2019/5/6 Elektronische Kriegsfuehrung

ELEKTRONISCHE KRIEGSFÜHRUNG - ZURÜCK ZU DEN GRUNDLEGENDEN FÄHIGKEITEN

Die USA befinden sich seit Beginn des Ukraine-Konfliktes 2014 wieder inmitten verstärkter Spannungen mit Russland. Der russisc
Wladimir Putin setzt alles daran, Russland nach dem Zusammenbruch der Sowjetunion wieder zu einer militärischen Großmacht z
Russland hat hybride Methoden entwickelt und verfeinert, um in einem Konflikt mit den USA und den alliierten Kräften die Oberhar
gewinnen. Die teils massive militärische Unterstützung des syrischen Regimes von Präsident Baschar al-Assad, einem alten Alliie
Sowjetzeiten, zeigt auf, dass Moskau heute gewillt ist, dem Westen die Stirn zu bieten. Russland hat bei seinem Vorgehen zur Un
der pro-russischen Rebellen in der Ostukraine und bei der Annexion der Krim durch Moskau aufgezeigt, in welcher Weise man ko
und unkonventionelle Mittel – unterhalb der Schwelle zu einem offenen Krieg – einsetzt, um seine Ziele zu erreichen.
Ein solcher asymmetrischer Hybridkrieg[1] wird gemeinhin meist als unkonventionelle, militärische, nicht-militärische, multimethodi
strategische Kriegsführung charakterisiert.
Die Festigung der Fähigkeiten etwa des U.S. Army Cyber Command aus Cyber-, Intelligenz-, elektronischen Kriegsführungs- und
stellt einen entscheidenden Faktor dar, um sich gegenüber gleichwertigen Herausforderern in künftigen Auseinandersetzungen erf
durchzusetzen.
Vor allem zielen die russischen und auch die wachsenden chinesischen Kapazitäten[2] darauf ab, die westlichen Streitkräfte „blind
durch diverse elektronische Störmanöver zu machen, um die Mobilität der eigenen Truppen möglichst zu hemmen. (Das gilt natürl
umgekehrt.) Speziell China fokussiert sich auf den Ausbau dieser asymmetrischen Hybridtaktik, um Amerika um jeden Preis auf A
erreichen, zu übertreffen und möglichst zu beherrschen.[3]
So gehört es zu den zentralen Aufgaben im Bereich der Elektronischen Kriegsführung des Westens, im Ernstfall die diesbezüglich
feindlichen Attacken bestmöglich zu neutralisieren und gleichzeitig das globale russische Navigationssatellitensystem und das Bei
Navigationssystem zu stören, bzw. die GPS-Nutzung durch feindliche Kräfte zu verhindern.[4] Zudem werden Wege und Mittel ge
defensive wie offensive Toolsets für die taktische Cyberkriegsanwendung zu verbessern. Dazu gehören etwa Cyber-Artillerie-Stur
vor der eigentlichen Attacke Malware in feindliche elektronische Verteidigungssysteme einschleust und die Kommunikation deaktiv
„defensive Aufmerksamkeit“ zu erregen.[5]
Insbesondere würden die westlichen Navigationssatelliten des Global Positioning Systems (GPS) von feindlichen Kräften attackier
Gesamtkommunikation zu beeinträchtigen, sodass NATO-Einheiten auf manuelle Mittel des Navigierens zurückgreifen müssten (e
Landkarten und Kompasse). Eine Störung oder gar Unterbrechung des GPS-Netzwerks würde zudem die Fähigkeiten der NATO-
empfindlich einschränken, was den Einsatz verbundener Waffensysteme wie Artillerie und Luftunterstützung betreffen. Im Kern zie
Attacken auf eine größtmögliche Außerkraftsetzung der Führungs- und Leitsysteme der NATO ab.
Eine der größten Stärken insbesondere etwa des US-Marine Corps, nämlich die Fähigkeit zur Bereitstellung und Integrierung vers
unterstützender Waffensysteme, könnte damit nicht zum Tragen kommen. Russland oder China würden im Konfliktfall natürlich ve
Einheiten des Marineinfanteriekorps zu lokalisieren und sie durch die Verfolgung elektronischer Emissionen zu erfassen. Wenn du
elektronische Kampfmittel erfolgreich Kommunikationsnetze des Gegners gestört werden können, dann können damit auch
Truppenbewegungen verlangsamt werden, da viele Einheiten an Ort und Stelle bleiben würden, bis die Kommunikation wiederher
worden ist.
Aus diesem Grunde müssen vor allem auch die Streitkräfte des Westens dafür bestmöglich geschult sein, um auf künftigen Schlac
etwa Maschinengewehre, Raketenwerfer und Handgranaten als militärische Hauptinstrumente in solchen Worst-Case-Szenarien e
Dazu zählt auch eine ausreichende Tarnung. Während die primäre Ausrichtung westlicher moderner Streitkräfte darin besteht, sic
Tech-Lösungen für das sich verändernde operative Umfeld auszurichten, dürfe jedoch nicht vergessen werden, dass grundlegend
Fähigkeiten, wie Tarnung und persönliche Belastbarkeit, es den Soldaten ermöglichen, auch unter schwierigen Bedingungen best
können.
Um einen wesentlichen militärtechnologischen Vorsprung vor den Gegner zu haben, investieren die Großmächte insbesondere in
Intelligenz (KI), maschinelles Lernen sowie in Quantencomputer. Hier sind die USA zwar weiterhin führend, aber dieser Vorsprung
Deshalb wird die Zusammenarbeit westlicher Parnter eine immer wichtigere Rolle bei der Bereitstellung von tragfähigen Technolo
diesem Zusammenhang spielen.[6]
In diesem Sinne ist das Beherrschen der grundlegenden militärischen Fähigkeiten im mehr oder weniger „vor-digitalen“ Bereich vo
Bedeutung, um im Falle von feindlichen Cyberangriffen bzw. -attacken auf dem Gebiet der elektronischen Kriegsführung dennoch
bestehen zu können.[7]

