Virus an Bord?

„Maritime Cyber“

Eike Tammen, Marco Schäfer und Mike Gronert

Stellen sie sich vor, Sie sind Kommandant einer seegehenden Einheit. Mit großem Engagement und unter vollem Einsatz haben sie Ihre Besatzung, Ihr Schiff und selbstverständlich sich selbst für den Einsatz vorbereitet. Das Personal wurde regelmäßig aus- und weitergebildet, Übungen und Manöver wurden gefahren und Ihre Einheit ist technisch auf dem aktuellen Stand.

Foto: PIZM

Systembetreuer in der OPZ

Sie befinden sich im Rahmen einer Maritime Interdiction Operation im UN-Einsatz im Mittelmeer und neben den üblichen technischen und systemspezifischen Problemen gab es bislang keine besonderen Vorkommnisse oder Ausfälle. Ihre Besatzung ist erfahren, die Soldaten kennen das Schiff mit seinen Anlagen und Waffen wie ihre Westentasche und „alle möglichen“ Verfahren und Abläufe wurden viele Male geübt. Alle? Nach einem Versorgungs- und Instandsetzungsaufenthalt in einem befreundeten Hafen geben sie den Befehl zum Auslaufen. Doch schon kurz nach dem Passieren der Molenköpfe geschehen unerwartete Dinge. Das Radar zeigt optisch verifizierte Kontakte nicht an. Ihr Navigationssystem in bewährter Verbindung mit dem lieb gewonnenen GPS zeigt Ihnen entgegen der Realität, dass Sie nicht vor gerade besuchtem Hafen stehen, sondern mitten im Pazifik mit 6 kn Fahrt nach Süden steuern. Ihre Antriebsdiesel fallen ohne ersichtlichen Grund von Zeit zu Zeit aus und auch die Bildschirme in der OPZ schalten größtenteils auf Schwarz um. Zudem meldet Ihr Waffeneinsatzoffizier elektronische Fehlfunktionen an fast allen Effektoren. Nun schießen Ihnen Fragen durch den Kopf, auf die Sie keine Antwort haben.

Was passiert hier gerade? Wie ist das überhaupt möglich? Und vor allem: Wie reagiere ich jetzt darauf? Genau in diesem Moment steht ein Bootsmann aus dem Bereich des Elektronischen Kampfes (EloKa) hinter Ihnen und wirft ein Stichwort auf die Brücke: Cyberattacke...?!

Unterbrechen wir dieses Gedankenspiel hier. Ist ein derartiges Szenario möglich, oder nur reine Fiktion und viel zu weit hergeholt?

