Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 189 (2023)

Heft: 7

Artikel: Russische elektronische Kriegsführung in der Ukraine

Autor: Gubler, Hans Peter

DOI: https://doi.org/10.5169/seals-1052757

Russische elektronische Kriegsführung in der Ukraine

Bei den russischen Streitkräften hat in den letzten Jahren eine starke Aufrüstung stattgefunden. Beim Angriffskrieg gegen die Ukraine kann Russland seine vermeintliche Stärke im elektronischen Spektrum nur teilweise unter Beweis stellen.

Hans Peter Gubler

Gemäss russischer Doktrin hat die elektronische Kriegsführung zum Ziel, die gegnerische Führung zu desorganisieren, den Einsatz respektive die Wirksamkeit der feindlichen Aufklärung zu verhindern oder mindestens einzuschränken und dadurch optimale Voraussetzungen für den Einsatz eigener Kampfmittel zu schaffen. Seit Russland im Jahre 2014 die Krim annektierte und die Separatisten im Donbass militärisch unterstützt, sind die Truppen im Zentralen Militärbezirk mit einer breiten Palette von EKF-Technologien ausgestattet worden. Zudem wurde die Zahl der EKF-Verbände und -Einheiten in dieser Region vergrössert. Aus diesem Grunde waren westliche Nachrichtendienste zu Beginn des Angriffskrieges gegen die Ukraine im Februar 2022 davon ausgegangen, dass die russische EKF schwerwiegende Auswirkungen auf die Einsatzbereitschaft der ukrainischen Truppen haben könnte. Doch diese Vorhersagen hatten sich wie auch die generelle Schlagkraft der russischen Kampftruppen nicht bewahrheitet.

Grossteil der EKF-Brigaden im Einsatz

Die russische Armee setzt ihre EKF-Mittel auf strategischer, operativer und taktischer Ebene ein. Die EKF-Brigaden sind unabhängige Armeeverbände, die in ihrem übergeordneten Militärbezirk für die elektronische Kriegsführung im operativ-strategischen Bereich eingesetzt werden. Divisionen und Kampfbrigaden verfügen über taktische EKF-Bataillone oder haben einzelne EKF-Kompanien zugeteilt. Mindestens drei der total fünf russischen EKF-Brigaden sollen in den letzten Monaten unmittelbar für den Krieg gegen die Ukraine im Einsatz gestanden haben oder sollen noch im Einsatz stehen.

Die von Russland eingesetzte EKF-Technologie ist in der Ukraine primär auf die Störung, Lokalisierung und Täuschung von Kommunikationsmitteln sowie auch von Navigations-, Lenk- und Leitsystemen ausgerichtet. Sie wird vor allem gegen gegnerische Führungs- und Aufklärungsorgane, Einsatzmittel der Kampftruppen, gegen Luftfahrzeuge inklusive Drohnen sowie gegen Lenkwaffen und gelenkte Munition eingesetzt.

Himars im Visier

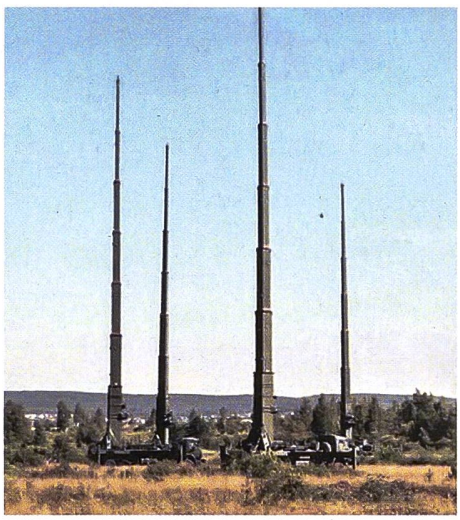
Gemäss einem RUSI-Bericht sollen die russischen Streitkräfte unterdessen entlang der über 1000 km langen Frontlinie in Abständen von 12 bis 15 km EKF-Stationen stationiert haben. Diese unterschiedlichen Systeme sollen 10 bis 15 km von der Front entfernt stationiert sein und ihre Standorte laufend wechseln.

