28. September 2018

Beitrag zum Sammelband über die
52. Sicherheitspolitische Informationstagung in Hamburg 2018

Moderation des
Panels 2
zum Thema
„Welche Rolle werden künftige passive und aktive Cyber-Verteidigungs-Fähigkeiten als integrierte Anteile von Operationen in der Militärstrategie einnehmen?“

Kurt Herrmann

Rahmen der Betrachtung

Der Sammelbegriff Cyberraum bezeichnet heute allgemein die Gesamtheit aller Informationstechnischen (IT) Systeme, Komponenten oder Dienste zur Vernetzung, Steuerung und Anwendung von digitalisierten Kommunikations- und Informationssystemen. Dieser virtuelle Raum erstreckt sich weltweit und grenzenlos; seine Hauptbasis ist das Internet, sein wesentliches Trägermedium das elektromagnetische Spektrum.

In dem eng damit verknüpften Informationsraum werden Informationen erzeugt, gespeichert, verarbeitet – d.h. analysiert, fusioniert, verdichtet, verknüpft, interpretiert, zweckorientiert aufbereitet - und verbreitet bzw. verteilt, auch mit dem Ziel, Denken und Handeln zu beeinflussen.

Risiken und potentielle Gefahren im Cyber- und Informationsraum (CIR) können schnell und unmittelbar staatliche Strukturen in ihrer Gesamtheit betreffen.

Das Internet ist für nahezu alle Lebensbereiche unserer modernen Industrie- und Dienstleistungsgesellschaft weitestgehend zur Kritischen Infrastruktur geworden. Die Systeme und Dienste im CIR bieten heute nahezu ungeahnte Fähigkeiten, erzeugen allerdings zugleich auch neue Verwundbarkeiten. Verwundbarkeiten im CIR bestehen vor allem durch unerlaubte Informationsweitergabe, Spionage, Manipulation, Verweigerung von Kommunikations- und Informationsdiensten oder sogar durch Sabotage.

Kritische Infrastrukturen im CIR, die Ziele potenzieller Cyberangriffe werden können, sind häufig in komplexer Weise vernetzt und hängen vielfältig voneinander ab. Dieser hohe Durchdringungsgrad verstärkt die Verwundbarkeiten bzw. Risiken und kann zu Kaskadeneffekten führen.

Ein Cyberangriff kann definiert werden als bewusste Projektion von Cyber-Fähigkeiten, um kinematische oder nicht-kinematische Wirkungen zu erzielen. Massive Cyberangriffe können die nationale Sicherheit bedrohen, den wirtschaftlichen Interessen schaden, politische oder kulturelle Instabilität hervorrufen, Personen verletzten oder töten oder Objekte (Geräte/Systeme) beschädigen oder zerstören. Die Palette heute verfügbarer Software-Applikationen oder Werkzeuge für potenzielle Cyberangriffe ist gewaltig und wächst dynamisch weiter. Man spricht bereits von einem „Malware Industrial Complex“.

Mit Steigerung der Artenvielfalt und Raffinesse von potentieller Schadsoftware in diesem Marktsegment vereinfachte sich vor allem auch die Anwendung, d.h. komplexe Angriffe können inzwischen relativ leicht, ohne ein hohes Maß an Fachwissen ausgeführt werden. Die modernen

„Tools“ erlauben es im Grunde jedem PC- oder Laptop-Nutzer Cyber-Angriffe weitgehend automatisiert durchzuführen.

Die spezifische Brisanz von Risiken und Bedrohungen im CIR liegt darin, dass die Gefährdungen in kürzester Zeit, unmittelbar, massiv und grenzüberschreitend auf Entscheidungs-, Führungs- und Steuerungsprozesse in allen Bereichen und auf allen Ebenen von Politik, Verwaltung, Sicherheitskräften und Unternehmen aller Branchen und Bereiche einwirken können. Damit kann bei Cyber-Angriffen relativ leicht und schnell die Schwelle zu einer Bedrohung von wahrhaft strategischer Dimension überschritten werden.

Der CIR hat das Potential, die Anforderungen und Bedingungen moderner Sicherheitspolitik radikal zu verändern. Die durch den CIR mögliche und realisierbare Erweiterung und Diversifizierung des Wirkungsspektrums der Gewaltanwendung ist keineswegs nur fiktiv oder virtuell, sondern bereits sehr real und auch militärisch relevant.

Der CIR weist als neue, fünfte operative Domäne der Sicherheitspolitik und Strategie – neben Land, Luft, See und Weltraum – eigentlich im klassischen Sinne alle Merkmale eines umfassend vernetzten Sicherheitsansatzes („Comprehensive Approach“) auf.

Es ist unter Fachleuten zwar nach wie vor umstritten, ob es bis heute überhaupt gelungen ist wirklich sicherheitspolitisch oder militärstrategisch relevanten Schaden anzurichten. Die Cyberangriffe auf Estland oder Georgien, aber evtl. auch der Angriff mit dem STUXNET-Wurm auf die iranische Atomanlage in Natanz sowie die im Frühsommer erfolgten „Wanna Cry“ und „Petya“ Ransomware Angriffe dürften jedoch die befürchtete Dimension zumindest in Ansätzen aufgezeigt oder sogar erreicht haben.

Ohne Zweifel bleibt allerdings auch ein nicht zu vernachlässigendes Restrisiko: Was wir nämlich nicht wissen ist – was wir nicht wissen. Denn sehr wahrscheinlich muss mit einer großen Vielfalt von verschiedenartigen und weitgefächerten Angriffstechniken, -Mitteln oder –Signaturen gerechnet werden, die derzeit überhaupt noch nicht erkennbar oder in Erscheinung getreten sind.

Darüber hinaus sind die Risiken durch Innentäter oder auch sogenannte „Leaker“– Beispiele Snowden/Wikileaks – nicht zu unterschätzen.