Ein Blick auf einige „Vorfälle“ der letzten zehn Jahre

Im Jahr 2007 legte eine Denial of Service-Attacke (DoS)[1] in Estland staatliche Organe, Banken und Medien für mehrere Wochen lahm. Ein Jahr später wurde der Computerwurm „Conficker“ zum ersten Mal registriert und ist seitdem in verschiedenen Varianten weiterhin im Umlauf. 2010 tauchte wieder ein Computerwurm auf mit dem Namen „Rootkit.TmpHider“, der später unter „Stuxnet“ bekannt wurde. Dieser wurde speziell zum Angriff auf ein System zur Überwachung und Steuerung (SCADA-System) des Herstellers Siemens entwickelt. Gerichtet war der Angriff „offenbar gezielt“ gegen das iranische Atomprogramm, wo zum damaligen Zeitpunkt der Großteil der betroffenen Systeme eingesetzt wurde. Es kam vermehrt zu außerplanmäßigen Störungen beim Betrieb der Uranzentrifugen. 2015 waren gleich drei Vorfälle in den Medien sehr präsent. Zum einen hatten Hacker des IS den Twitter-Account und den Youtube-Kanal des Zentralen Einsatzkommandos der US-Streitkräfte (USCENTCOM) übernommen und eigene Propaganda eingespielt. Beide Accounts wurden nach ca. einer Stunde vom Netz genommen. Danach wurde der französische Fernsehsender „TV 5 Monde“ gehackt. In der Folge waren elf Kanäle für Stunden gestört. Des Weiteren wurde 2015 der Deutsche Bundestag Opfer einer Cyberattacke der Gruppe „CyberBerkut“, bei der Daten von mindestens 16 Abgeordneten ausspioniert wurden. Ende 2015 sorgte der „BlackEnergy“-Angriff in Kiew für massive Probleme bei der Stromversorgung und am Flughafen. Im Mai 2017 machte das Schadprogramm „Wanna Cry“ auf sich aufmerksam. Dieser bislang größte Cyber-Angriff betraf 200.000 Organisationen und Einzelpersonen weltweit, darunter Krankenhäuser, Logistikunternehmen und auch die Deutsche Bahn. Die bislang aufgeführten Fälle betrafen den maritimen Bereich allenfalls am Rande. Jedoch nur drei Monate nach Wanna Cry wurde unter vielen anderen Firmen die Reederei Maersk Opfer einer Variante der Schadsoftware „Petya“. Diese legte Computersysteme und Terminals lahm und beeinträchtigte die Containerschifffahrt wochenlang. Der geschätzte Schaden wurde allein von Maersk mit 200–300 Mio. Dollar beziffert. Last, but not least: Was geschah tatsächlich im April 2014 im Schwarzen Meer und 2016 in der Ostsee auf der USS „Donald Cook“? Angeblich fielen nach Überflügen russischer Jets die verschiedensten Systeme aus. Wurde hier tatsächlich eine Cyber-Waffe eingesetzt?

An dieser Stelle soll es einmal dahingestellt bleiben, ob die „Cyberangriffe“ auf die „Donald Cook“ Propaganda oder Fakt sind. Viel wichtiger ist die Auseinandersetzung mit der Tatsache, dass Cyber-Attacken ähnlicher Ausprägung möglich sind und es auch in Zukunft sein werden. Zur Verdeutlichung sollte hier betrachtet werden, dass über 600 Mio. Schadprogammvarianten bekannt sind und jeden Tag knapp 400.000 neue hinzukommen (Stand Mitte 2016).

Die Fragen, die sich die Deutsche Marine mit Blick auf die fortschreitende Vernetzung nun stellt, sind folgende: Sind wir auf solche Cyber-Attacken/Angriffe (ausreichend) vorbereitet? Wie können wir den Cyber-Raum zur Unterstützung eigener Operationen nutzen? Wird die „neue" Warfare Area Cyber den Seekrieg, wie wir ihn bislang kannten, verändern?

