



- bundeswehr.de ·

Sie sind hier: [Startseite](#) > [Service](#) > [Archiv](#) > [2018](#) > [April](#) > Zentrum Cyber-Operationen offiziell in Dienst gestellt

Zentrum Cyber-Operationen offiziell in Dienst gestellt

„Nach vielen Jahren, in denen vergleichbare Appelle oft anlässlich der Außerdienststellung von Einheiten und Verbänden gewohnter Alltag waren, stellen wir hier und heute eine neue Dienststelle auf – das Zentrum Cyber-Operationen“, so Generalmajor Axel Binder, Kommandeur des Kommandos Strategische Aufklärung, Anfang April in Grafschaft beim Aufstellungsappell des neuen Zentrums im Organisationsbereich Cyber- und Informationsraum.



Der angetretene Ehrenzug (Quelle: PIZ CIR/Pump)[Größere Abbildung anzeigen](#)

Bei der Aufstellung des Zentrums handelt es sich um einen weiteren bedeutenden Schritt für den jüngsten Organisationsbereich der Bundeswehr. 100 Soldaten und zivile Mitarbeiter, die zuvor ihren Dienst in der ehemaligen Abteilung Computer Netzwerk Operationen im Kommando Strategische Aufklärung leisteten, bekamen mit dem neugegründeten Zentrum in Gegenwart des Inspektors des Organisationsbereiches Cyber- und Informationsraum, Generalleutnant Ludwig Leinhos, nun eine neue militärische Heimat. Dort werden die Fähigkeiten der militärischen Computernetzwerkoperationen nun zentral gebündelt, gestärkt und künftig weiter ausbaut. Ziel ist, noch handlungsfähiger im Cyber- und Informationsraum zu werden, einen besseren Beitrag zu einer gemeinsamen Cyber-Lage zu leisten und zur Stärkung des Schutzes eigener Netze und Waffensysteme beizutragen. *„Damit ist heute die Geburtsstunde eines maßgeblichen Fähigkeitsbausteins für die Aufklärung und Wirkung in der Dimension Cyber- und Informationsraum“*, so Binder weiter.

http

Vielfältiges Aufgabenfeld

Das Zentrum Cyber-Operationen stellt künftig die offensiven Cyber-Kräfte der Bundeswehr. Die Angehörigen des Zentrums planen und bereiten militärische Computernetzwerkoperationen für den Verteidigungsfall sowie mandatierte Einsätze der Bundeswehr aus ortsfesten und mobilen Anlagen vor und führen diese – wenn die rechtlichen Voraussetzungen gegeben sind – auch aus. Grundlage für die eigentliche Arbeit der Mitarbeiter des Zentrums ist dabei ein klares Lagebild. Um dieses zu erzeugen, müssen Netzwerke und Kommunikationsbeziehungen aufgeklärt und analysiert werden. Dabei werden Daten insbesondere hinsichtlich eingesetzter Hard- und Softwareprodukte ausgewertet. Zudem sollen mögliche Netzwerkschwachstellen identifiziert werden. Diese Informationen werden dann mit Erkenntnissen anderer Netzwerkanalysen korreliert, um Handlungsoptionen ableiten zu können.

Red Teaming

MV8t5EE63



Die Cyber-Kräfte der Bundeswehr (Quelle: PIZ CIR/Pump)[Größere Abbildung anzeigen](#)

Zusätzlich werden die Angehörigen des Zentrums mit der Fähigkeit Red-Teaming künftig zur wirkungsvollen Unterstützung des Zentrums Cybersicherheit der Bundeswehr und der Truppe im Rahmen von Übungen beitragen. Mittels Red-Teaming soll ein unerlaubtes Eindringen in die Netzwerkstruktur von außen simuliert werden, um Schwachstellen in Netzwerken von Dienststellen der Bundeswehr zu identifizieren. Die aus Sicht eines „Angreifers“ gewonnenen Erkenntnisse hinsichtlich Erkennungs- und Reaktionsfähigkeit tragen dann zum einen zur Verbesserung des Schutzes in Netzwerken von Dienststellen bei. Sie sind aber auch ständiger „Übungsplatz“ für die eigenen aktiven Fähigkeiten und deren Weiterentwicklung.