Schließlich – und nicht zuletzt – trägt auch ein eher laxer, wenig sicherheitsbewusster Umgang von Nutzern und Betreibern mit Kommunikations- und Informationstechnik erheblich zur Cyber-Gefährdung bei.

Das inzwischen erkennbare Ausmaß tatsächlicher oder potentieller Cyber-Angriffe rechtfertigt es deshalb durchaus, die Bezeichnung Cyberkrieg zu verwenden. Frei nach Clausewitz ist das ursprüngliche Wesensmerkmal eines Krieges die Gewaltanwendung. Der Angreifer will einem Gegner seinen Willen aufzwingen. Der Verteidiger will den Angreifer durch Gewaltandrohung oder im äußersten Fall auch durch Gewaltanwendung von der Aussichtslosigkeit oder den unverhältnismäßig hohen Kosten seines Vorhabens überzeugen.

Cyberangriffe können in ihrer Wirkung kinematischen Angriffen durchaus vergleichbar sein oder diese sogar noch übertreffen. Wie bei jeder Form der Sicherheitsvorsorge gilt es auch im CIR Schritt zu halten mit den Bedrohungen und dabei möglichst immer einen Schritt der potentiellen Gefährdung voraus zu sein.

Durch die Komplexität und ungebremste Dynamik der Entwicklung im CIR ist eine ausreichende Frühwarnfähigkeit äußerst problematisch und schwierig darzustellen.

Die operative Cyberabwehr bzw. die Cyberverteidigung muss das Ziel haben, insbesondere eine hohe Widerstandsfähigkeit („Resilienz“) zu erzielen. Es gilt den Betrieb und eine zuverlässige Funktionsweise der zu schützenden Systeme und Dienste im CIR auch nach massiven Sicherheitsvorfällen aufrecht zu erhalten. Hierzu dienen Vorkehrungen und Maßnahmen, die sich in drei Kategorien einordnen lassen:

- Präventive Schutz- und Sicherungsmaßnahmen
- Fähigkeiten bzw. Systeme zur Erkennung und Abwehr von Cyber-Angriffen und
- Verwundbarkeits- und Nachhaltigkeits-Management.

Eine wichtige Rolle spielen natürlich Experten, die zur raschen Verteidigung gegen erkannte Bedrohungen oder Angriffe aus dem CIR eingesetzt werden. Diese sogenannten (Cyber oder) Computer Emergency Response Teams (CERT) bestehen aus gut ausgebildeten, sehr erfahrenen Spezialisten zur Wahrnehmung der vorhin erwähnten Aufgaben. Sie werden im Grunde als „Schnelle Cyber Eingreiftruppe“ verwendet und eingesetzt.

Nationale Zuständigkeiten für Cyber-Sicherheit, Abwehr und Verteidigung

Ein erheblicher Teil der Risiken, Gefährdungen und Bedrohungen im CIR ist Einzeltätern (Hackern), Organisierter Kriminalität oder auch terroristischen Gruppen zuzuordnen. Damit liegen die nationalen Zuständigkeiten für Schutz und Sicherheit der Netze sowie für die Cyber-Abwehr vor allem in der Ressortzuständigkeit der Innenminister und bei den entsprechenden Innenbehörden, insbesondere beim Bundesamt für die Sicherheit in der Informationstechnik (BSI), beim Verfassungsschutz und der Polizei. Koordiniert werden die Aktivitäten in Deutschland durch das Nationale Cyber-Abwehr-Zentrum.

Da aber auch staatliche oder zumindest staatlich geduldete Akteure von außen, global agierend erkennbar werden, hat die Cyber-Gefährdung schon seit Jahren ebenfalls zunehmende außen- und sicherheitspolitische Bedeutung gewonnen.

Um den Bedrohungen aus dem CIR entschlossen und konzertiert entgegen wirken zu können, hat das Bundeskabinett am 9. November 2016 eine neue Cyber-Sicherheitsstrategie beschlossen. Damit wird unterstrichen, dass die Wahrung der Cyber-Sicherheit eine gesamtstaatliche Aufgabe darstellt, die nur im Zusammenwirken aller relevanten Kräfte wirkungsvoll und nachhaltig bewältigt werden kann. Für die Implementierung der Cyber-Sicherheitsstrategie wurden folgende vier Handlungsfelder definiert:

- Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung
- Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft
- Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur
- Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik.

Vorgesehen ist die Entwicklung einer gemeinsamen Cyber-Sicherheitsarchitektur unter der Federführung des Bundesministeriums des Innern (BMI) und in enger Abstimmung mit dem Auswärtigen Amt (AA) sowie dem Bundesministerium der Verteidigung (BMVg).

Als Kernelement soll das Nationale Cyber-Abwehr-Zentrum zur „zentralen Kooperations- und Koordinationsplattform“ weiterentwickelt und mit eigenen Bewertungs- und

Auswertungsfähigkeiten ausgestattet werden. Außerdem ist beabsichtigt, das Abwehrzentrum im Bedarfsfall zu einem Krisenreaktionszentrum aufwachsen zu lassen.

Ebenfalls geplant ist die Einrichtung sogenannter schneller Eingreiftruppen, die im Fall von Cyber-Angriffen gezielt an Brennpunkten eingesetzt werden können.

Die Verteidigungsaspekte der gesamtstaatlichen Cyber-Sicherheit werden gemäß Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr dem BMVg und der Bundeswehr zugeordnet, während die Gesamtverantwortung für die internationale Cyber-Sicherheitspolitik beim AA liegt. Dort gibt es seit 2013 einen Sonderbeauftragten für die Cyber-Außenpolitik.

Im BMVg wurde im Herbst 2016 eine eigenständige Abteilung Cyber- und Informationstechnik (CIT) eingerichtet. Im Frühjahr 2017 erfolgte in der Bundeswehr die Aufstellung eines neuen militärischen Organisationsbereichs, das Kommando Cyber- und Informationsraum (KdoCIR) mit einem Inspekteur an der Spitze. An der Universität der Bundeswehr München wurde ein Forschungszentrum für den Cyber-Raum etabliert, unterstützt durch den Ausbau des Fachbereichs Informatik und Cyber-Sicherheit.

