DGAPkompakt

Nr. 17 / Oktober 2019

Der vernetzte Krieg
Warum moderne Streitkräfte von elektronischer Kampfführung abhängen

Torben Schütz

Europas Armeen haben seit Ende des Kalten Krieges im digitalen Bereich nicht ausreichend modernisiert. Vor allem bei der immer bedeutender werdenden elektronischen Kampfführung wird diese Lücke deutlich. Länder wie China und Russland holen auf und zeigen die Schwächen westlicher Streitkräfte. Diese Fähigkeitslücke können EU- und NATO-Staaten nur gemeinsam schließen, um glaubhafte Abschreckung und Verteidigung sicherzustellen.

Elektronische Kampfführung – von der Überlegenheit in die Verwundbarkeit

Das zentrale Nervensystem moderner Streitkräfte liegt im sogenannten elektromagnetischen Spektrum (EMS). Hier finden sich neben Licht auch alle anderen elektromagnetischen Wellen, Infrarot, Radiowellen oder Radarwellen.

Die Kontrolle des EMS ist entscheidend für den Erfolg und die bisherige Überlegenheit vor allem westlicher Streitkräfte. Immer mehr Sensoren, Datenbanken und einzelne Waffen, aber auch militärische Einheiten sind über das EMS zu einem Netzwerk zusammengeschaltet. Diese Vernetzung erlaubt es, Informationen und Befehle an jeden angeschlossenen Teilnehmer zu senden. Dabei macht es keinen Unterschied mehr, ob sich Sender oder Empfänger zu Land, See, Luft, im Weltall oder im Cyberraum bewegen.

Vernetzung hat mehrere Folgen für Streitkräfte

Statt einzelnen Plattformen (z.B. Flugzeugen, Panzern oder unbemannten Systemen) wird deren Zusammenspiel in einem Netzwerk, in dem digitale Informationen geteilt werden, zum militärischen Zentrum. Wer mehr und bessere Informationen besitzt und diese mit möglichst vielen Plattformen teilt, kann gegnerische Kräfte schnellstmöglich und zielgenau bekämpfen.

Sie schaffen militärische Vorteile: Um einer gezielten und schnellen Bekämpfung durch gegnerische Kräfte zu entgehen oder um diese selbst anzugreifen, müssen Streitkräfte hochmobil oder in der Lage sein, ihre Gegner zu täuschen. Vernetzung ermöglicht beides: Einheiten werden dadurch kleiner, können entfernter voneinander operieren und unterschiedliche Missionen durchführen. So entstehen militärische Vorteile gegenüber nicht vernetzten Gegnern.

Ohne EMS ist kein erfolgreicher Einsatz von Streitkräften mehr denkbar. Mit der zunehmenden Digitalisierung wächst seine Bedeutung weiter. Ein Aussteigen aus der Digitalisierung bzw. ein technisches Hinterherhinken würde dem Gegenüber wachsende Vorteile verschaffen.

Elektronische Kampfführung – Schutz und Angriff im elektromagnetischen Spektrum

Mit der zunehmenden Bedeutung des EMS steigt auch die Notwendigkeit seiner Kontrolle. Ohne funktionierende Vernetzung können moderne Streitkräfte nicht operieren. Deshalb gibt es einen eigenen Bereich der Kampfführung im EMS, die elektronische Kampfführung (EloKa). Die EloKa soll die Nutzung des EMS für die eigenen und ver-

DGAP
Deutsche Gesellschaft
für Auswärtige Politik

bündeten Streitkräfte sicherstellen und sie zugleich dem Gegenüber verwehren. Dazu bedient sich die EloKa neben Maßnahmen zum Schutz und Angriff Methoden, die Erkennung, Tarnung, Täuschung, Störung und Degradation ermöglichen.

Aus Abhängigkeit wird Verwundbarkeit

Bis vor kurzem war die Überlegenheit westlicher Streitkräfte bei der Vernetzung unangefochten. Zudem stellte die Kontrolle des EMS keine große Herausforderung dar: Nach Ende des Kalten Krieges sank die Gefahr eines Krieges mit einem ähnlich gut gerüsteten Gegner wie dem Warschauer Pakt. Deshalb baute Europa seine EloKa-Fähigkeiten ab. Die wesentliche Aufgabe der verbleibenden EloKa-Verbände lag in zwei Nischen bei Auslandseinsätzen: Sie neutralisierten sogenannte Improvisierte Sprengsätze (Improvised Explosive Devices, IEDs) und orteten Gegner, die das EMS nutzten, etwa durch Mobiltelefone oder Funkgeräte.