Gemäss Berichten der CNN soll Russland in den letzten Monaten vermehrt versuchen, die Wirkung der von den USA gelieferten mobilen Raketenwerfer Himars zu beeinträchtigen. Immer häufiger werden die GPS-gesteuerten Zielsuchsysteme der Raketen durch russische EKF-Mittel gestört und negativ beeinflusst, sodass diese ihre Ziele teilweise verfehlen.

Erkannte russische EKF-Mittel

Laut einem vom russischen Verteidigungsministerium im Internet veröffentlichten Video, verwenden die russischen Streitkräfte in der Ukraine unterdessen ihre neusten Systeme der elektronischen Kriegsführung.

Die fahrzeuggestützte Breitband-Störstation Krasukha-4. Bild: russian mil. Photos



▲ **Antennen des strategischen Störkomplexes Murmansk-BN.** Bild: army recognition

► **Eine Störstation R-934 UM des EKF-Komplexes Borisoglebsk-2.** Bild: russian mil. Photos

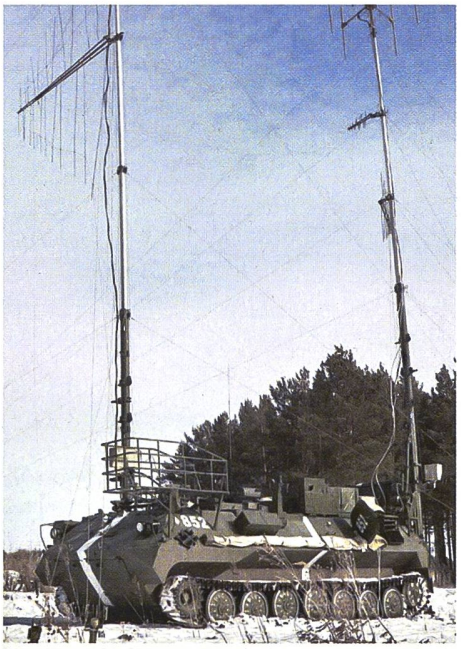
▲ Eine mobile Störstation Krasukha-2.
Bild: russian mil. Photos

◀ Ein Schützenpanzer MT-LBU mit einer Störstation des Borisoglebsk-2-Komplexes.
Bild: Photos Sputinik

Das mobile SIGINT-System Zhitel.
Bild: russian mil. Photos

Erwähnt werden die leistungsfähigen elektronischen Störsysteme Murmansk-BN und Krasukha-4, die gemäss russischen Angaben mit Erfolg bei den laufenden Operationen in der Ukraine eingesetzt worden sind. Von anderen Quellen erwähnt wird auch der Einsatz mobiler russischer EKF-Systeme Borisoglebsk-2, von elektronischen Störmitteln Zhitel und Sinitsa sowie von Funkaufklärungssystemen Torn.

Der strategische Störkomplex Murmansk BN wurde von der russischen Firma Kret entwickelt. Das System kann Kommunikationsstörungen über grosse Entfernungen durchführen und wird als Teil eines russischen strategischen, elektronischen Kriegsführungssystems bezeichnet. Laut russischen Militärquellen soll die maximale Reichweite 5000 bis 8000 km betragen. Die Hauptaufgabe des Systems besteht darin, Hochfrequenzübertragungen (HF) von NATO-Streitkräften zu kontrollieren und hochfrequente militärische Satellitenkommunikation zu stören.



Ein Murmansk-BN-Komplex besteht aus verschiedenen Fahrzeugen auf der Basis von Geländelastwagen, inklusive Gruppen von bis zu vier ausfahrbaren Antennenmasten. Die Masten können bis zu einer maximalen Höhe von 32 Metern ausgefahren werden. Jeder vollständige Murmansk-BN-Komplex hat normalerweise vier dieser Antennengruppen, was insgesamt 16 Antennen ergibt. Ein erweiterter Komplex dieses strategischen EKF-Systems wurde bereits vor Beginn des Angriffskrieges gegen die Ukraine auf der Krim, vermutlich in der Nähe von Sewastopol, stationiert und soll dort immer noch im Einsatz stehen.

