Bundesministerium der Verteidigung

Der Organissationsbereich Cyber- und Informationsraum (OrgBer CIR) als wichtiger Teil einer gesamtstaatlichen Sicherheitsvorsorge und Treiber der Digitalisierung in der Bundeswehr

Auswirkungen der Digitalisierung

Die Digitalisierung ist das dominierende kulturelle und gesellschaftliche Merkmal der Gegenwart, der Megatrend für das 21. Jahrhundert. Die Digitalisierung und nahezu grenzenlose Vernetzung bietet in unseren demokratischen, freiheitlichen Gesellschaften ungeheure Chancen für Staat, Wirtschaft und Wissenschaft – auch für die Streitkräfte. Prozesse und Kommunikation sind schneller und effizienter, Vieles ist bequemer und einfacher geworden. Wann fährt der nächste Bus? Wie wird das Wetter heute Abend? Schnell noch von unterwegs die Heizung ein wenig herunter regeln. Der technische Fortschritt ermöglicht Verbesserungen in allen Bereichen des Lebens und der Gesellschaft.

Bei allen Vorteilen und Errungenschaften gibt es aber auch die Kehrseite der Medaille: Die Digitalisierung hat neue Abhängigkeiten und Verwundbarkeiten geschaffen. Sie bietet auch enorme Chancen für potentielle Gegner und damit Risiken für unsere Gesellschaft. Cyber-Angriffe auf Staaten, Wirtschaftsunternehmen inklusive kritische Infrastrukturen und private Haushalte sind schon lange Realität. Neben Angriffen aus dem Cyber-Raum sind auch Aktivitäten im Informationsumfeld, etwa Fake-News-Kampagnen um Unruhen zu schüren, an der Tagesordnung. Zunehmend werden staatliche und innerstaatliche Konflikte durch Propaganda und Desinformation beeinflusst.
Mittlerweile ist allgemein bekannt, welche gravierenden Folgen ein Befall mit Schadsoftware für global agierende Unternehmen als auch für Privatpersonen haben kann. So richtete die Ransomware „WannaCry“ weltweit insbesondere bei Unternehmen große wirtschaftliche Schäden an. Im Juli 2020 gab es einige große „Twitter-Hacks“, als Konten von Barack Obama, Joe Biden oder Bill Gates obskure Bitcoin-Tweets versendet haben. Es wird deutlich: Beide Elemente – Cyberangriffe und Desinformation – sind inzwischen wesentliche Bestandteile einer Strategie von hybrider Einflussnahme, die heutzutage immer wieder beobachten werden kann.

Verfasser: PIZ Kdo CIR, Stand: 1. Juli 2021

Besonderheiten des Cyber- und Informationsraums aus militärischer Sicht

Die militärische Dimension Cyber- und Informationsraum unterscheidet sich gegenüber klassischen Operationsräumen durch viele Besonderheiten. Der Cyber- und Informationsraum zeichnet sich durch ein hohes Maß an Komplexität aus. Territorialität wird durch Virtualität ergänzt. Ein Aufteilen des Cyber- und Informationsraums in Gefechtsstreifen mit klaren räumlichen Grenzen ist nicht möglich. Gleiches gilt für das Manövrieren von Truppen. Allerdings können im und durch den Cyber- und Informationsraum durchaus physische Wirkungen erzielt werden. Der Ort der Auswirkung von CIR-Operationen kann dabei theoretisch zehntausende Kilometer entfernt von der Quelle der Aktivität liegen. Auch die Zeit hat eine andere Bedeutung. Eine Wirkung kann z.B. über eine beliebige Entfernung ohne Zeitverzug erzielt werden. Effekte erfolgen in Echtzeit.

Durch die Möglichkeiten der Digitalisierung können inzwischen nichtstaatliche Akteure über Cyberangriffe Wirkungen erzielen, die bisher staatlichen Akteuren vorbehalten waren. Zudem können aufgrund der technischen Möglichkeiten Handlungen besonders gut verschleiert werden. Deshalb gestaltet sich die Attribuierung von Angriffen besonders problematisch. Es gibt eine Vielzahl möglicher Tätergruppen und Motive. Sie reichen von Kriminellen über Terroristen bis hin zu staatlichen Akteuren.