Die konzeptionelle Umstellung der NATO von Auslandseinsätzen auf Bündnis- und Landesverteidigung seit 2014 veränderte die Anforderungen an EloKa erneut: Im Konflikt mit einem gut gerüsteten staatlichen Gegner führt die entstandene Abhängigkeit von der Vernetzung – und damit von der Kontrolle des EMS – zur erhöhten Verwundbarkeit. Die heute noch vorhandene Ausrüstung für zwischenstaatliche Konflikte ist wegen fehlender Modernisierung veraltet. Die europäischen Streitkräfte sind also einem Gegner unterlegen, der die heute verfügbaren technischen Möglichkeiten nutzt.

Diese Verwundbarkeit ist real: Russland hat seine Fähigkeiten in der elektronischen Kampfführung erheblich ausgebaut. Das hat schon in Friedenszeiten unmittelbare Folgen für westliche Streitkräfte: So hat Russland während der NATO-Übung „Trident Juncture“ in Nord-Norwegen im Jahr 2018 das Satellitennavigationssystem GPS in der Region aktiv gestört. Aber auch in Auslandseinsätzen spielt diese Verwundbarkeit eine Rolle. Deutsche Tornado-Aufklärungsflugzeuge fliegen ohne ernstzunehmenden Schutz oder Täuschmöglichkeiten gegen Luftabwehrsysteme im Rahmen des Anti-IS-Einsatzes.[1]

Rahmenbedingungen, um die Fähigkeitslücke zu schließen

Drei Rahmenbedingungen sind bei den Bemühungen zu berücksichtigen, Handlungsfähigkeit im Bereich der elektronischen Kampfführung wiederherzustellen – die Umstellung europäischer Streitkräfte auf Szenarien der Landes- und Bündnisverteidigung bildet den Hintergrund dafür. Diese Umstellung bedeutet erstens, sich auf konventionelle zwischenstaatliche Konflikte einzustellen bzw. diese durch Abschreckung zu vermeiden. Zweitens nehmen die Digitalisierung und Vernetzung von Streitkräften weiter zu. Bislang gibt es mit Blick auf Schutz und Angriff keine Alternativen, als an der Spitze der technologischen Entwicklungen zu stehen. Dieses Ziel bedeutet, drittens, die rasanten Fortschritte in den Bereichen Mikroelektronik, Materialwissenschaft und Softwareentwicklung für militärische Systeme zu adaptieren und solche zu beschaffen.

Zwischenstaatliche Konflikte als Planungsgrundlage

Seit 2014 fokussieren sich Bundeswehr und NATO wieder auf Abschreckung sowie Landes- und Bündnisverteidigung. Konkret stehen dabei derzeit große militärische Operationen im Mittelpunkt, die Russland davon abhalten, NATO-Staaten anzugreifen – oder wenn die Abschreckung fehlschlägt, diese Staaten zu verteidigen. Im Gegensatz zum Westen hat Russland in den letzten zehn Jahren massiv in EloKa-Fähigkeiten für zwischenstaatliche Konfrontationen investiert. Einige Beobachter attestieren den russischen Streitkräften daher sogar eine Überlegenheit in bestimmten EloKa-Bereichen.[2]

Aber auch jenseits Russlands rücken klassische Konflikte mit einem staatlichen Akteur wieder ins Zentrum der Planungen. In diesem Kontext ist elektronische Kampfführung eine elementare Fähigkeit. Verglichen mit nicht-staatlichen Gegnern in Auslandseinsätzen wie den Taliban oder Aufständischen in Mali haben staatliche Akteure wesentlich größere militärische und industrielle Fähigkeiten, um EloKa effektiv in ihre militärischen Operationen einzubinden. Westliche Streitkräfte müssen daher viel eher damit rechnen, dass EMS vom Gegner genutzt wird, um ihre Angriffe zu stören oder aufzuklären und die Kommunikation zu verfälschen.