Breite Einsatzpalette

Vom mobilen bodengestützten EKF-System Krasukha sind verschiedene Typenversionen vorhanden, die in den russischen Streitkräften für mehrere Aufgaben eingesetzt werden. Im Krieg gegen die Ukraine wird das Störsystem Krasukha-4 von den russischen Truppen gegen Funk- und Radarsysteme gegnerischer Aufklärungs- und Führungsmittel, gegen Lenksysteme feindlicher Drohnen und zur Störung gelenkter Munitionstypen eingesetzt. Die maximale Reichweite der Krasukha-Systeme soll bei etwa 300 km liegen. Krasukha-4 ist ein multifunktionales Breitbandstörsystem, das auf einem vierachsigen Geländelastwagen montiert ist. Es soll im Ukraine-Krieg ergänzend zu den etwas älteren Krasukha-2-Systemen eingesetzt werden.

Zusätzlich zu den Krasukha-Stationen stehen auf der taktischen Ebene auch die automatischen Störstationen Zhitel im Einsatz. Diese sollen vor allem Radarsignale von anfliegenden Luftfahrzeugen und Drohnen lokalisieren und dabei versuchen, deren Funkverbindungen auf grosse Entfernungen zu stören. Zhitel soll aber auch für die Erkennung, Analyse, Peilung und Störung von Satelliten- und Mobiltelefonkommunikationssystemen dienen, die im Frequenzbereich von 100 bis 2000 MHz betrieben werden.

Störer von Ukraine erbeutet

Im Herbst 2022 ist es den ukrainischen Truppen gelungen, ein taktisches EKF-System Borisoglebsk-2 zu erbeuten. Dieser mobile Mehrzweck-Störkomplex wird für SIGINT-Einsätze, vor allem aber für die Un-

◀ Die Drohnen Orlan-10 werden auch mit Störsendern Leer-3 eingesetzt.
Bild: russian min. of defense

terdrückung respektive Störung von HF/VHF/UHF-Frequenzen der boden- und luftgestützten Funk- und Satellitenkommunikation genutzt. Das Borisoglebsk-2-System besteht aus einem Kontrollposten und unterschiedlichen EKF-Systemen, die alle auf gepanzerten MT-LBU-Kettenfahrzeugen montiert sind.

Das russische Verteidigungsministerium hat kürzlich ein Video veröffentlicht, das den Betrieb des luftgestützten Störgeräts Leer-3 in der Ukraine zeigt. Das russische Video zeigt Aufklärungsdrohnen vom Typ Orlan-10, die für einen Einsatz mit diesen Störsendern vorbereitet werden. Der Leer-3 ist ein Kommunikationsstörgerät, das primär vorhandene Mobilfunknetze über längere Zeit stören kann. Die Reichweite der Störgeräte soll etwa 100 km betragen. Das Gerät blockiert den Betrieb aller Geräte in bestimmten Frequenzbändern, während die Mobilfunknetze aber nicht vollständig blockiert werden. Diese luftgestützten Störmittel können die Mobilfunkkommunikation der ukrainischen Armee über mehrere Stunden stören.

EKF-Systeme sind Primärziele für die ukrainische Artillerie

Bis zum Frühjahr 2022 ist man bei Militärexperten davon ausgegangen, dass die russischen Streitkräfte über erfahrene und mit modernen Mitteln ausgerüstete EKF-Einheiten verfügen. In den ersten Tagen der Invasion am 24. Februar erwarteten daher die westlichen Militäranalysten, dass Russland in der Ukraine relativ schnell die Kontrolle über das elektromagnetische Spektrum erlangen und dann auch dominieren würde.

Offensichtlich hatten aber die Russen ihre eigenen Fähigkeiten in diesem Bereich überschätzt und die diesbezüglichen Gegenmassnahmen der Ukraine unterschätzt. Zudem konnten die ukrainischen Truppen relativ rasch Gegenmassnahmen treffen und auch auf die Unterstützung durch die USA und NATO zählen. Dennoch lag der Misserfolg der russischen elektronischen Kriegsführung nicht primär an der Qualität und der Anzahl der technischen Systeme. Moskaus elektronische Offensive scheiterte im Prinzip aus den gleichen Gründen wie auch die Bodenoffensive. Schlechte Planung, mangelnde Koordination beim Einsatz der Mittel und eine allgemeine Gleichgültigkeit der russischen Kommandeure. Dennoch konnten die russischen Störsysteme im Verlaufe der letzten Monate gemäss NATO-Angaben eine bedeutende Zahl ukrainischer Drohnen ausschalten.