Deutsche Dienststellen kooperieren zudem eng mit den für Cyber-Abwehr zuständigen NATO- (NATO Computer Incidence Response Capability, NCIRC, der NATO Communications and Information Agency) und EU-Stellen (u.a. European Network and Information Security Agency, ENISA).

Deshalb lohnt sich ein Blick auf die NATO- und EU-Strukturen für die Sicherheitsvorsorge im CIR.

<u>Cyberverteidigung in der NATO</u>

Die NATO befasst sich bereits seit 2002 intensiv mit der Cyber-Verteidigung. In Reaktion auf die erheblich angewachsene potentielle Bedrohung im CIR wurden Cyber-Angriffe auf dem NATO-Gipfel in Lissabon im November 2010 als „strategische Bedrohung“ eingestuft. Das Strategische Konzept der NATO hat demzufolge mehr Augenmerk auf den Schutz kritischer Infrastrukturen gerichtet und die Voraussetzungen für einen umfassenden Cyber-Sicherheitsansatz geschaffen, der seitdem anhand eines umfassenden Aktionsplans implementiert wird.

Auf dem Gipfel in Wales im September 2014 wurde eine neue, erweiterte Cyber-Verteidigungsstrategie beschlossen. Diese wurde auf dem NATO-Gipfel in Warschau im Juli 2016 nochmals bekräftigt und erweitert. Sie stuft Cyber-Verteidigung als integralen Bestandteil der kollektiven Verteidigung ein, was insbesondere auch bedeutet, dass ein Cyber-Angriff auf einen oder mehrere Mitgliedstaaten den Bündnisfall gemäß Artikel 5 des Nordatlantikvertrags auslösen kann.

In der Gipfelerklärung von Warschau wird der „virtuelle Raum“ – also der CIR – als eine Domäne anerkannt, „... in der sich die NATO genauso wirksam verteidigen muss wie in der Luft, auf dem Lande und zur See. Damit wird die Fähigkeit der NATO verbessert, Operationen in all diesen Domänen zu schützen und durchzuführen, und … Handlungs- und Beschlussfreiheit [der NATO] in allen Szenarien gewahrt. Auch damit wird die Abschreckung und Verteidigung der NATO insgesamt unterstützt: Die Cyber-Verteidigung der NATO wird weiter in die Operationsplanung und die Operationen und Missionen des Bündnisses integriert…“. Der NATO-Gipfel in Brüssel im Juli 2018 verlieh der Cyber-Verteidigung der NATO eine zusätzliche Dynamik.

Organisatorisch ist die Cyber-Verteidigung der NATO nach einem mehrschichtigen Modell strukturiert:

- Das politische „Cyber Defence Committee“ und das auf der Arbeitsebene angesiedelte „Cyber Defence Management Board“ beurteilen die Cyber-Lage und bereiten notwendige Maßnahmen vor zur Entscheidung im Nordatlantik Rat.
- Die „NATO Communications and Information Agency (NCIA)“ betreibt mit dem „NATO Computer Incidence Response Capability Technical Centre (NCIRC-TC)“ das primäre Dienstleistungszentrum für die operative Cyber-Verteidigung.

Die NATO-Stellen für Cyber-Verteidigung kooperieren u.a. eng mit den entsprechenden nationalen Stellen der NATO-Mitgliedsstaaten. Die Cyber-Verteidigungsfähigkeiten des Bündnisses werden grundsätzlich komplementär ergänzend zu den nationalen Fähigkeiten der Mitgliedsstaaten im Rahmen des „NATO Defence Planning Processes“ geplant.

Das „Cooperative Cyber Defence Centre of Excellence (CCDCoE)“ in Tallin, Estland, ist eine multinationale Einrichtung, dessen Zuständigkeiten und Aktivitäten in erster Linie auf den Gebieten konzeptionelle Aufgaben, Weiterentwicklung und Ausbildung liegen.

Cybersicherheit in der Europäischen Union (EU)

Auch die EU widmet der Sicherheit im CIR ein hohes Maß an Aufmerksamkeit. Die konzeptionellen Grundlagen für ihre Abwehrmaßnahmen gegen Cyberangriffe sind in einem spezifischen EU-Politikrahmen zusammengefasst. Mit der im Juli 2016 verabschiedeten Richtlinie zur Sicherheit von Netzwerken und Datensystemen (NIS-Richtlinie) hat sich die EU erstmals gemeinsame Regeln zur Cyber-Sicherheit gegeben. Die Mitgliedstaaten der EU verpflichten sich mit ihrer Zustimmung zu dieser Richtlinie, nationale Abwehrstrategien zu entwerfen, Eingreif- und Überwachungsteams aufzustellen und sich regelmäßig auf EU-Ebene abzustimmen.

Sie haben sich auch darauf geeinigt, im Bereich der Cyberabwehr stärker mit der NATO zusammenzuarbeiten. Zu ihrer Umsetzung sollen verstärkt gemeinsame Sitzungen von entsprechenden Gremien der NATO und der EU stattfinden. Die spezifischen Interessen beider Organisationen sowie die Partikularinteressen einzelner Mitgliedstaaten sollen dabei entsprechende Berücksichtigung finden. Bekräftigt wurde ferner, alle 28 EU-Mitgliedstaaten bei der Entwicklung von Fähigkeiten zur Cyber-Abwehr zu unterstützen.

Von besonderer Bedeutung sind in diesem Zusammenhang drei Einrichtungen der EU:

- Die „EU-Agentur für Netz- und Informationssicherheit“ (ENISA),
- das „Europäische Polizeiamt“ (EUROPOL) und
- das bei EUROPOL angesiedelte „Zentrum zur Bekämpfung der Cyberkriminalität“ (EC3).