Sachstand: Der Anfang ist gemacht

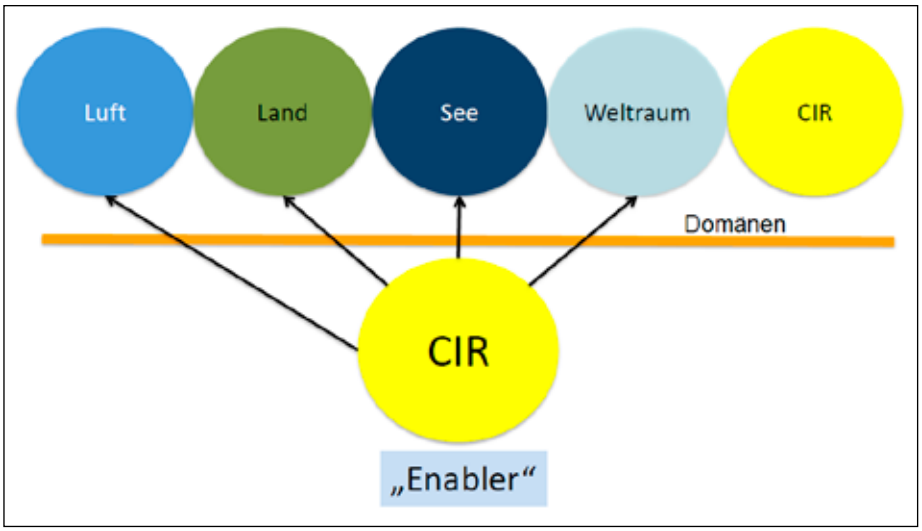
Auf dem NATO-Gipfel in Warschau im Juli 2016 wurde von den Bündnispartnern eine „Vereinbarung zur Cyber-Abwehr" verabschiedet und der Cyber- und Informationsraum als neue Domäne festgelegt. Im virtuellen Raum sollen die Bündnispartner zukünftig genauso gut verteidigen können, wie in der Luft, auf dem Land und zur See. Zudem hat allgemein die Nutzung von Informationstechnologie (IT), die Digitalisierung und Vernetzung an Bord sowie die vernetzte Operationsführung einen derart tiefgreifenden Einzug in die Domäne der Kriegsführung und alle anderen Domänen gehalten, dass diese unter Ausschluss der Nutzung von IT kaum noch, nur noch erschwert oder gar nicht mehr möglich ist. Nach deutscher Auffassung ist auch die hier genutzte IT Bestandteil des Cyber- und Informationsraumes. Daher spricht man davon, dass Cyber als eigene Domäne und gleichzeitig „Enabler" (Helfer/Befähiger) zu betrachten ist.

Um den Herausforderungen im neuen Operationsraum angemessen begegnen zu können, wurde im Oktober 2016 im BMVg die Abteilung CIT (Cyber und IT) eingerichtet. Darauf folgte im April 2017 die Aufstellung des Militärischen Organisationsbereiches (MilOrgBer) Cyber und Informationsraum (CIR), mit dem Kommando CIR. Diesem wurden das Kommando Strategische Aufklärung (KdoStratAufkl), das Kommando Informationstechnik der Bundeswehr (KdoITBw), das Zentrum für Geoinformationswesen der Bundeswehr (ZGEoBw) sowie das Zentrum für Operative Kommunikation (ZOpKom) unterstellt. Das Kommando CIR ist somit für die Dimension Cyber- und Informationsraum als Ganzes verantwortlich. Es stellt den Schutz und Betrieb des IT-Systems der Bundeswehr, sowohl im Inland als auch im Einsatz sicher, stärkt die Fähigkeiten im Bereich Aufklärung und Wirkung im Cyber- und Informationsraum und entwickelt diese weiter. Der Begriff „Cyber" umfasst nach deutschem Verständnis mehr als nur „hacken und gehackt werden". Unter dem Begriff vereinen sich die Fähigkeiten der IT-Technik (Hardware, Software, Security, Cyber Operations etc.) des Militärisches Nachrichtenwesens sowie des Elektronischen Kampfes und des Geo-Informationswesens.

Für die Bearbeitung marinespezifischer Aspekte und Interessen im Bereich Cyber wurde im Marinekommando (MarKdo) die „AG Maritime Cyber" eingerichtet. Sie setzt sich aus Angehörigen aller Abteilungen des MarKdo zusammen und befasst sich u. a. mit der Entwicklung/Implementierung von Taktiken und Verfahren der Cyber Warfare im maritimen Bereich. Dabei müssen die Einzelaspekte Cyber and Information Exploitation, Defensive & Offensive Cyber, Information Warfare, die rechtlichen Hintergründe und Zusammenhänge sowie die Zuständigkeiten und die materielle Ausstattung betrachtet werden. Das benötigte, umfangreiche Fähigkeitsportfolio der Marine im kritischen Bereich Cyber macht deutlich, dass die Befassung in Nebentätigkeit mittels einer Arbeitsgruppe nicht hinreichend umgesetzt werden kann. Aufgrund der stetig wachsenden Anforderungen und Bedarfe in diesem Bereich muss künftig darüber nachgedacht werden, dieses Aufgabenportfolio fest in der Struktur der Marine abzubilden.