Bereits heute schränken die EloKa-Fähigkeiten Russlands und Chinas die militärische Handlungsfähigkeit der westlichen Streitkräfte ein. Sogenannte Anti-Access/Area-Denial-Zonen (A2/AD) entstehen durch das Zusammenspiel verschiedener Elemente: Dazu zählen zielgenaue ballistische Raketen und Marschflugkörper für die Bekämpfung von Landzielen sowie dichte und integrierte Luftverteidigungsnetze und eine große Anzahl an Kampfflugzeugen mit modernen Luft-Luft-Raketen, die den Luftraum sichern. Daneben sichern Aufklärungssysteme mit Echtzeitübertragung und redundante Kommando- und Führungseinrichtungen die eigenen Führungsfähigkeiten. EloKa-Fähigkeiten, Anti-Satellitenwaffen sowie Cyberkräfte sollen derweil die Führungsfähigkeiten des Gegners einschränken und ihn damit lähmen.

Solche A2/AD-Zonen können Operationen von Streitkräften in größeren Regionen erschweren, wie zum Beispiel den Transport von Nachschub und Truppen ins Baltikum. Sie erlauben auch, mit ihren Verteidigungsfähigkeiten eigene offensive militärische Operationen abzuschirmen: EloKa-Systeme spannen einen elektromagnetischen Schirm auf, der es dem Gegner erheblich erschwert, Bewegungen und Aktivitäten eines Angreifers zu erkennen. Denkbar sind z.B. im europäischen Kontext abgeschirmte russische Operationen im Baltikum, in der Arktis oder im Schwarzen Meer. Auch die Bundeswehr hat diese Bedrohung erkannt: Sie verweist in der „Konzeption der Bundeswehr" von Juli 2018[3] explizit auf die sicherheitspolitische Herausforderung von A2/AD-Zonen. Eine glaubhafte Abschreckung und Rückversicherung von NATO- und EU-Partnern setzt die Fähigkeit voraus, A2/AD-Zonen zu überwinden. Diese braucht Deutschland, um Verbündeten, die sich innerhalb der Reichweite von A2/AD-Zonen befinden, glaubhaft versichern zu können, dass es ihnen im Falle eines Angriffs hilft.

Digitalisierung und Vernetzung militärischer Einheiten

Die zunehmende Digitalisierung und Vernetzung von militärischen Einheiten soll vor allem die Effizienz steigern: Neben den Routinearbeiten im Frieden gilt es vor allem, die Kette von Informationssammlung, Entscheidung und Einsatz so kurz wie möglich zu halten. Gleichzeitig sollen so viele Informationen wie möglich über ein Redundanz schaffendes Netzwerk transportiert werden. Diese Anforderungen verschieben den Fokus von einzelnen Plattformen (z.B. Flugzeugen, Panzern oder unbemannten Systemen) auf das Zusammenspiel von Plattformen in einem Netzwerk. Innerhalb dieses Netzwerks werden Informationen geteilt. Damit kann schnell und effektiv entschieden werden, welche Plattformen welche Aufgaben übernehmen. Zudem ermöglicht das Netzwerk, dass Kommandierende jederzeit eine Übersicht über die militärische Operation haben.

Die Effektivität der US-Truppen im Golfkrieg 1991 hat deutlich gemacht, wie groß der militärische Vorteil eines solchen Netzwerks von Plattformen sein kann. Deshalb treiben seither nicht nur westliche Armeen die Digitalisierung von Plattformen und Führungsfähigkeiten voran, sondern auch Russland und China.

Diese digitale Verknüpfung schafft aber auch Schwachstellen: Jeder Knotenpunkt des Netzwerkes (Plattform oder Soldat) oder ihre Verbindungen untereinander können angegriffen, abgehört oder gestört werden. Wenn ein Gegner es schafft, die Verbindungen zu stören, sind die Plattformen und Soldaten „blind und taub". Dann sind sie leicht angreifbar oder zumindest unfähig, koordiniert zu operieren. Heute halten westliche Streitkräfte weder das Monopol auf netzwerkzentrierte Kriegsführung noch die technischen Grundlagen für diese Art der Kriegsführung.