Fazit: Die Gefahrenlage hat sich durch die Digitalisierung deutlich verkompliziert. Dies hat auch Auswirkungen auf das zukünftig wahrscheinlichste Konfliktbild mit dem sich die Bundeswehr und auch der Staat beschäftigen müssen.

Verändertes Konfliktbild

Eine groß angelegte kinetische Auseinandersetzung ist in Zukunft nicht mehr das wahrscheinlichste Szenar. Konventionelle militärische Kräfte müssen zwar nach wie vor in hinreichender Qualität und Quantität vorgehalten werden, allerdings vorrangig um eine glaubhafte Abschreckung zu gewährleisten. Hybridität wird zunehmend zum bestimmenden Merkmal. Sie ist sowohl ohne als auch in Verbindung mit klassischer militärischer Gewalt möglich – was man zum Beispiel auf der Krim beobachten konnte. Bei hybriden Strategien existieren besondere Herausforderungen: Sie nutzen Freiräume im Recht, die durch technologischen Fortschritt entstanden sind. Zudem nutzen sie unklare Zuständigkeiten – z.B. die Abgrenzung innere und äußere Sicherheit. Außerdem bleiben sie in der Regel unterhalb der Schwelle des „klassischen“ Krieges. Das heißt aber nicht, dass sie gewaltfrei verlaufen. Solange es nur um „normale“ Cyberkriminalität geht, greifen die aktuellen Strukturen der

Strafverfolgungsbehörden. Was aber, wenn Cyberangriffe eine Qualität und ein Ausmaß erreichen, die die Handlungsfähigkeit des Staates oder die Versorgung der Bevölkerung oder die öffentliche Ordnung bedrohen? Die Schwellen zum Spannungs- und Verteidigungsfall sind zu Recht sehr hoch. Es sind aber durchaus auch Szenarien vorstellbar, in denen diese Schwellen nicht überschritten werden, gleichwohl aber massive Schadenslagen beherrscht werden müssen. Cyberangriffe haben die unangenehme Eigenschaft, dass man zur Schadensminimierung in der Regel sehr schnell und an vielen unterschiedlichen Fronten handeln muss. Daher hat der Schutz gegen Gefahren aus dem Cyber- und Informationsraum eine wichtige strategische Bedeutung und muss unter gesamtstaatlichen Aspekten betrachtet werden.

Der OrgBer Cyber- und Informationsraum – Bündelung von Fähigkeiten und Kompetenzen der Bundeswehr

Als Reaktion auf die Herausforderungen durch die zunehmende Digitalisierung hat die Bundesregierung 2016 ihre aktuelle Cyber-Sicherheitsstrategie für Deutschland erlassen. Danach liegt die Verantwortung für die Cybersicherheit beim Bundesministerium des Inneren. Für die Cyberverteidigung ist die Bundeswehr zuständig. Unter diesen Voraussetzungen wurde zum 1. April 2017 der neue OrgBer CIR aufgestellt. In ihm wurde die bereits in der Bundeswehr vorhandene Expertise zum Themenbereich gebündelt, weitere Fähigkeiten wurden aufgebaut. Zu den militärischen Dimensionen Luft, Land, See und Weltraum trat eine fünfte hinzu, der „Cyberraum“. Gemäß dem aktuellen Eckpunktepapier der Bundesministerin der Verteidigung wird der OrgBer CIR als einer von vier Dimensionsbereichen bestehen bleiben, seine Fähigkeiten werden weiter ausgebaut. Damit wird der herausragenden Bedeutung des Themas Digitalisierung Rechnung getragen.

Aufgaben und Verständnis des OrgBer Cyber- und Informationsraum

Die Aufgaben des OrgBer CIR umfassen weit mehr als die reine Cyber-Thematik. Dem OrgBer CIR obliegt der Schutz und Betrieb des IT-Systems der Bundeswehr im Inland und in den Einsatzgebieten. Ein weiteres Aufgabengebiet ist das Militärische Nachrichtenwesen.

Hier werden Aufklärungsergebnisse bewertet, die den jeweiligen Adressaten als maßgeschneiderte Lageinformation zur Verfügung gestellt werden. Auch die Aufklärung und die Wirkung im Cyber- und Informationsraum gehört zu seinem Aufgabengebiet. Hierzu zählen Cyberoperationen, beispielsweise das Eindringen in gegnerische IT-Netze zur Informationsgewinnung und/ oder Manipulation, der Elektronische Kampf und die Operative Kommunikation in den Einsätzen.