Einen weiteren kritischen Faktor stellt dabei das Personal aus dem Tätigkeitsfeld Cyber und IT dar. Die allgemein schon angespannte Personallage ist im Bereich Cyber und IT bei der Marine schon jetzt besonders ausgeprägt. Zudem fordert der Aufbau des MilOrgBer CIR auf ca. 13.700 Personen, mit zum Teil aus anderen OrgBer abgezogenen Soldaten, z.B. die

Grafik: Autorenteam



Cyber ist als eigene Domäne und gleichzeitig als „Enabler“ zu betrachten

Abgabe von Personal und Dienstposten aus dem Bereich IT-Sicherheit Marine an das Kommando CIR, seinen Tribut. Erschwert wird die Gewinnung und Bindung von Personal mit der benötigten Fachkompetenz durch die direkte Konkurrenz zu anderen Behörden und der teilweise erheblich flexibleren und oftmals finanziell attraktiveren Wirtschaft.

Herausforderung für die Marine

Als Basis steht die Gewinnung und Ausbildung von Personal mit Cyber-Know-how. Zusätzlich muss das Bewusstsein für das Handeln und die Gefahren im Cyberraum (Cyber Awareness) geschaffen bzw. erweitert werden, insbesondere auch bei Soldaten aus Fachgebieten ohne direkten IT-Bezug. Ohne ausreichende fachliche Kompetenz im Operationsfeld Cyber und einem verantwortungsvollen, sachgemäßen Umgang mit IT-Systemen, wird es allein durch technische Maßnahmen nicht möglich sein, Cyber-Attacken zu verhindern. Der Mensch mit seinen natürlichen Schwächen ist auch in diesem Bereich die häufigste Fehlerquelle!

Im Bereich der in Nutzung oder Beschaffung befindlichen IT-Systeme (Hard- und Software) gilt es, zeitnah vorhandene Schwachstellen zu identifizieren und zu beseitigen. Hierzu können neben der Analyse einzelner IT-Komponenten unter „Laborbedingungen“ auch Cyber-Tests bei schwimmenden Einheiten als Gesamtsystem im Normalbetrieb durchgeführt werden.

Die Implementierung von umfangreicheren Cyber-Übungsanteilen während klassischer maritimer Manöver auf nationaler und internationaler Basis ist anzustreben. Gemeint sind an dieser Stelle z.B. Penetration Tests[2], längerfristige Kommunikationsausfälle, Days without Space[3], GPS-Störungen oder die Einspielung falscher Informationen. Die Einheit und Ihre Besatzung soll im Zuge dieser Übungsanteile nicht nur darauf vorbereitet werden, gegen Cyber-Angriffe und mögliche IT-Ausfälle vorzugehen, sondern ihren primären Auftrag auch weiter fortsetzten können. Das bedeutet, dass Redundanzen gebildet und ggf. Verfahren vertieft werden müssen, die sich nicht auf vernetzte IT abstützen.

Des Weiteren gilt es, künftig die Berücksichtigung maritimer Faktoren im Planungs- und Beschaffungsprozess im Bereich der IT-Projekte voranzutreiben. Einheiten der Marine dürfen nicht als einfache mobile Einheiten betrachtet werden, sondern müssen als eigenständige mobile Dienststellen, ja sogar als schwimmende Serverfarmen mit erhöhten Anforderungen an Vernetzung, Anbindung und Autarkie in teilweise widrigen Umgebungen verstanden werden.

Um diesen besonderen Anforderungen der Marine gerecht werden zu können, muss in Zukunft gewährleistet sein, dass auch in der übergeordneten und umfassenden Prozessablauf- und Aufbauorganisation Cyber an den fachlich exponierten Stellen maritimer Sachverstand vertreten ist. Sind schließlich die Rahmenbedingungen klar geregelt und die Berücksichtigung maritimer Bedürfnisse sichergestellt, gilt es, nicht zuletzt Augenmaß bei der Einführung neuer, modernster Informationstechnologie, unbemannter/autonomer Systeme und neuester Kommunikationsmittel zu halten. Vor jeder weiteren Digitalisierung maritimer Verfahren und Abläufe muss der tatsächliche operative Nutzen eines neuen Systems Kern der Betrachtung sein. Dieser muss gegen mögliche Schwachstellen/Fehlerquellen abgewogen werden: Must have or only nice to have?