Technischer Fortschritt in Hard- und Software

Neben der Vernetzung zur Kommunikation wird das EMS auch genutzt, um feindliche Kräfte zu identifizieren und zu lokalisieren. Sowohl Hardware als auch Software, die in der EloKa zum Einsatz kommen, profitieren vom anhaltenden Fortschritt in der zivilen Mikroelektronik und Software-Entwicklung. Die Miniaturisierung und zunehmende Leistungsfähigkeit digitaler Hardware-Komponenten wie Prozessoren führt zu einem immer kleineren und leistungsfähigeren EloKa-Equipment. Beides verändert die Bedingungen unter denen Konzeption, Beschaffung und Ausbildung von EloKa-Fähigkeiten stattfinden.

Auf Grundlage dieser Entwicklungen bieten passive oder energiearme Sensoren heute eine wesentlich erhöhte Leistungsfähigkeit gegenüber ihren Vorgängern. Sie senden keine oder nur sehr schwache Signale aus, sind aber damit in der Lage, das EMS zu „lesen" und so Ziele zu finden, z.B. Flugzeuge. Auch aktive (sendende) Störmaßnahmen profitieren vom Fortschritt. Sie sind nun in der Lage, andere aktive Signale, z.B. von Flugabwehrradaren, in Echtzeit auszuwerten und zu stören. Vormals erforderte dies die genaue Kenntnis der elektromagnetischen Signatur des Senders. Passive und kleine Sensoren ermöglichen den Aufbau von Sensornetzwerken, die auf viele Plattformen verteilt sind. Ältere EloKa-Systeme sind häufig auf einer Plattform konzentriert, was eine Verwundbarkeit für alle beteiligten Truppen schafft, sobald diese zerstört ist. Technischer Fortschritt schafft hier die Möglichkeit für eine neue Art der „verteilten" elektronischen Kampfführung, in der sich viele Sensoren auf verschiedenen Plattformen befinden. Diese erstellen gemeinsam ein Lagebild. Gleichzeitig erhöht das aber die Wichtigkeit der sicheren Kommunikation der Plattformen untereinander.

Leistungsfähigere Hardware schafft zudem die Voraussetzungen, leistungsfähigere Software nutzen zu können. Um eine kognitive Überlastung der Soldaten, die das EloKa-System bedienen, in einem immer komplexeren elektromagnetischen Umfeld zu vermeiden, ist unterstützende Software notwendig. Nur durch software-basierte Vorarbeiten ist die Entscheidungsfähigkeit dieser Bediener möglich. Automatisierung von EloKa-Systemen ist deshalb ein Bereich, in dem sowohl Industrie als auch z.B. das US-Militär intensive Forschung durchführen.

Da kommerzielle Innovationen die Entwicklung von mikroelektronischen Komponenten und leistungsfähiger

Software treiben, werden Innovationszyklen in der EloKa immer kürzer. Lebenszyklen von früheren EloKa-Großsystemen von 20 Jahren und mehr sind heute auf wenige Jahre geschrumpft. Diese Veränderung beeinträchtigt die Streitkräfteplanungen bei der Beschaffung und Ausbildung und erfordert Reformen in beiden Bereichen.

Die Größe der Fähigkeitslücke – eine erste Annäherung

Für Deutschland und Europa sind Fähigkeiten zur elektronischen Kampfführung unerlässlich, um glaubwürdige Abschreckungs- und Bekämpfungsoptionen zu haben.

Zwar ist Europa technologisch und industriell in der Lage, diese Fähigkeiten bereitzustellen. In den Streitkräften aber sind sie teilweise abgebaut worden. Will Europa den Herausforderungen einer veränderten Sicherheits- und Technologielandschaft begegnen, dann muss es den Fähigkeitsabbau der letzten Jahre stoppen, bestehende Systeme ersetzen oder modernisieren und enger kooperieren. Da zivile Innovationszyklen den technischen Fortschritt bestimmen und neue Lösungen für alte Probleme bieten, reicht es nicht, bestehende Fähigkeiten zu erhalten. Eine umfassende Modernisierung benötigt auch Investitionen in die Forschung und Entwicklung neuer Herangehensweisen und Systeme.