CIR-Operationen werden durch den OrgBer CIR „aus einer Hand“ in nationale Planungs- und Führungsprozesse eingebunden. Die Operationsplanung und -führung von CIR-Operationen folgt grundsätzlich der Methodologie des Planungsprozesses der NATO. Sie decken das gesamte Spektrum von Aufklärung, Wirkung und Schutz ab. Operationen im CIR können den jeweiligen Forderungen als Beitrag im Rahmen der Landes- und Bündnisverteidigung, des Internationalen Krisenmanagements und zur gesamtstaatlichen Sicherheitsvorsorge im Cyber- und Informationsraum als nationales Krisen- und Risikomanagement angepasst werden. Zukünftig wird der Bereich CIR-Operationen auch zur Unterstützung von Weltraum Operationen ausgestaltet.

Darüber hinaus deckt der OrgBer CIR das Thema Geoinformationswesen ab. Dort werden hochauflösende, qualitätsgesicherte digitale Geoinformationen jeglicher Art hergestellt. Ein ganz profanes Beispiel hierfür ist die Herstellung traditioneller Geländekarten – sowohl in Papierform als mittlerweile natürlich auch digital.
Der OrgBer CIR ist damit auf der einen Seite Enabler für die klassischen Teilstreitkräfte – auf der anderen Seite hat er aber auch den Auftrag, eigenständig Operationen zu planen und zu führen und dabei, wenn nötig, von anderen Teilstreitkräften unterstützt zu werden.
Zudem ist der OrgBer CIR Koordinator und Garant für die erfolgreiche Digitalisierung der Bundeswehr. Er stellt sicher, dass einzelne IT-Beschaffungsvorhaben zu einem funktionierenden gesamten IT-System der Bundeswehr zusammengeführt werden können, stellt Standards in Bezug auf die Informationssicherheit und Cyberawareness. Darüber hinaus ist er federführend bei querschnittlichen Anwendungen wie Kollaborationswerkzeugen, d. h. er gestaltet Stabsarbeit voll digitalisiert und damit schneller und direkter.

Die NATO hat bereits 2016 auf ihrem Gipfel in Warschau den Cyberraum als eigenständige militärische Dimension anerkannt – analog zu den Dimensionen Land, Luft, See und Weltraum. Die Bundeswehr fasst diese neue militärische Dimension bewusst noch weiter als die NATO und bezieht den Informationsraum mit ein. Dies ist ein wichtiger Ansatz, denn, wie bereits erläutert: Neben Angriffen
aus dem Cyber-Raum nehmen auch Aktivitäten im Informationsumfeld, etwa Fake-News-Kampagnen oder Desinformation, immer mehr zu. Laut einer aktuellen Studie wird die Manipulation der öffentlichen Meinung durch sogenannte Fake News inzwischen von Politikern und Wirtschaftsvertretern als die größte „Cyber-Gefahr“ für Deutschland angesehen. Dem trägt der OrgBer CIR Rechnung. Die sicherheitspolitische Schwerpunktsetzung der Bundeswehr hat sich seit der Aufstellung des OrgBer CIR deutlich weiterentwickelt. Mit der immer stärkeren gesamtpolitischen Bedeutung des Cyber- und

Informationsraumes und der zunehmenden Auftragslage in der Fähigkeitsentwicklung CIR sowie der Ausrichtung am Fähigkeitsprofil der Bundeswehr wurde deutlich, dass das Gesamtportfolio an Aufträgen bei unveränderter Ressourcenlage nur mit erheblichen Einschränkungen zu erfüllen sein wird. Dies betrifft insbesondere die Bereiche Refokussierung auf Landes- und Bündnisverteidigung, Aufstellung eines Joint Intelligence Centers, Digitalisierung der Bundeswehr und Aufstellung von Kompetenzzentren im OrgBer CIR. Die Struktur des OrgBer CIR wurde daher 2019/2020 detailliert analysiert und beginnend in 2021 mit dem Ziel der Verschlankung, deutlich höherer Agilität, dem Ausbau der Fähigkeit zum Planen und Führen von CIR-Operationen und dem Umsteuern von Ressourcen in die Fachlichkeit neu ausgerichtet. Viele dieser Leitgedanken und Planungen wurden durch das Eckpunktepapier der Bundesministerin der Verteidigung bestätigt. Die Neustrukturierung des OrgBer CIR mit schlanken, agilen Strukturen und Reinvestition in die Fachlichkeit wird nun konsequent um- und fortgesetzt. Die Kernaufträge des OrgBer CIR bleiben dabei unverändert, die Fähigkeit zum Planen und Führen von CIR-Operationen im Rahmen des Internationalen Krisenmanagements und der Landes- und Bündnisverteidigung wird ausgebaut. Mit der Umsetzung der neuen Struktur wird ab dem 01.08.2021 begonnen, im Jahr 2025 soll sie abgeschlossen sein.

