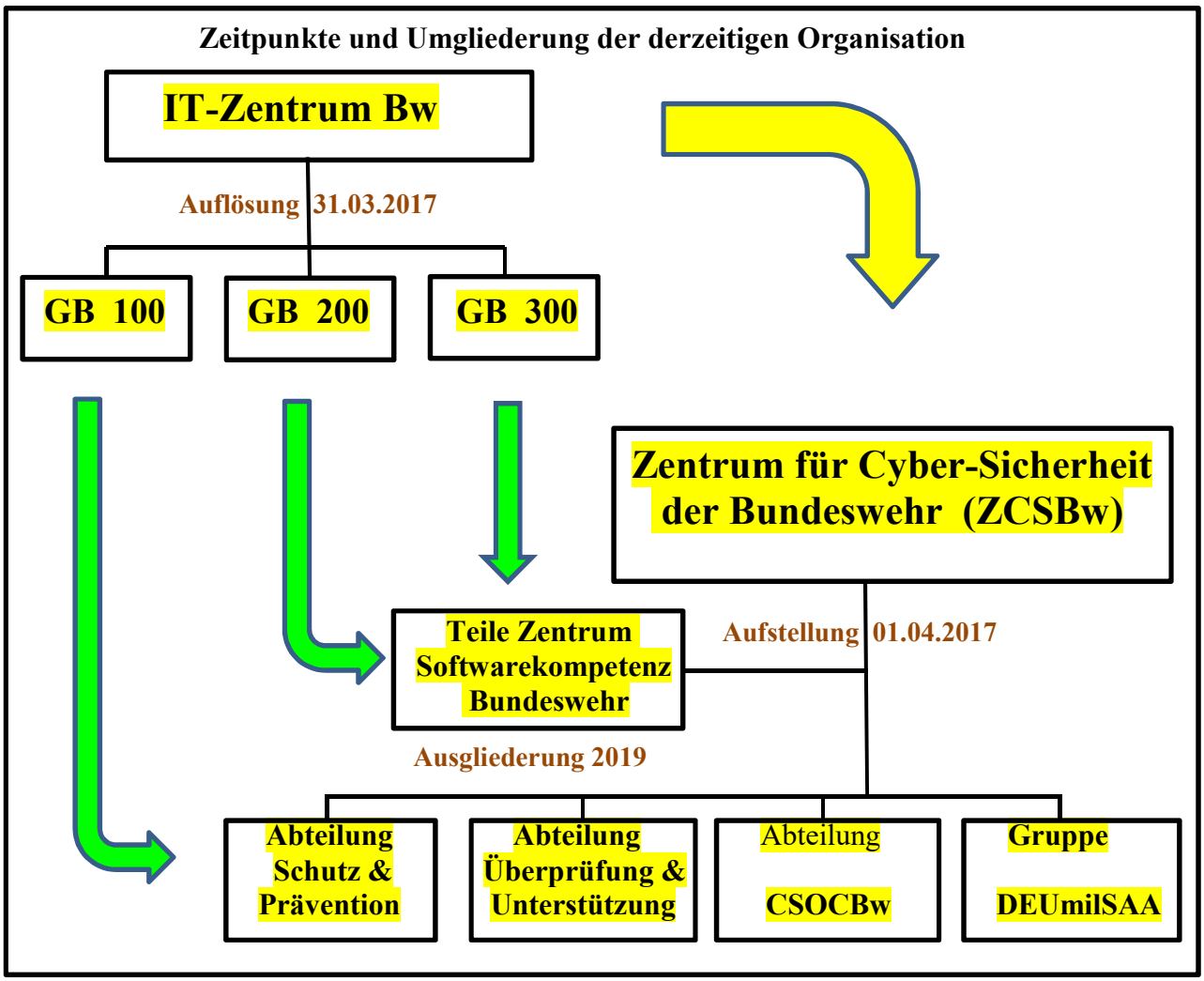
---

- **Zukünftige Struktur Kommando Cyber / Informationsraum (CIR)**

Startaufstellung: Organisationsbereich 2017



- **Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw)**




- **Dislozierung**
  **Viele Verbände des OrgBer Cyber/Informationsraum konzentrieren sich im Großraum BONN:** *(ca. 4000 Personen ziv /mil)*

  **BMVg Abt Cyber/IT II** **BONN**
  **Kommando CIR**
  **Kommando ITBw**

  **Zentr Cyber-Sicherheit** **EUSKIRCHEN**
  **Zentr Software Komp. Bw**
  **Zentr GEOBw**

  **Zentr Cyber-Operationen** **RHEINBACH**
  **BtrbZ IT-SysBw**
  **Kdo StratAufkl**

- **Zentrum Cyber-Sicherheit**
  Geplant sind weiterhin **Regionalzentren in den Standorten**
  **Nord-** **WILHELMSHAVEN**
  **West-** **KÖLN-WAHN und MÜNSTER**
  **Süd-** **ULM**
  **Ost-** **Berlin**

- **Personal**
  Das Personal für die neue Organisation wird vorrangig durch **Personal der bisherigen Struktur** gewonnen. Gleichzeitig wird auch Personal von **anderen Dienststellen** abgezogen sowie an den entsprechenden Schulen und **Ausbildungseinrichtungen** für die Verwendungen im neuen Organisationsbereich ausgebildet.
  **Die Neubesetzung wird sich insgesamt auf mehrere Jahre ausdehnen**.
  Durch informative Werbung und Vorstellung der technischen Möglichkeiten im Bereich des Kommandos Cyber/Informationsraum soll die Personalgewinnung unterstützt werden.

- **Hierzu wird auch ein neues Barett (Anthrazit) mit einem neuen Emblem eingeführt –**
  **Eichenblattkranz mit** einem zentralen **Weltkugelsymbol** (GeoInfo-Unterstützung, weltweite Aufklärung sowie Internet mit globaler Vernetzung des Cyber- und Informationsraums),
  einem **Schild mit den Initialen „CIR“** (Schutz des Operationsraumes) und einem
  das Ganze **überlagernd** mit einem **entgegen gerichtetem Pfeilsymbol** (Überwachung und Aufklärung im Cyber- und Informationsraum) für die
  **Angehörigen des 6. Militärischen Organisationsbereiches – Cyber und Informationsraum Bw -**
  neben Heer – Marine – Luftwaffe – Streitkräftebasis und Zentraler Sanitätsdienst -

---

**Herr Oberst G. Weiß beendete seinen Vortrag mit einer kurzen Zusammenfassung und stellt sich anschließend Fragen aus dem Teilnehmerkreis.**

---

**Abschließend bedankte sich Herr Oberst a.D. Siegel bei Herrn Oberst Weiß für die hervorragend dargebrachten, ausführlichen Informationen und wünschte Glück für die Tätigkeit im neu gegliederten Dienstbereich, gab einen Hinweis auf die nächste Veranstaltung, 20. Mai 2017, 13:00 – 20:00 Uhr, Besuch der Genovevaburg und des Schiefermuseums MAYEN (Leitung Herr OStFw a.D. Sikorski),**
**und lud danach zu einem Gedankenaustausch mit geselligen Zusammensein und Veranstaltungs-ausklang ein.**

Die Sicherheitspolitische Informationsveranstaltung wurde gegen 20:30 offiziell beendet.

*11.02.2017, KdFm-SchrFhr, D. Clausen, Hptm.a.D.*