Gerade im Bereich der Kriminalitätsbekämpfung auf europäischer Ebene hat die EU mit ihrem Verbund polizeilicher Behörden effektive Instrumente zur Hand, die in Kooperation mit der NATO sowie den nationalen Institutionen im Bereich CIR eine bedeutende Wirksamkeit entfalten können.

Sicherheitspolitische Herausforderungen im Cyberraum

Es ist anzunehmen, dass heute mehr als 100 Nationen bereits militärische Organisationen oder Strukturen eingerichtet haben, die Cyber-Angriffs- oder –Abwehrfähigkeiten besitzen.

Eine nach wie vor weitgehend ungelöste Herausforderung im CIR ist die Erkennung und Zuordnung von Angreifern, also das Problem der Attribution. Da sich Cyber-Angreifer in der Regel geschickt tarnen, zumeist eine mehrstufige, indirekte Vorgehensweise wählen und stets versuchen Ihre Spuren zu verwischen, sind sie schwer zu fassen. Hierbei spielt nicht zuletzt auch der Zeitfaktor eine erhebliche Rolle.

Bisherige Analysefähigkeiten der Cyber-Forensik sind höchst komplex und benötigen immer noch relativ viel Zeit. Leistungsfähige, zuverlässige Forensik-Werkzeuge, die in Echtzeit (on-line) eingesetzt werden können und nahezu zeitverzugslos Ergebnisse liefen, stehen derzeit zwar (noch) nicht zur Verfügung, intensive Bemühungen sind jedoch im Gange. Hohe Erwartungen richten sich dabei u.a. an den technischen Fortschritt bei der ehrgeizigen Entwicklung von „Supercomputern“.

Wie bei jeder Form der Sicherheitsvorsorge gilt es auch im CIR Schritt zu halten mit den erwartbaren Bedrohungen und dabei möglichst immer einen Schritt der potentiellen Gefährdung voraus zu sein. Durch die Komplexität und ungebremste Dynamik der technologischen Entwicklung im CIR ist hier jedoch eine ausreichende Frühwarnfähigkeit als äußerst problematisch und schwierig realisierbar zu bewerten.

Als besondere Herausforderung erweist sich die Abschätzung des anzunehmenden Ausmaßes potentieller Gefährdungen im CIR. Ein grundsätzlich erheblicher Unsicherheitsfaktor besteht darin, dass sehr wahrscheinlich mit einer großen Vielfalt von verschiedenartigen und weitgefächerten Angriffstechniken und Angriffsmitteln gerechnet werden muss, die auch durch intensive Aufklärung nicht erkennbar sind.

Vorrangiges Ziel einer operativen Cyber-Verteidigung muss es sein, eine hohe Widerstandsfähigkeit („Resilienz“) der zu schützenden Objekte zu erreichen. Es gilt den Betrieb und eine zuverlässige Funktionsweise der potentiellen Angriffsziele, also der kritischen Systeme und Dienste im CIR, auch nach massiven Attacken oder Sicherheitsvorfällen aufrecht zu erhalten.

Nach Clausewitz ist das ursprüngliche Wesensmerkmal eines Krieges die Gewaltanwendung, um einen Gegner zur Erfüllung des eigenen Willens zu zwingen (s.o.). Im Lichte der aktuellen Erkenntnisse moderner vernetzter Kriegsführung hat die neue sicherheitspolitische Dimension oder Domäne Cyber das Wirkungsspektrum der „Gewaltanwendung“ deutlich erweitert. Cyber könnte in dem hier betrachteten Zusammenhang sogar als eine Art Wirkungskatalysator bezeichnet werden.

Zu beobachten ist ein zunehmender Trend zur offensiven Nutzung von Cybertechnologien. Es ist zu befürchten, dass Cyber-Angriffsfähigkeiten sich immer mehr zu einem strategischen Instrument zwischenstaatlicher Konfliktaustragung entwickeln. Vermutlich hat ein „Wettrüsten“ der Nationen im Internet längst begonnen.

Nach Auffassung etlicher Experten kann es im Cyberraum keine wirksame „Eindämmungs-Politik“ geben. Die Technologien sind überwiegend „dual-use“ Technologien und die Entwicklung erhält ihre hohe Dynamik maßgeblich durch die zivile, kommerzielle Nutzung.

Angesichts der bereits genannten Anonymität von Cyber-Angriffen dürfte auch das so wichtige strategische Prinzip der Abschreckung im CIR in Frage gestellt sein.

Die Abschätzbarkeit von Kollateralschäden bzw. eine Fähigkeit, die Wirkung offensiver Maßnahmen – also letztlich das Eskalationspotential - hinreichend verlässlich vorherzusagen oder zu kalkulieren, dürfte ebenfalls bisher noch nicht mit der erwünschten oder notwendigen Wahrscheinlichkeit gewährleistet sein.

Wenn der CIR künftig zum zentralen Raum für die Austragung politischer und wirtschaftlicher Konflikte werden sollte, stellt sich die Frage: Müssen wir uns dann, z.B. durch verschränkte virtuelle und physische Formen der Kriegsführung, auf einen latenten oder sogar offenen Zustand permanenten Krieges und einen weiter zunehmenden Rüstungswettlauf im CIR einstellen?

Weiterentwicklung von Cybersicherheit und Cyberverteidigung als gesamtstaatliche Aufgaben

Analog zu Schutz und Verteidigung durch defensive und offensive konventionelle (kinetische) Fähigkeiten, sind im CIR – neben defensiven Schutz- oder Abwehrmaßnahmen – auch aktive oder offensive Gegenmaßnahmen in Betracht zu ziehen. Hierzu bedarf es entsprechender Strategien und Fähigkeiten. Dabei kommt allerdings auch wiederum der Forderung nach eindeutiger Identifizierung und Zuordnung von Angreifern im CIR – der sogenannten Attribution - besondere Bedeutung zu.

Um den Risiken und Bedrohungen aus dem CIR wirksam zu begegnen, sind ganzheitliche sicherheitspolitische Ansätze erforderlich. Hieraus erwächst die Forderung, Cyber-Verteidigung in alle einschlägigen Prozesse zur Gewährleistung innerer und äußerer Sicherheit zu integrieren.

