



Fighting  
hackers.

## Anerkennung der Ausbildung

Nach Abschluss des Lehrgangs kann die Berufsprüfung zum «Cyber Security Specialist» mit eidgenössischem Fachausweis abgelegt werden.

Die akademische Anerkennung des Lehrgangs mittels ECTS-Punkten ist zurzeit in Abklärung.

Die in der Weiterbildung zum Wachtmeister absolvierte Führungsausbildung kann ebenfalls mit einer zivil anerkannten Bescheinigung abgeschlossen werden.



# Cyber-Lehrgang

## Kontakt

Schweizer Armee  
Führungsunterstützungsbasis  
[info.fub@vtg.admin.ch](mailto:info.fub@vtg.admin.ch)  
[www.cyberdefence.ch](http://www.cyberdefence.ch)



## Allgemeine Ziele

Die Armee muss jederzeit – im Alltag wie in der Krise – ihre eigenen Informations- und Kommunikationssysteme und -infrastrukturen vor Angriffen schützen und Cyber-Angriffe abwehren können. Dazu setzt sie Teile der Berufsorganisation der Führungsunterstützungsbasis (FUB) ein, welche durch Milizangehörige der Armee unterstützt werden.

Das bereits etablierte und bewährte Vorgehen ist aufgrund der sich abzeichnenden Bedrohungsentwicklung nicht mehr ausreichend; es braucht mehr gut ausgebildetes Personal. Der Cyber-Lehrgang deckt eines der vielen Elemente des gesamten Ausbildungsplans im VBS ab.

## Selektion

Spezifische Zulassungsbedingungen sind für den Cyber-Lehrgang mit seinen 800 Unterrichts- und Praktikumsstunden zwingend:

- Dienstauglichkeit
- geeignete Persönlichkeit (belastbar, überdurchschnittliche Auffassungsgabe, verschwiegen, verantwortungsbewusst)
- Bereitschaft zur Weiterausbildung zum Wachtmeister
- bestandene erweiterte Personensicherheitsprüfung

Folgende Kandidaten werden akzeptiert:

- Personen mit abgeschlossener Berufslehre als Informatiker/-in EFZ, Mediamatiker/-in EFZ, ICT-Fachfrau/ICT-Fachmann EFZ
- Maturanden mit Schwerpunkt in naturwissenschaftlichen Fächern
- Studenten (ETH, Uni, FH) mit Fachrichtungen Informatik, Physik, Mathematik, Elektrotechnik, Automation oder/und Pädagogik
- Personen, welche sich autodidaktisch umfassende Kenntnisse angeeignet haben

## Ausbildungsbereiche und Inhalte

### Spezialist CNO

Computer Network Operations (CNO) mit Aufgaben u. a. als Entwickler von Softwarewerkzeugen, Analyst von Cyber Ereignissen und Attacken sowie Analyst von Schwachstellen.

### Spezialist milCERT

Spezialist milCERT mit Aufgaben u. a. als Analyst in einem Security Operation Center (SOC) mit Analysen von Cyber-Bedrohungen auf die Informatik- und Kommunikationstechnik Systeme der Armee, Incident-management sowie technische und forensische Untersuchungen.

### Spezialist Cyber Defence

Spezialist im Rahmen Cyber Defence mit Aufgaben u. a. in der Lage-Analyse und -Darstellung, zur Unterstützung (auch technisch/forensisch), Beratung und Ausbildung von Truppen im Feld.

## Durchführung des Lehrganges

Im Sommer 2018 findet der Pilot-Lehrgang statt; rund ein gutes Dutzend Rekruten soll dabei ausgebildet und diplomiert werden. Ab dem Frühling 2019 wird der Lehrgang 2 Mal jährlich durchgeführt.

Cyber-Lehrgang (40 Wochen)				
EKF RS 64-2/18			EKF UOS	EKF RS 64-1/19
AGA * 6 Wochen	FGA 7 Wochen	VBA 5 Wochen	UOS 4 Wochen	Praktischer Dienst als Wachtmeister 18 Wochen
Folgender Lehrgang			AGA * 6 Wochen	FGA 7 Wochen
			VBA 5 Wochen	UOS 4 Wochen
			Praktischer Dienst als Wachtmeister 18 Wochen	

Fachausbildung Cyber-Lehrgang	
Allgemeine Grundlagen	60 h
Technische Grundlagen	170 h
Querschnittsausbildung	30 h
Führungsausbildung	90 h
Fachausbildung	300 h
Einsatz und Übungen	150 h
<b>Total Ausbildungsstunden</b>	<b>800 h</b>

AGA = Allgemeine Grundausbildung, FGA = Funktionsgrundausbildung, VBA = Verbandsausbildung, UOS = Unteroffizierschule, EKF = Elektronische Kriegführung

\* Die AGA wird in der Schule abgeschlossen, durch welche das Aufgebot für die RS erfolgte. Der Übertritt in die EKF RS 64 bzw. in den Cyber-Lehrgang erfolgt per Ende AGA (nach bestandener Selektion).