Resümee/Zusammenfassung

Ein Anfang ist sowohl streitkräfteübergreifend als auch innerhalb der Marine gemacht: Die Auseinandersetzung mit dem Thema Cyber ist im Gange. Um den aktuellen und künftigen Bedrohungen innerhalb dieser „neuen“ Domäne gewachsen zu sein und selbst in ihr agieren zu können, gilt es, die Zuständigkeiten zwischen den Organisationsbereichen abzustecken und zu formulieren sowie benötigte Fähigkeiten auszubauen bzw. zu erlangen. Teilstreitkraftspezifische Kompetenzen, Fähigkeiten und Bedarfe müssen beachtet und in die streitkräfteübergreifende Planung, Organisation und Steuerung eingebracht werden. Sind einzelne Fähigkeiten nicht in eine TSK-übergreifende Organisation zu implementieren, müssen diese TSK-spezifisch abgebildet und mit einem angemessenen Personalkörper ausgestattet werden. Derzeit befinden sich einige grundlegende Regelungen unter Federführung des Kommandos CIR in der Bearbeitung. Im Bereich Maritime Cyber ist, auch in Abhängigkeit übergeordneter und teilweise noch zu erstellender Vorgaben, viel zu tun.

Greifen wir das Eingangsszenario noch einmal auf. Denkbar wären hier u.a. zwei Ausgänge.

Szenario Nummer eins: Alle Verantwortlichen und Beteiligten haben im Vorfeld gemeinschaftlich Vorsorge getroffen, technische und personelle Maßnahmen koordiniert umgesetzt sowie entsprechende Verfahren regelmäßig geübt. Dadurch war es nach der Verdachtsäußerung des ELOKA-Bootsmanns möglich, unter Zuhilfenahme des gemeinsam mit dem Kommando CIR für diesen Fall entwickelten Notfallplans zumindest die Antriebssektion und die Navigationseinrichtungen relativ schnell wieder betriebsfähig zu machen. Nachdem anschließend der an Bord befindliche Cyber-Soldat alle erforderlichen Analysen durchgeführt und die Ergebnisse an das Kommando CIR gemeldet hat, konnte die Schadsoftware im Reach-Back-Verfahren identifiziert und von den Bordsystemen entfernt werden. Nach einem Neustart aller Systeme konnte die Einheit ihren Auftrag weiter durchführen.

Szenario Nummer zwei: Nach Erhärtung des Verdachts blieb keine andere Möglichkeit, als die Einheit mit Schlepperhilfe in den Hafen zurück zu bringen. Dort mussten das FüWES, die Fernmeldeeinrichtungen, die gesamte IT sowie die Antriebssteuerung mühsam instandgesetzt werden, die Einheit fiel für Monate aus, und ihren Einsatz musste ein anderes Schiff übernehmen. Bis heute hat man den Schaden noch nicht vollkommen im Griff …

Wir arbeiten an Variante eins! ■

Eike Tammen, Marco Schäfer und Mike Gronert arbeiten in der Abteilung Planung des Marinekommandos.

1 DoS = Angriff auf die Verfügbarkeit oder Erreichbarkeit eines Dienstes, Servers oder eines ganzen Netzwerks

2 Penetration Test = umfassender Sicherheitstest bei Computern und Netzwerken, bei dem mit Methoden in das System eingedrungen wird, die ein Angreifer für einen unautorisierten Zugriff verwenden würde

3 Days without Space = Tage (länger andauernde Übungseinheiten) ohne Netzwerk-/Internetanbindung