Grundsätzlich ist dabei eine gestaffelte Abwehr in der Tiefe, vergleichbar einer virtuellen Festungsanlage mit mehreren Verteidigungsringen, vorzusehen. Dabei sind geeignete Kombinationen aus Taktik, Technik und Verfahren zu wählen. Da heute im Grunde alle Systeme und Komponenten im CIR über das Internet miteinander verbunden sind, gilt es zu verhindern, dass durch Eindringen, Kompromittieren oder Lahmlegen einzelner Netzanteile sofort die gesamte Netzstruktur in Mitleidenschaft gezogen wird. Deshalb sind die Systeme bereits in der Architektur gehärtet und resilient auszulegen, was u.a. redundante Komponenten und Fähigkeiten zur flexiblen Reaktion bei der Abwehr von Angriffen sowie bei der Wiederherstellung von Funktionalitäten verlangt.

Etliche Experten können sich Cyber-Angriffe im Grunde nur als ergänzende oder begleitende Maßnahmen zu anderen (kinetisch wirkenden) militärischen Handlungen in einem bewaffneten Konflikt vorstellen. Gerade dafür ist eine vollständige Integration von Operationen im CIR mit Operationen in den klassischen Domänen Land, Luft, See und Weltraum zwingend geboten; also ein echter „Kampf der verbundenen Waffen“.

Defensive oder auch offensive Cyber-Verteidigungs-Fähigkeiten werden die anderen, klassischen Fähigkeiten nicht überflüssig machen. Sie stellen allerdings eine notwendige, künftig unverzichtbare Ergänzung des Fähigkeits-Spektrums dar.

Ob ein Cyberangriff den Verteidigungs- oder Bündnisfall auslösen kann, das ist letztendlich eine politische Entscheidung, die im konkreten Fall unter Bewertung der Gesamtlage erwogen und evtl. getroffen werden muss. Cyber-Aktivitäten als Mittel der Kriegsführung werden also in der Regel innerhalb eines politischen Kontextes stattfinden. Sie sind grundsätzlich ebenfalls den entsprechenden politischen und rechtlichen Auflagen unterworfen, die bereits bisher für klassische militärische Einsätze gelten.

Die Art und Weise, wie Cyber-Angriffe eingesetzt werden können, berührt natürlich auch wesentliche Aspekte des Konfliktvölkerrechts, insbesondere die Regeln für die

- Anwendung von Gewalt in bewaffneten Konflikten („Recht im Krieg“, ius in bello) und die
- Regeln, wann überhaupt zur Gewalt gegriffen werden darf („Recht zum Krieg“, ius ad bellum).

Die NATO Mitgliedstaaten haben auf dem Gipfel in Warschau 2016 ihre Entschlossenheit bekräftigt, bei der Cyber-Verteidigung im Einklang mit dem Völkerrecht einschließlich der Charta der Vereinten Nationen, dem humanitären Völkerrecht und den internationalen Menschenrechtsnormen vorzugehen. Sie haben zugleich versichert, den Grundsatz der Zurückhaltung zu verfolgen und die Erhaltung von Frieden, Sicherheit und Stabilität im CIR weltweit zu unterstützen.

Als gesamtstaatliche oder gesamtpolitische Aufgabe und Herausforderung erfordert die Gewährleistung von Sicherheit im CIR eine intensive Zusammenarbeit aller relevanten staatlichen und nicht-staatlichen Stellen. Risiken und Gefahren im CIR sind ein transnationales Problem, denen wirksam nur kooperativ und multinational begegnet werden kann. Weitreichende Kooperation in einem umfassend vernetzten Sicherheitsansatz gilt somit als Grundvoraussetzung für Erfolg und Effizienz von Cyber-Verteidigung. Die Politik ist diesbezüglich gefordert, die notwendigen Rahmenbedingungen und Voraussetzungen zu schaffen.

Die Schutz-, Abwehr- und Verteidigungsmaßnahmen werden künftig verstärkte Investitionen in die Cyber-Sicherheit erfordern. Sie werden letztlich aber nur dann nachhaltig sein, wenn eine kontinuierliche Aus- und Weiterbildung des Personals in Cyber-Angelegenheiten stattfindet, die mit der hohen Entwicklungsdynamik im CIR Schritt hält.

Darüber hinaus sind geeignete Verfahren zur Bewältigung von Eventualfällen im CIR („Contingency Cases“) zu entwickeln und praktisch zu erproben. Die darin festgelegten Führungs-, Entscheidungs- und Durchführungsverfahren müssen regelmäßig im Zusammenwirken der Verantwortlichen auf allen Ebenen auch praktisch geübt werden. Dies gilt gleichermaßen für die EU und die NATO.

Statements der Panellisten

Professor Dr. Peter Martini, der Leiter des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), geht in seinem Beitrag unter dem Titel „Cyber-Verteidigung – Eine gesamtstaatliche Aufgabe“ auf einige spezielle Aspekte sowie Schwerpunkte ein und schildert ausgewählte praktische Beispiele.

Generalmajor Dipl.-Inform. Jürgen Setzer, der Stellvertretende Inspekteur des Cyber- und Informationsraumkommandos und Chief Information Security Officer der Bundeswehr (CISOBw), geht der Frage nach „Welche Rolle werden künftig passive und aktive Cyber-Verteidigungs-Fähigkeiten als integrierte Anteile von Operationen in der Militärstrategie einnehmen?“

Das NATO Cooperative Cyber Defence Center of Excellence (CCDCoE) in Tallinn spielt eine herausragende Rolle in der internationalen Cyber-Verteidigungsgemeinschaft. Besonders das "Tallinn Manual" ist ein weithin bekanntes und wichtiges Produkt des Zentrums. Die Direktorin des CCDCoE, M.A. Merle Maigre, präsentiert ihre Sicht auf die Cyber-Verteidigung in der

NATO. Sie fokussiert ihre Betrachtungen insbesondere auf die politischen und operativen Implikationen der kooperativen Cyber-Verteidigung.