Voraussetzung für den Schutz vor den Herausforderungen der Digitalisierung: Enge nationale und internationale Zusammenarbeit

Um den Herausforderungen der Digitalisierung erfolgreich zu begegnen ist es wichtig, alle relevanten Akteure – Staat, Wirtschaft und Wissenschaft, national wie international – miteinander zu vernetzen, um im Fall der Fälle hinreichend reaktionsfähig zu sein, und zwar über alle Zuständigkeitsgrenzen hinweg. In Deutschland wurde bereits 2011 unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik das Nationale Cyber-Abwehrzentrum als erstes Forum für die Zusammenarbeit staatlicher Stellen im Kontext Cybersicherheit geschaffen. Dieses wurde und wird weiterhin zu einer ressortübergreifenden, operativen Institution unter Einbindung aller wichtigen Akteure weiter-entwickelt – eine wesentliche Voraussetzung dafür, die Handlungsfähigkeit Deutschlands auf diesem Gebiet in Zukunft zu gewährleisten. Die Grundlagen wurden bereits gelegt. Eine erste vernetzte Handlungsfähigkeit ist gegeben, ein erstes gemeinsames Lagebild existiert. So wird die sogenannte „Cyber-Sicherheitslage Deutschland“ wöchentlich erstellt. Die Präsenz der entsprechenden Behörden im Nationalen Cyber-Abwehrzentrum wurde erhöht. Auch der OrgBer CIR bringt sich prominent in dieses Cyber-Abwehrzentrum ein. Das Kommando CIR stellt derzeit einen der beiden Stellvertretenden Koordinatoren, einen Verbindungsoffizier sowie Unterstützungspersonal.

Auch international ist eine enge Zusammenarbeit zwingend erforderlich, denn der Cyberraum endet nicht an Staatsgrenzen. Im militärischen Bereich findet bereits eine sehr enge Zusammenarbeit auf EU- und NATO-Ebene statt. So wurde im Oktober 2019 das Cyber Operation Centre der NATO etabliert. Im November 2019 wurde als eines der jüngsten PESCO-Projekte das Cyber and Information Domain Coordination Centre (CIDCC) eingerichtet, für das Deutschland, bzw. der OrgBer CIR, die Federführung hat. Zentrale Aufgabe dieser ständigen multinationalen Koordinierungsstelle soll die Erstellung von einheitlich strukturierten Lagebildern des Cyber- und Informationsraumes sein. Außerdem gehört es zum Aufgabenspektrum des CIDCC, die verfügbaren Lageinformationen zu bewerten und anschließend umfassend in den militärischen Planungs- und Führungsprozess von EU-Operationen und EU-Missionen einzubringen.

Last but not least muss natürlich der direkte Austausch mit der Wissenschaft und der Industrie im Gesamtthemenfeld Digitalisierung und Cybersicherheit zunehmend gefördert werden, um den aktuellen Herausforderungen begegnen zu können. Letztlich wird ein durchgängiges Ökosystem aus Wirtschaft, Forschung, Behörden und Zivilgesellschaft benötigt. Im Bereich der Wissenschaft leistet das Forschungsinstitut CODE der Universität der Bundeswehr München hervorragende Arbeit. Es vernetzt Experten für Cybersicherheit aus Forschung, Militär, Wirtschaft, Industrie, Behörden und Verbänden. Im wissenschaftlichen Fokus stehen dabei die Themenfelder KI, Quantencomputing und Blockchain. Mit der Erschließung und Förderung von Innovationen beschäftigen sich darüber hinaus der Cyber- und Innovation Hub der Bundeswehr in Berlin sowie die Cyberagentur (BMI/BMVg).