Die Einsatzmittel der russischen elektronischen Führungs- und EKF-Mittel sind im Verlaufe des Krieges immer mehr zu Primärzielen der ukrainischen Streitkräfte geworden. Vor allem die ukrainische Artillerie konzentrierte sich mit Priorität auf die Bekämpfung der meist aus mehreren Fahrzeugen und Antenneneinrichtungen bestehenden russischen Führungs- und EKF-Komplexe. Die USA und die NATO dürften dabei die Ukraine mit den benötigten Aufklärungsdaten unterstützen. Gemäss ukrainischen Meldungen wurden im bisherigen Verlauf der Kampfhandlungen diverse russische EKF-Systeme zerstört und auch erbeutet, wobei wichtige Hardwareteile für eigene Zwecke ausgewertet werden konnten. ■

Oberstleutnant a D
Hans Peter Gubler
3045 Meikirch

CYBER OBSERVER

Marc Ruef
Head of Research
scip AG

CH Media und die NZZ wurden Opfer einer Ransomware-Attacke. Der Betrieb wurde massgeblich gestört, was zwangsweise zu einem gewissen Medieninteresse geführt hat. Man ist der Erpressung scheinbar nicht nachgekommen, weshalb die Angreifer die erbeuteten Daten im Darknet veröffentlicht haben. Verschiedene Medien haben dazu berichtet.

Dies wäre nichts Ungewöhnliches. Nennenswert ist jedoch, dass CH Media und NZZ mittels superprovisorischer Verfügungen verschiedene Zeitungen dazu gedrängt haben, die Berichterstattung zu schwärzen.

Ich habe viel zu diesem Fall zu erzählen. Doch als der unterwürfige Kolumnist, der ich bin, zensiere ich meine Worte gleich selbst. Ich will nicht, dass die mediale Obrigkeit betupft ist und auf ihr Geheiss der Zorn von Justitia auf mich niederfährt. Wo kämen wir auch hin, wenn Journalisten einfach über Ereignisse berichten dürften? Hier meine Meinung:

[redacted]

ICT Berufsbildung

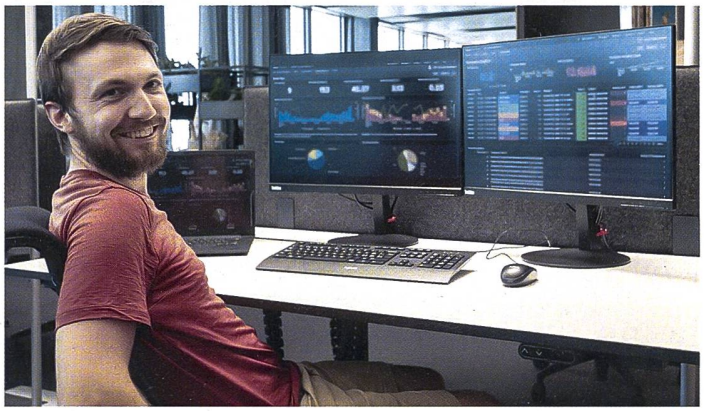
Cyber Security Specialist: mit Sicherheit zum beruflichen Erfolg

Fachkräfte im Bereich der Cyber Security sind gefragter denn je. Der eidgenössische Fachausweis Cyber Security Specialist sorgt für qualifizierten Nachwuchs und bietet Absolventinnen und Absolventen beste Zukunftsaussichten. Die Berufsprüfung kann im Anschluss an den Cyber-Lehrgang der Armee absolviert werden. Entwickelt wurde der Fachausweis von ICT-Berufsbildung Schweiz in Kooperation mit der Schweizer Armee und der Wirtschaft.