Intensive Ausbildung

Um diese vielfältigen Aufgaben bewältigen zu können braucht es vor allem gut ausgebildetes Personal. *„Die Verfügbarkeit von Dienstposten ist sicherlich eine wichtige Voraussetzung, aber wichtiger sind qualifizierte Menschen, die diese Dienstposten besetzen und mit Leben füllen“*, so Binder bei seiner Rede während des Appells. Dabei ist der Weg in das Zentrum Cyber-Operationen sowohl für Feldweibel als auch Offiziere von intensiver Ausbildung gekennzeichnet. Auf eine Ausbildung zum IT-Administrator und den entsprechenden Feldweibel-Fachlehrgang beziehungsweise ein akademisches Studium, schwerpunktmäßig in den Bereichen Informatik und Elektrotechnik, folgt eine Eignungsfeststellung. Bei dieser müssen die Bewerber bereits grundlegendes Verständnis und erste Kenntnisse und Fähigkeiten im Bereich der Cyberoperationen nachweisen. Erst nach diesem Test, schließt sich eine 13-wöchige Fachausbildung Computernetzwerkoperationen an. Diese umfasst unter anderem rechtliche Aspekte, Programmiersprachen und Verfahren der Informationsgewinnung. Ist auch dieser Teil der Ausbildung erfolgreich absolviert, können die IT-Spezialisten im Zentrum Cyber-Operationen eingesetzt werden und Ihren Teil zur Verteidigung Deutschlands im Cyber- und Informationsraum leisten.

Weiterer Aufbau



Generalmajor Binder übergibt Oberst Pawlik die Truppenfahne des ZCO (Quelle: PIZ CIR/Pump)[Größere Abbildung anzeigen](#)

Mit der ersten Aufstellung ist jedoch noch nicht die endgültige Struktur des Zentrums erreicht. *„Es ist bereits heute absehbar, dass wir das Zentrum Cyber-Operationen entsprechend seiner Bedeutung weiter entwickeln und weiter ausbauen werden“*, so Binder.

• INHALT DES ARTIKELS

- ↗ [Vielfältiges Aufgabenfeld](#)
- ↗ [Red Teaming](#)
- ↗ [Intensive Ausbildung](#)

[↗ Weiterer Aufbau](#)

• WEITERE BEITRÄGE



- [Die Bedrohung aus dem Cyber-Raum für die Bundeswehr bleibt konkret.](#)
- [Interview Inspekteur Cyber- und Informationsraum: Ein Jahr Kommando Cyber- und Informationsraum](#)
- [Verantwortungsvolle Aufgabe - neuer Stellvertretender Inspekteur Cyber- und Informationsraum](#)

- **WEITERE INFORMATIONEN**
- [Kommando Strategische Aufklärung](#)

Stand vom: 18.04.18 | Autor: [Fritz Kessel](#)

[http://cir.bundeswehr.de/portal/poc/cir?](http://cir.bundeswehr.de/portal/poc/cir?uri=ci%3Abw.cir.service.archiv.2018.april&de.conet.contentintegrator.portlet.current.id=01DB16000000001%7CAXXCJH553DIBR)

[uri=ci%3Abw.cir.service.archiv.2018.april&de.conet.contentintegrator.portlet.current.id=01DB16000000001%7CAXXCJH553DIBR](http://cir.bundeswehr.de/portal/poc/cir?uri=ci%3Abw.cir.service.archiv.2018.april&de.conet.contentintegrator.portlet.current.id=01DB16000000001%7CAXXCJH553DIBR)