Abgeschlossen

Weiterführende LINKS:

Electronic Warfare – The Forgotten Discipline

Electronic Warfare - an overview | ScienceDirect.com

What's in an Electronic Warfare System?

Electronic Warfare - The Unseen Battlefield - YouTube

Electronic Warfare: Electronic Protection & Attack | BAE Systems

Electronic Warfare | Raytheon

The evolution of electronic warfare: a timeline - Army Technology

China electronic warfare | The Diplomat

China Develops New Electronic Warfare Aircraft - Defenseworld.net

Russia’s Electronic Warfare Capabilities to 2025 – Center for Strategic & International Studies

Live übertragen am 29.01.2018 - YouTube

Electronic Warfare: Element of Strategy and Multiplier of Combat Power

3-D 360 Experience with electronic warfare - YouTube

Anmerkungen:

[1] Vgl. dazu: Vortrag von Dr. Johann Schmid an der Wiener Strategiekonferenz 2019 (24. – 28. Juni 2019) zum Thema „THE PAR
TRINITY OF HYBRID WARFARE“.

[2] Vgl. dazu: Daniel Huynh, „TACTICAL CONSIDERATIONS FOR A COMMANDER TO FIGHT AND WIN IN THE ELECTROMAG
SPECTRUM“. In: Amry Cyber Institute 3/2018, S. 15-25.
Adam Segal, „WHEN CHINA RULES THE WEB“. In: Foreign Affairs 5/2018, S. 10-18.

[3] Autorenkollegium, „THE SECRET WAR AGAINST THE UNITED STATES - THE TOP THREAT TO NATIONAL SECURITY AN
AMERICAN DREAM CYBER AND ASYMMETRICAL HYBRID WARFARE – AN URGENT CALL TO ACTION“. In: The Cyber Defe
Vo.2, No.3 Fall 2018, S. 25-32.

[4] Siehe: Robert K. Ackerman, „CONVERGENCE GUIDES ARMY CYBER“. In: Signal 8/2018, S. 12-14.

[5] Andrew White, „SPECIAL FORCES UPGRADE CYBER-WARFARE CAPABILITIES“. In: Jane’s Intelligence Review 1/2018, S.

[6] Dazu: Autorenkollegium, „FIGHT TONIGHT IN THE CYBER DOMAIN“. In: Marine Corps Gazette 10/2018, S. 19-21.
George I. Seffers , „THE CYBER TIES THAT BIND NATO AND THE EU REINFORCE THEIR CYBERSECURITY PARTNERSHIP
/2018, S. 19-21.

[7] Matthew I. Shibata, „FIELD CRAFT: OUR LOST ART - Lessons learned from the British Royal Marine Commandos“. In: Marine
Gazette 11/2018,
S. 20-23.