Die Nachfrage nach Fachkräften im Bereich der Cyber Security nimmt überdurchschnittlich zu: Bis ins Jahr 2030 werden 60 Prozent zusätzliche ICT-Security-Fachkräfte benötigt (IWSB 2022). Gleichzeitig kann ein Fachkräftemangel in diesem sensiblen Bereich äusserst unangenehme und weitreichende Folgen für Wirtschaft und Gesellschaft haben. Deshalb hat der nationale Verband ICT-Berufsbildung Schweiz gemeinsam mit der Schweizer Armee und Vertretenden der Wirtschaft den eidgenössischen Fachausweis Cyber Security Specialist entwickelt. Der Abschluss stösst auf grosses Interesse: Seit der Erstdurchführung im Jahr 2020 hat sich die Zahl der Prüfungskandidatinnen und -kandidaten vervierfacht.

Praktische Kompetenzen im Fokus

Cyber Security Specialists analysieren aktuelle Bedrohungslagen, decken Schwachstellen auf, leiten Schutzmassnahmen ein und wehren Angriffe gegen Informations- und Kommunikationssysteme ab. Diese Handlungskompetenzen stellen die Kandidierenden an der eidgenössischen Berufsprüfung in drei Teilen unter Beweis. In der praktischen Fallbearbeitung im «Hacking Lab» werden sie wirklichkeitsgetreuen Bedrohungslagen ausgesetzt. Dabei meistern sie anspruchsvolle, praktische Challenges in Bezug auf die Prävention, Erkennung und Bewältigung von Sicherheitsvorfällen. Der schriftliche Prüfungsteil beinhaltet Projektmanagement und berufsspezifische betriebswirtschaftliche Aspekte. Im dritten Teil werden in einer mündlichen Fallbearbeitung Kompetenzen in den Bereichen Teamführung und Kommunikation geprüft.



„ Der Cyber-Lehrgang der Armee ist eine gute Vorbereitung für den eidgenössischen Fachausweis Cyber Security Specialist. Für einige Arbeitgeber sind jedoch die zusätzlichen Kompetenzen von Bedeutung, die mit der eidgenössischen Berufsprüfung bestätigt werden. Sie erkennen daher erst den Fachausweis als funktions- und lohnrelevante Ausbildung an. "

Absolvent* des Cyber-Lehrgangs und Cyber Security Specialist mit eidgenössischem Fachausweis

Auf internationalem Anforderungsniveau eines Bachelors

Die eidgenössische Berufsprüfung wird zentralisiert von ICT-Berufsbildung Schweiz im Auftrag des Bundes durchgeführt. Gerade im sensiblen Bereich der Informations- und Cybersicherheit ist diese Trennung von Ausbildung und Prüfung ein Qualitätsmerkmal. Mit einer Einstufung im nationalen Qualifikationsrahmen (NQR) auf Niveau 6 befindet sich der Abschluss auf einem sehr hohen Level: im internationalen Vergleich entspricht dies dem Anforderungsniveau eines Bachelors. Dem NQR dient der Europäische Qualifikationsrahmen (EQR) als Referenzinstrument, somit können die Schweizer Abschlüsse mit denen anderer Länder verglichen werden.

Anrechnung des Cyber-Lehrgangs der Armee

Die Schweizer Armee bietet einen Cyber-Lehrgang an, welcher im Rahmen der Rekrutenschule absolviert werden kann. Absolventinnen und Absolventen dieses Lehrgangs mit mindestens einem Jahr Berufspraxis im Bereich der Informations- oder Cybersicherheit sind zur Berufsprüfung Cyber Security Specialist zugelassen. Zudem bereiten verschiedene Bildungspartner von ICT-Berufsbildung Schweiz interessierte Kandidatinnen und Kandidaten auf die eidgenössische Berufsprüfung vor.

Weitere Infos:
ict-berufsbildung.ch/css

* möchte aus berufsspezifischen Gründen anonym bleiben

Zukunftsaussichten von Cyber Security Specialists mit eidgenössischem Fachausweis:

- ICT Security Operations Manager
- ICT Security Incident Manager
- Cyber Security Engineer
- Zulassung zum eidg. Diplom ICT Security Expert (ict-berufsbildung.ch/sec)
- Zulassung oder Anrechnung für Studiengänge (BA/MA) oder Weiterbildungen (CAS/DAS/MAS) auf Hochschulstufe möglich (individuelle Abklärung mit der entsprechenden Bildungsinstitution empfohlen)

ICT Berufsbildung
Formation professionnelle
Formazione professionale