ISPK Institut für Sicherheitspolitik an der Universität Kiel

Maritime Sicherheitspolitik im digitalen Zeitalter

Warum der Cyberraum zentraler Bestandteil moderner Kriegsführung im 21. Jahrhundert ist

*Alexander Pries**

Foto: ISPK

Vladimir Putins Angriffskrieg gegen die Ukraine ist eine Zäsur für Europa. Das Fundament dieses Angriffs verdient nähere Betrachtung, da es einen Aspekt birgt, der zukünftigen militärischen Konfrontationen immanent sein wird: Die Nutzung des Cyberraums als militärischer Teildimension. Russland gehört mit seinem „New Generation Warfare"-Konzept zu den führenden Nationen bei der Nutzung des Cyberraums. Ziel dabei ist es, die neuen Abhängigkeiten von digitaler und vernetzter Technologie für die eigenen Interessen zu nutzen, und so in erster Linie die Kosten für einen „heißen" Krieg auf das absolute Minimum zu reduzieren. Kriegsführung beginnt nicht mehr ab dem Moment des ersten Schusses. Der Cyberraum selbst wird zum Kriegsgebiet, in welchem Falschinformationen und Propaganda verbreitet, soziale, kulturelle und regionale Konflikte via Social Media katalysiert sowie Unternehmen, Behörden und staatliche Infrastruktur destabilisiert werden. Operationen in diesem Raum sind kostengünstig, anonym und können die eigene Position im Vorfeld oder während eines „heißen" Krieges signifikant stärken. Die Cyberattacken in der Ukraine (bspw. Blackout 2015, NotPetya 2017 sowie die Attacken vor und während des russischen Angriffs in diesem Jahr) zeigen, dass diese Überlegungen keine strategische Theorie, sondern taktische Realität sind.

Im maritimen Raum gilt die Aufmerksamkeit insbesondere GPS Spoofing-Attacken mit deren Hilfe jüngst auch das AIS-Signal der britischen HMS Defender und der niederländischen HNLMS Evertsen manipuliert werden konnte. Beide Schiffe lagen zur Zeit der Attacke in Odessa, als das AIS-Signal fälschlicherweise eine Route bis ganz in die Nähe des Krimhafens von Sewastopol anzeigte. Diese Daten dienten als Rechtfertigungsgrundlage für das Bedrängen von HMS Defender durch russische Patrouillenboote und Jets wenige Tage später.

Die empirische Umsetzung von Russlands angepasstem Kriegskonzept ist jedoch nicht auf die Ukraine beschränkt. Laut Nato StratCom sind insbesondere die Staaten im Baltikum Adressat russischer Desinformationskampagnen und Cyberattacken. Aber auch Deutschland hat laut BSI im letzten Jahr einen starken Anstieg an Cyberattacken erleben müssen. Die „Ghostwriter" Phishing Attacken 2021 (vermeintlich seriöse Mails, die wichtige Benutzerdaten abfragen) auf baltische, polnische und deutsche Politiker sind aktuelle Beispiele für Angriffe aus dem Cyberraum, die laut EU von Russland ausgegangen sind und die verdeutlichen, dass in Zukunft der Cyberraum auch für die Sicherheit von Anrainerstaaten der Ostsee relevant ist. Im Zuge der sich nun neu sortierenden europäischen Sicherheitsordnung ist davon auszugehen, dass GPS Spoofing und ähnliche Attacken auf private oder staatliche Akteure in der Ostsee zunehmen werden. Wie das Beispiel im Schwarzen Meer zeigt, ist es möglich, durch das Manipulieren von Positionsdaten in nationalen oder konfliktreichen Gewässern, Gründe für militärische Aggressionen zu schaffen. Es ist daher entscheidend, dass Deutschland und die Nato auf diese Form der vernetzten Kriegsführung vorbereitet sind.

Mit dem „Warfighting Capstone Concept" hat die Nato im letzten Jahr eine wichtige Grundlage für „Multi-Domain Operationen" gelegt, um die neuen Operationsräume Cyber und Space in bestehende Konzepte zu integrieren. So hatte Baltops 2021 erstmals eine Komponente, in der „defensive Cyber-Krieg-Taktiken, -Techniken und -Verfahren geübt [wurden]".

Der Cyberraum verknüpft die konventionellen Gefechtsräume Land, Luft und See und macht Multi-Domain Operationen erst möglich. Entsprechende Aufmerksamkeit sollte er zukünftig taktisch, operativ und konzeptionell erfahren.

Alexander Pries studiert Politikwissenschaft und Soziologie an der Christian-Albrechts-Universität (CAU) und hat vor Kurzem ein Praktikum am Institut für Sicherheitspolitik an der Universität Kiel (ISPK) absolviert.