Hans-Jörg Kreowski und Aaron Lye

Cyberpeace – für Frieden, Freiheit und eine lebenswerte Welt

Seit der Ausgabe 2+3/2021 ist die Cyberpeace-Rubrik Teil der FIfF-Kommunikation*. Die Rubrik ist gedacht für Ankündigungen, Berichte, kurze Texte und Stellungnahmen rund um das Thema* Cyberpeace – für Frieden, Freiheit und eine lebenswerte Welt*. Aber auch längere Beiträge sind willkommen. Alle Leser:innen sind aufgerufen, die Rubrik für eigene Beiträge zu nutzen. Sie können jederzeit an uns geschickt werden: kreo@fiff.de und lye@fiff.de.*

In der Ausgabe 4/2021 füllte das Thema Künstliche Intelligenz (KI) und Kriegsführung einen ganzen Schwerpunkt. Auf dieser Grundlage fand am 10. März 2022 ein Online-Hearing des Arbeitskreises *Gegen bewaffnete Drohnen* zum Thema *Krieg mit Künstlicher Intelligenz* statt. Siehe dazu folgenden Bericht. Der Schwerpunkt, das Hearing und auch die kontinuierlichen Berichte zu KI zeigen, dass es wichtig bleibt, die militärischen und repressiven Anwendungen der KI aufzuzeigen und dem entgegenzuwirken.

In Ausgabe 1/2022 ist ein Artikel von Aaron Lye zu dem Thema abgedruckt, wie die NATO den Cyberkrieg probt. Der Artikel ist ein Nachdruck, der zuerst erschienen ist bei der *Informationsstelle Militarisierung* (IMI) Ausgabe 1/2022. Er basiert auf einem Vortrag beim IMI-Kongress im November 2021 zum Thema Manöver als Brandbeschleuniger: Kriegsspiele, Manöver und Konfrontation.

Ebenfalls im November 2021 fand zum sechsten Mal die jährliche Sicherheitskonferenz des *Stockholm International Peace Research Institute* (SIPRI) statt. Das Thema der Konferenz war *Schlachtfelder der Zukunft: Trends der Konflikt- und Kriegsführung im 21. Jahrhundert*. Als FIfF-Themen sind insbesondere die Sessions zu Kriegsführung im Cyber- und Weltraum, Kriegsführung mittels KI, Informationskrieg als auch Quantentechnologie zu nennen.

Der Weltraum und der Cyberraum sind zwar getrennte und unterschiedliche Domänen der Kriegsführung mit ihren eigenen (geo-)physikalischen Eigenschaften. Gemein haben sie, dass sie die Grundlage der globalen Kommunikations- und Informationsinfrastruktur sind. Das Funktionieren sowohl der Weltwirtschaft als auch militärischer Kommandostrukturen hängen von ihr ab. Des Weiteren ist die Abhängigkeit vom Funktionieren dieser Infrastruktur dabei stetig gewachsen. Operationen im Weltall wird ein enormes Eskalationspotenzial zugesprochen, denn auf Grund der globalen und strategischen Bedeutung von Weltraum-Ressourcen kann ein regionaler Konflikt durch Weltraum-Operationen schnell zu einem globalen Konflikt anwachsen. Dennoch ist es üblich, dass Staaten (und nicht-staatliche Akteure) Satelliten und ihre Computernetzwerke angreifen (oder dieses üben). Diese Entwicklungen müssen wir als FIfF beobachten. Erfreulich ist, dass die IMI sich mit dem Thema in der Ausgabe 2/2022 beschäftigt.

Im Jahr 2021 wurde auch das Weltraumkommando der Bundeswehr in den Dienst gestellt. Es ging aus dem erst am 21. September 2020 aufgestellten *Air and Space Operations Centre* hervor. Das Kommando soll alle mit dem Weltraum verbundenen Aktivitäten der Bundeswehr bündeln. Im Kommando erfolgt eine enge Zusammenarbeit mit dem Kommando Cyber- und Informationsraum sowie mit dem Deutschen Zentrum für Luft- und Raumfahrt. Offiziell heißt es, sollen künftig Defensivoperationen im All geplant und geführt werden. Vordringliche Aufgabe ist die Überwachung und der Schutz der sieben Satelliten der Bundeswehr zur Kommunikation und Aufklärung (Systeme SATCOMBw bzw. SAR-Lupe; SARah) vor Schäden durch Weltraumschrott und -waffen. Seit einigen Jahren nimmt die Bundeswehr auch am internationalen Weltraum-Manöver *Schrievers Wargame* teil. Aaron Lye hat für die IMI-Ausgabe 2/2022 einen Artikel verfasst, der dort zeitnah erscheint.

Satelliten sind von entscheidender Bedeutung für die militärische Kommunikation, Frühwarnsysteme, Aufklärung und Lagebild sowie globale Positionsbestimmung und Navigation via GPS in Echtzeit. Satelliten, Bodenstationen, Starteinrichtungen etc. sind entsprechend kritische Infrastrukturen, die resilient gegenüber Angriffen gestaltet werden. Ein aktuelles Beispiel ist der informationstechnische Angriff auf den Satellit KA-SAT 9A des amerikanischen Satelliteninternet-Betreibers Viasat am ersten Kriegstag der russischen Invasion in der Ukraine. Ukrainische Behörden bestätigten, dass der Angriff auf den Satelliten zu ernsten Problemen geführt hat.

Sichere Kommunikation ist im Zeitalter von Quantencomputern ein Problem. Quantencomputer nutzen quantenmechanische Eigenschaften und arbeiten deshalb anders als klassische Computer. Dies ist bemerkenswert, da mit diesen Rechnern bestimmte Probleme schneller berechnet werden können. Zu diesen Problemen gehören solche, auf die wir aktuell bei Verschlüsselung vertrauen. Wenn es gelingt, entsprechende Quantencomputer zu bauen, dann sind wesentliche und weltweit täglich viel genutzte Verschlüsselungsverfahren unsicher. Aus diesem Grund wird nach neuen Verschlüsselungsverfahren gesucht, die von Quantencomputern nicht effizient berechnet werden können. Quantenmechanische Eigenschaften ebenfalls für Verschlüsselung zu verwenden, ist eine Idee. Aaron Lye zeigt in seinem Artikel *Quantenschlüsselverteilung: Von Glasfaser zu Satelliten* die Entwicklungen an dieser Technik auf. Der Artikel ist ein Nachdruck eines Artikels, der zuerst in der IMI-Ausgabe 2/2022 zeitnah erscheint.

Auch die 100 Mrd. Euro *Sondervermögen* (Neusprech für Schulden) der Bundeswehr werden uns noch einige Zeit beschäftigen. Obwohl die Details noch nicht klar sind, bedeuten die Investitionen doch eine wesentliche Aufrüstung für Kriege der Zukunft.