Vorhandene militärische Fähigkeiten

EloKa-Fähigkeiten wurden in den vergangenen Jahren und Jahrzehnten in westlichen Streitkräften quantitativ bestenfalls gehalten oder abgebaut. Zudem ist das in Tabelle 1 aufgeführte Material in wenigen Staaten konzentriert. Diese stellen damit einen überproportional hohen Anteil in der EU und NATO.[4]

Tabelle 1: Vorhandenes europäisches EloKa-Gerät im Zeitvergleich 2008-2018

Domäne	Vorhandenes Gerät in Europa (EU und europäische NATO)		Änderung in Prozent
	2008	2018	Seit 2008
Luft	**69** Flugzeuge (in acht Staaten)	**51** Flugzeuge (in neun Staaten)	**-26%**
See	**10** Aufklärungsschiffe (in sieben Staaten)	**10** Aufklärungsschiffe (in sieben Staaten)	**0%**

Quelle: International Institute for Strategic Studies – Military Balance 2009 und 2019

Die Staaten der NATO- und der EU haben zwischen 2008 und 2018 die Anzahl der für EloKa-Aufgaben zur Verfügung stehenden Flugzeuge um rund ein Viertel (26 Prozent) reduziert. Der Abbau von Fähigkeiten steht in Widerspruch zu den steigenden Herausforderungen für zukünftige Luftoperationen. Aufgrund dieser Reduktionen sind luftgestützte EloKa-Fähigkeiten heute[5] in Europa kritisch, d.h. nur in geringen Mengen vorhanden und in wenigen Staaten verfügbar. Zudem sind sie oftmals stark veraltet.

Bei einem Blick in die Unterbereiche dieser Fähigkeiten wird die geringe Verfügbarkeit noch deutlicher: Spezielle EloKa-Fähigkeiten für Luftoperationen teilen sich in drei Bereiche: die Unterdrückung und Bekämpfung feindlicher Flugabwehr, die Aufklärung elektronischer Signale ohne Kommunikationsinhalt sowie die Aufklärung elektronischer Kommunikation. In der NATO haben nur Deutschland, Italien und die USA die Fähigkeit, die gegnerische Flugabwehr durch spezialisierte Flugzeuge mit Anti-Radar-Luft-Boden-Raketen zu umgehen. Sowohl Deutschland als auch Italien nutzen dazu die veralteten „Tornado“-Kampfbomber. Das Unterdrücken oder Zerstören feindlicher Flugabwehr stellt eine der ersten Aktivitäten offensiver Operationen dar. Die Befähigung dazu ist also für Interventionen oder Gegenoffensiven nach einer gegnerischen Aggression kritisch. Auch in den anderen Bereichen der EloKa sieht es nicht besser aus: Flugzeuge zur elektronischen Aufklärung (ELINT, elektronische Signale ohne Kommunikationsinhalt) stehen nur in fünf Staaten zur Verfügung (Finnland, Frankreich, Großbritannien, Schweden, USA); Flugzeuge zur Signalaufklärung (SIGINT) nur in Italien, Großbritannien und den USA.

Maritime EloKa-Fähigkeiten in Form von SIGINT durch Flottendienstboote führen sieben europäische Staaten mit insgesamt zehn Schiffen. Die Hauptaufgabe dieser Schiffe ist die Aufklärung und Auswertung von Signalen im EMS, seien es gefunkte Nachrichten oder elektromagnetische Spezifika von gegnerischen Radarsystemen. Zudem können sie über charakteristische elektronische Signale z.B. Truppenbewegungen verfolgen. Die europäischen Flottendienstboote waren aufgrund dieser Eigenschaften in den vergangenen Jahren öfter vor den Küsten der Ukraine oder Syriens im Einsatz. Bei den Einsätzen handelte es sich in den allermeisten Fällen um dieselben Schiffe wie 2008, die damit zumindest teilweise veraltet sind. Viele nähern sich dem Ende ihrer Lebenszeit und werden mittelfristig ersetzt werden müssen.