Merle Maigre stellt Cyberverteidigung der NATO als integralen Bestandteil der Kollektiven Verteidigung des Bündnisses heraus. Auch mit Hinweis auf die Ergebnisse des NATO-Gipfels 2018 in Brüssel erwähnt sie den beschlossenen Aufbau eines Cyber-Operationszentrums im NATO Hauptquartier, die Integration der Cyber-Verteidigungselemente in die Struktur des Allied Command Operations (ACO), dabei insbesondere auch die Integration der entsprechenden Prozesse in die Operationsplanung, die Bedeutung von Abschreckungsfähigkeiten im Cyberraum und die Notwendigkeit umfassender Kooperation in der Cyberverteidigung, vor allem im Bereich Nachrichtengewinnung und Aufklärung. Zugleich erwähnt sie, dass die NATO selbst nur defensive oder passive Fähigkeiten für die Cyberverteidigung besitzt und hinsichtlich offensiver oder aktiver Cyberverteidigungsfähigkeiten auf die Bereitstellung solcher Fähigkeiten seitens der Mitgliederstaaten angewiesen ist.

Wann immer Fragen der Cyber-Verteidigung diskutiert werden, bezeichnen Experten Israel als eine der erfahrensten und professionellsten Nationen in dieser Arena. Daher kommt den Aussagen von Herrn Iddo Moed besondere Bedeutung zu. Iddo Moed ist der Cyber Security Coordinator im israelischen Außenministerium.

Moed bezeichnet Cyberverteidigung als Erweiterung der bereits bestehenden Sicherheitsdomänen. Zugleich weist er darauf hin, dass bei der Cyberverteidigung enge und vertrauensvolle Zusammenarbeit unbedingt erforderlich ist. Angesichts globaler Vernetzung seien im Bedarfsfall insbesondere gemeinsame oder verbundene Verteidigungsmaßnahmen auch jenseits der nationalen Grenzen notwendig. Dabei gelte es internationales Recht zu beachten und einzuhalten. Zugleich unterstreicht er, dass 95% der Cyberaktivitäten im zivilen Umfeld stattfinden und dementsprechend eine enge zivil-militärische Kooperation geboten ist.

<u>Erkenntnisse aus der Diskussion</u>

In der Diskussion wurden u.a. angesprochen:

- Klarstellung, wann von einem „Cyberkrieg“ gesprochen werden kann und muss. Hierbei wurde unterstrichen, dass der Cyberkrieg ist eine äußerst hybride Kriegsform darstellt, die in der Regel unterhalb der Schwelle stattfindet, die im Völkerrecht als konventioneller Krieg gilt.

- Die erhöhte globale Cyber–Gefährdungslage erfordert eine Revision veralteter nationaler Cyber-Strategien insbesondere hinsichtlich kontroverser Werkzeuge wie offensiven Cyberoperationen, Hack Backs und Cyber-Abschreckung („Cyber Deterrence“). Während andere Nationen derzeit proaktiv neue Teilstrategien formulieren und der Begriff „Cyber Deterrence“ fest in der strategischen Gesamtarchitektur verankert wird, hat Deutschland hier nach Meinung einiger Experten Nachholbedarf.

- Eine zuverlässige Attribution ist letztlich der wichtige Schlüssel für Entscheidungen über aktive Cyber-Abwehrmaßnahmen. Die derzeit vorhandenen Fähigkeiten zur "Attributierung“, insbesondere die „on-line“ oder „real-time“ Fähigkeiten haben noch nicht ein hinreichendes

Maß an Zuverlässigkeit erreicht, die für politische und / oder militärische Entscheidungen über aktive oder offensive Cyber-Verteidigung ausreichen.

- Weitere Anstrengungen sind erforderlich, um Cyberverteidigung wirksam und effizient in das gesamte Spektrum der kombinierten gemeinsamen Operationen – im Sinne des Kampfs verbundener Waffen („Combined-Joint-Operation“) zu integrieren.

- Das rechte Maß der Mittel, also letztlich die Kosten-Nutzen-Kalkulation, ist ein entscheidender Faktor jeder Kriegs- oder Operationsführung. Im operativen Bereich Cyber- und Informationsraum hat sich das bisher erfahrene Kostengleichgewicht zwischen Angriff und Abwehr deutlich verändert. In der digitalen Welt sind Angriffe vergleichsweise billig; Verteidigung hingegen ist teuer und komplex. Dennoch kann angesichts der Attributionsproblematik dem Angriff bzw. offensiver Cyberverteidigung nicht einfach der Vorzug gegenüber defensiven Maßnahmen erteilt werden.

- Die inhärent virtuelle (technologische) Natur des Cyberraums hat einen beträchtlichen Einfluss auf elementare Abschreckungsaspekte. Die Cyberforensik muss grundsätzlich virtuellen Spuren folgen, die leicht manipulierbar sind. Deswegen müssen Cyberabschreckungs-Fähigkeiten insbesondere invasive Werkzeuge für die Gewinnung notwendiger Zusatzinformationen in Betracht ziehen, um eine zuverlässige und zeitnahe Attribution zu erreichen.

Zusammenfassung und Ausblick:

Instabilität sowie konkrete Angriffs-Risiken und Bedrohungen im Cyberraum stellen eine Gefahr von potentiell strategischer Dimension dar. Bereits ein nicht funktionierendes Internet würde Gesellschaft, Politik und Wirtschaft innerhalb kurzer Zeit ins Chaos stürzen. Gerade die digitalisierte Welt braucht ein hinreichendes Maß an Resilienz und Sicherheitsvorsorge in allen Lebensbereichen.

Angesichts der Komplexität der Domäne CIR ist die Anwendung einfacher Analogieschlüsse von klassischen Domänen auf die Domäne CIR mit Vorsicht zu behandeln. Für die Übertragung klassischer Erkenntnisse der Kriegs- oder Operationsführung auf Konflikte mit hybrider Bedrohung und insbesondere auf Operationen im CIR bedarf es jeweils eingehender spezifischer Analysen und Bewertungen und letztlich auch kreativer, innovativer Denkansätze. Dies ist jedoch kein Mysterium. Vielmehr kann und muss gerade auch die neue Domäne CIR bei strategischen und operativen Problemen und Planungen logisch stringent erschlossen und mit ihren Fähigkeiten innovativ und integrativ im Rahmen der Gesamtverteidigungsplanung genutzt werden. Es bedarf also jeweils intelligenter Transferleistung.

Alle verantwortlichen politischen und militärischen Führungskräfte sollten künftig über hinreichende Kenntnisse zur Bewertung und Nutzung der fünften sicherheitspolitischen Domäne im Kontext gesamtstaatlicher Sicherheitsvorsorge verfügen. Die dafür notwendige Lehre sowie die konkrete Aus- und Weiterbildung, aber auch die unverzichtbare Inübunghaltung sollten in Zukunft integrale Bestandteile der entsprechenden Lehrgänge und Übungen sein. Letztlich ist die Forderung zu erheben, dass die politischen und militärischen Führungsstrukturen ebenfalls entsprechend auf die Herausforderungen des CIR ausgerichtet und angepasst werden müssen, um

künftig den höchst anspruchsvollen zeitlichen Kriterien und auch der potentiell strategischen Dimension von Risiken und Bedrohungen im CIR wirkungsvoll begegnen zu können.

Im Falle des Falles wird es unverzichtbar sein, unverzüglich die Gesamtlage zu beurteilen, die erforderlichen politischen und militärstrategischen Entscheidungen aufgrund einer umfassenden Lagebeurteilung zu treffen und alle notwendigen Verteidigungsmaßnahmen in einem umfassenden, verbundenen Ansatz reaktionsschnell, koordiniert, gezielt und effizient durchzuführen. Das hierzu erforderliche theoretische Wissen, die grundlegenden strategisch-operationellen Kenntnisse und die entsprechenden praktischen Fähigkeiten müssen von allen beteiligten zivilen und militärischen Akteuren hinreichend sicher beherrscht werden. Eine entsprechende Ausbildung und auch Inübunghaltung des Führungspersonals aller kritischen Bereiche und Ebenen ist für die Gewährleistung von erfolgreicher Sicherheitsvorsorge im Cyber-Zeitalter eine entscheidende und in dieser Brisanz wohl bisher nicht gekannte Grundvoraussetzung.

Die Planung und Umsetzung von "effect-based operations" in der Cyber-Domäne erfordert letztlich eine vollständige Integration in gemeinsame Operationen und entsprechend intensiv abgestimmte Aus- und Weiterbildung auf verschiedenen Ebenen.

Laut Clausewitz ist "Krieg die Fortsetzung der Politik, indem man andere Mittel hinzufügt". Daher sollten Politiker und militärische Führer sich der verfügbaren "Cyber-Verteidigungs-Toolbox" bewusst sein und damit hinreichend vertraut sein.

Nichtstaatliche Cyberakteure verfügen inzwischen über Cyberfähigkeiten, die zuvor ausschließlich Nationalstaaten vorbehalten waren. Cybersicherheit muss darauf eingestellt sein; sie zu gewährleisten ist eine allgemeine Regierungsaufgabe. Insbesondere müssen die strategischen Risiken und Bedrohungen, die von Cyberspace ausgehen, angemessen berücksichtigt und als integrale Elemente in eine zukunftsorientierte Strategie integriert werden. Dies muss auf einem ganzheitlichen Ansatz beruhen, der alle relevanten Faktoren und potenziellen Akteure berücksichtigt.

Cyberverteidigung muss ein integraler Bestandteil der allgemeinen Landesverteidigung, der kollektiven Verteidigung in der Allianz bzw. im Nordatlantischen Bündnis oder auch des Krisenmanagements im Rahmen einer Koalition sein. Die Entwicklung, Vermittlung und Erprobung von Strategien, Taktiken und Verfahren für den Einsatz in der Cyber-Domäne muss grundsätzlich auf die gleiche Weise erfolgen wie in den konventionellen Domänen Land, Luft, See und Weltraum. Vor allem aber müssen die allumfassende Durchdringung aller konventionellen Domänen durch Cyber und die spezifischen Eigenschaften der Cyber-Verteidigung berücksichtigt und in der Sicherheitsvorsorge hinreichend verankert werden.

Nationale und multinationale sowie weitvernetzte Lösungen, taktische Flexibilität, ständige Adaption der Cyber-Verteidigungsfähigkeiten durch technische Innovation und umfassende zivil-militärische Kooperation gelten als wichtige Schlüssel zum Erfolg in der Cybersicherheit. Im Rahmen eines effektiven ressortübergreifenden Ansatzes müssen insbesondere verstärkte koordinierte Planung und gemeinsame Nutzung ziviler und militärischer sowie staatlicher und nichtstaatlicher Kräfte und Ressourcen der Cyber-Abwehr und Verteidigung in nationale und multinationale Strukturen und Prozesse einbezogen und effizient umgesetzt werden.

Angesichts wachsender Risiken und Bedrohungen für die Sicherheit einerseits und begrenzter Ressourcen andererseits besteht eine zunehmende Dringlichkeit für umfassende Zusammenarbeit

aller beteiligten Parteien und Akteure. Insbesondere enge Kooperation und sich komplementär ergänzende gemeinsame Aktionen aller relevanten nationalen Regierungsressorts sowie eine enge zivil-militärische Zusammenarbeit mit den beteiligten internationalen Institutionen und Organisationen sind ein Gebot der Stunde. Synergien gilt es zu erschließen und zu nutzen wo immer sich die Gelegenheit dazu bietet.