Im internationalen Vergleich liegen die Europäer in Bezug auf das verfügbare Gerät ungefähr auf Augenhöhe mit Russland. Allerdings ist zu berücksichtigen, dass die Vielzahl unterschiedlicher Typen, Prozesse und Ausbildungen die reale militärische Effektivität im Vergleich mit den russischen Truppen wahrscheinlich negativ beeinträchtigt.

Tabelle 2: Vorhandenes europäisches EloKa-Gerät im internationalen Vergleich

Domäne	Vorhandenes Gerät 2018		
	Europa*	USA	Russland
Luft	**51** Flugzeuge (in neun Staaten)	**185** Flugzeuge	**38** Flugzeuge **35** Helikopter
See	**10** Aufklärungsschiffe (in sieben Staaten)	**Keine** (EloKa-Ausrüstung nur auf Kampfschiffen)	**14** Schiffe

*EU und europäische NATO
Quelle: International Institute for Strategic Studies – Military Balance 2009 und 2019

Deutschlands Rolle und Europas Fähigkeit zu elektronischer Kampfführung

Die Bundeswehr hat sich der Herausforderung gestellt, für konventionelle zwischenstaatliche Konflikte zu planen. Moderne und einem möglichen Gegner angemessene EloKa-Fähigkeiten sind das zentrale Rückgrat, auf das die Bundeswehr und alle anderen europäischen Streitkräfte für effektive Abschreckung und Verteidigung angewiesen sind. Nur so lassen sich Kommunikations- und Handlungsfähigkeit sicherstellen.

Darüber hinaus hat die Bundesregierung im „Strategiepapier zur Stärkung der Verteidigungsindustrie in Deutschland“ von 2015[6] wesentliche Elemente der EloKa – nämlich Sensorik, vernetzte Operationsführung und Verschlüsselung – zu nationalen Schlüsseltechnologien erklärt. Deren Verfügbarkeit für die Bundeswehr und Verbündete dient demnach dem nationalen Sicherheitsinteresse. Das zeigt ein politisches Verständnis für die Rolle dieser Fähigkeiten in moderner Kriegsführung.

Wenn Deutschland seine eigene Streitkräftekonzeption und verteidigungsindustrielle Strategie ernst nimmt, sollten diese modernisiert und ausgebaut werden. Im europäischen Vergleich verfügt es noch über signifikante EloKa-Fähigkeiten. Zudem gibt es in Deutschland und Europa derzeit noch eine solide verteidigungsindustrielle Basis im Bereich der EloKa. Auch halten Alliierte wie die USA und weitere befreundete Staaten wie Israel solche Kapazitäten vor.

Ein nationaler Alleingang in der Wiederherstellung der EloKa-Fähigkeiten dürfte jedoch scheitern: Angesichts der vorhandenen Risiken sind die zu unternehmenden finanziellen Anstrengungen zu groß und es bleibt zu wenig Zeit. Zudem braucht gerade der Bereich der Digitalisierung und EloKa so viel Gemeinsamkeit wie möglich, um möglichst effizient wirken zu können. Politisch würde Deutschland mit einer europäischen Initiative die militärische Handlungsfähigkeit Europas steigern. Dafür sollte es drei Dinge priorisieren:

- Deutschlands EloKa-Fähigkeiten sichern und ausbauen: Ein deutscher Beitrag kann vor allem über zum Teil bereits laufende Beschaffungen schnell geleistet werden. Zum einen betrifft das die Lücke bei fliegenden SIGINT-Systemen, die Deutschland seit der Außerdienststellung seiner SIGINT-Flugzeuge 2010 und der gescheiterten Beschaffung der „EuroHawk“-Drohne aufweist. Hierfür ist momentan der Kauf des Nachfolgers der „EuroHawk“-Drohne geplant. Da die Finanzierung allerdings bisher nicht gesichert ist, droht sich die Fähigkeitslücke über 2025 hinaus auszudehnen. Zweitens ist die Entscheidung zur „Tornado“-Nachfolge wichtig: Deutschland und Italien stellen mit diesen Maschinen die wichtige Fähigkeit zur Bekämpfung von Flugabwehr, doch sind sie völlig veraltet. Drittens nähern sich die Flottendienstboote der Marine dem Ende ihrer Lebenszeit, weshalb mittelfristig gleichwertiger Ersatz nötig wird.
- Rechtzeitige Entscheidungen würden Deutschland helfen, bei der Beschaffung und Modernisierung nicht ins Hintertreffen zu geraten und damit proaktiv EloKa-Fähigkeiten gestalten zu können.
- PESCO-Projekt für EloKa-Kräfte ausweiten: Deutschland sollte das laufende PESCO-Projekt mit Tschechien zu EloKa als Ausgangspunkt für weitere europäische Kooperationen nutzen. Das würde die Angleichung der Prozesse und Standards und damit die militärische Effektivität steigern. Eine Ausweitung des Projektes auf Technologien oder ein gänzlich neues Projekt zur Zukunft der EloKa könnte außerdem attraktiver für Partner wirken als der jetzige Fokus auf Prozessvereinheitlichung.
- EU-NATO-Kooperation bei Härtung (Erhöhung der Widerstandkraft gegen elektronische Kriegsführung) von Systemen fördern: Hier sind momentan Zuständigkeiten und Kompetenzen zwischen einzelnen Staaten, EU und NATO geteilt. Ziel der Bündnispartner muss der Schutz von Netzwerken und Komponenten vor Angriffen über das elektromagnetische Spektrum sein. Das betrifft alle Akteure, insbesondere da z.B. die russische EloKa-Doktrin nicht vor Angriffen auf zivile Infrastruktur und Industrie Halt macht. Außerdem zählt Russland auch Informationskriegsführung und psychologische Kriegsführung in Teilen zur EloKa. Das sind Bestandteile, die klar über die Verantwortung der NATO hinausgehen und eher für die EU und einzelne Staaten relevant sind.

Über diese prioritären Maßnahmen hinaus sollte Deutschland mit seinen Partnern versuchen, Einigkeit über eine gemeinsame Vorstellung der Zukunft von EloKa herzustellen. Der technologische Fortschritt ermöglicht heute die Neujustierung des Verhältnisses von Plattform und Fähigkeit. Damit würden EU- und NATO-Staaten den Trend hin zu netzwerkbasierter Kriegsführung auch für die EloKa nachvollziehen und ihren potentiellen Gegnern wieder einen Schritt voraus sein.

Torben Schütz ist Associate Fellow im Programm Sicherheit, Verteidigung und Rüstung bei der Deutschen Gesellschaft für Auswärtige Politik (DGAP).

Anmerkungen

1 Über die chinesischen EloKa-Kräfte ist öffentlich zwar wenig bekannt, aber es ist sicherlich kein Zufall, dass sie einen prominenten Platz in der Militärparade zum 70. Gründungsjubiläum der Volksrepublik einnahmen.
2 Siehe z.B. Phillips, M. (2017): "Battlefield Electronic Warfare", Military Technology, 2 (2017): S.94
3 Bundesministerium der Verteidigung (2018): „Konzeption der Bundeswehr", Juli 2018: S.47f
4 Öffentliche Daten über die Anzahl an bodengebundenem EloKa-Gerät sind kaum verfügbar, weshalb sie hier nicht weiter behandelt werden.
5 Letzter Stand öffentlich verfügbarer Daten 2018.
6 Bundesregierung der Bundesrepublik Deutschland (2015): „Strategiepapier der Bundesregierung zur Stärkung der Verteidigungsindustrie in Deutschland", Juli 2015, S.3f.

DGAP**kompakt** / Nr. 17 / Oktober 2019

DGAP
Deutsche Gesellschaft für Auswärtige Politik
German Council on Foreign Relations

Die DGAP trägt mit wissenschaftlichen Untersuchungen und Veröffentlichungen zur Bewertung internationaler Entwicklungen und zur Diskussion hierüber bei. Die in den Veröffentlichungen geäußerten Meinungen sind die der Autoren.

Rauchstraße 17 / 18 · 10787 Berlin
Tel. +49 (0)30 25 42 31 -0 / Fax -16
info@dgap.org · www.dgap.org

Herausgeber
Deutsche Gesellschaft für Auswärtige Politik e.V.
ISSN 2198-5936

Redaktion Susann Kreutzmann
Layout/Satz Reiner Quirin
Designkonzept Carolyn Steinbeck · Gestaltung