In allen möglichen gegenwärtigen und zukünftigen Missionen der Streitkräfte im Rahmen von Landes- und Bündnisverteidigung sowie internationalem Krisenmanagement ist die gegenseitige vertrauensvolle Zusammenarbeit der beteiligten Kräfte einer Allianz oder einer Koalition in der Cyberdomäne von größter Bedeutung. Ein ungehinderter Austausch oder Transfer von missionsbezogenen Daten in einer sicheren Umgebung, die allen truppenstellenden Nationen zugänglich ist, gilt dabei als Grundvoraussetzung.

Risiken und Bedrohungen, die vom Cyberspace ausgehen, können innerhalb kürzester Zeit strategische Dimensionen annehmen. Daher ist es dringend notwendig, eng zusammenzuarbeiten, um eine wahrhaft kollektive Cyber-Verteidigung zu unterstützen. Nach dem bewährten Konzept der "combined-joint-operations" müssen Cyber-Operationen daher vollständig in das ganzheitliche Planungs- und Maßnahmenspektrum von Sicherheit und Verteidigung integriert werden.

Angesichts der besonderen Brisanz durch höchst zeitkritische Bedingungen und Abläufe in der Cyberdomäne sind, analog zu den bisher bekannten Notfallplänen für kritische Regionen, künftig funktionale Notfallpläne für die Cyber-Abwehr/Verteidigung („Responsive Protection“) unverzichtbar. Hinreichende Resilienz, also vor allem die Aufrechterhaltung und Gewährleistung der Funktionalität kritischer Infrastrukturen und Dienste im Falle von Störungen oder Angriffen, gilt es zu garantieren.

Die Tatsache, dass bisher keine spezifischen völkerrechtlichen Vorgaben für den Cyber-Raum als Domäne militärischer Auseinandersetzungen gegeben sind, bedeutet nicht, dass hier ein rechtsfreier Raum vorliegt. Die geltenden Regelungen des Friedensvölkerrechts wie des Rechts des bewaffneten Konflikts finden grundsätzlich Anwendung. Dies führt zwar zu Herausforderungen für das Völkerrecht, hat aber keine unüberwindlichen Schwierigkeiten zur Folge.

Der Einsatz militärischer Cyber-Fähigkeiten in bewaffneten Konflikten unterliegt den jeweils einschlägigen Vorgaben des humanitären Völkerrechts. Als besondere Herausforderungen erweisen sich jedoch u.a. die folgenden Aspekte:

- Die Verknüpfung militärisch und zivil genutzter Netzwerke wirft die Frage nach Gewährleistung des Trennungsgebots auf.
- Die äußerst schwierige Voraussehbarkeit oder Abschätzung der Folgen eines Cyber-Angriffs bzw. Begrenzung von Kollateralschäden berührt das Prinzip des Exzess Verbots bzw. der Verhältnismäßigkeit.
- Durch den Einsatz von Firmenunterstützung, Outsourcing von IT-Diensten etc. gewinnt das Handeln von Zivilpersonal im Auftrag von Streitkräften oder Privater aus eigenem Antrieb besondere Brisanz, insbesondere muss dabei der Kombattantenstatus bzw. der Teilnahme von Zivilpersonal an Cyber-Kampf-Handlungen einer eingehenden Betrachtung unterzogen werden.

- Nicht zuletzt stellt sich die Frage, ob die klassische Definition von Konfliktgebieten oder der Neutralität von Staaten im Cyber-Raum bzw. Cyber-Zeitalter noch Gültigkeit besitzt, angesichts der weltweit vernetzten IT-Infrastruktur.

Ungeachtet juristischer Definitions- oder Abgrenzungsprobleme im Einzelnen, kann festgestellt werden, dass militärische Cyber-Offensivfähigkeiten allein aufgrund ihrer Art als solche keinen Verstoß gegen völkerrechtliche Bestimmungen darstellen. Im Sinne der Verhältnismäßigkeit bzw. Vermeidung von Gewalt gegen Personen können vermutlich offensive Cyber-Operationen sogar eher humanitäre Standards einhalten als traditionelle kinetische militärische Vorgehensweisen.

Eng damit verbunden sind natürlich ebenfalls stets die Beachtung des Prinzips der Verhältnismäßigkeit von Maßnahmen sowie die Frage nach Möglichkeiten zur Ächtung bzw. zum Bann von bestimmten Cyber-Angriffs-Formen.

Angesichts der international divergierenden Standpunkte zur Cyber-Politik erscheint es auf absehbare Zeit eher unwahrscheinlich, dass verbindliche völkerrechtliche Regelungen und Verträge im Hinblick auf operative oder gar militärische Cyber-Abwehr oder Verteidigung geschaffen werden. Auch eine sicher wünschenswerte Anlehnung an traditionelle Instrumentarien der Rüstungskontrolle dürfte für den Cyberraum nur schwer zu erreichen sein.

Im Falle des Falles wird es unverzichtbar sein, unverzüglich die Gesamtlage zu beurteilen, die erforderlichen politischen und militärstrategischen Entscheidungen aufgrund einer umfassenden Lagebeurteilung zu treffen und alle notwendigen Verteidigungsmaßnahmen in einem umfassenden, verbundenen Ansatz reaktionsschnell, koordiniert, gezielt und effizient durchzuführen. Das hierzu notwendige theoretische Wissen, die grundlegenden strategisch-operationellen Kenntnisse und die entsprechenden praktischen Fähigkeiten müssen von allen beteiligten zivilen und militärischen Akteuren hinreichend sicher beherrscht werden. Eine entsprechende Ausbildung und auch Inübunghaltung des Führungspersonals aller kritischen Bereiche und Ebenen ist für die Gewährleistung von erfolgreicher Sicherheitsvorsorge im Cyber-Zeitalter eine entscheidende und in dieser Brisanz wohl bisher nicht gekannte Grundvoraussetzung.

Letztlich gilt: Sicherheit im global vernetzten CIR geht alle an.

Zum Autor: Generalleutnant a.D. Dipl.-Inform. Kurt Herrmann ist Präsident der Clausewitz-Gesellschaft e.V.