Aaron Lye

NATO-Manöver im Cyberraum: Cyber Coalition, Locked Shields und Crossed Swords

Auf dem Warschauer Gipfel im Jahr 2016 hat die NATO den Cyberraum/Cyberspace zum Operationsgebiet erklärt und sich die Verbesserung ihrer operativen Reaktionen und die Entwicklung der Kriegsführung durch Übungen als Ziel gesetzt. Allerdings wurden informationstechnische Angriffe bereits auf dem Gipfel 2006 in Riga als mögliche asymmetrische Bedrohungen genannt und gemeinsame Programme zum Schutz von Informationssystemen als notwendig festgehalten. Seit 2008 trainiert die NATO in gemeinsamen Manövern den Cyberkrieg.

Die eingesetzten Waffen sind Werkzeuge aus dem Bereich der Informatik. Offensive Operationen umfassen Aktionen, die durchgeführt werden, um Daten von IT-Systemen des Ziels oder des Gegners zu exfiltrieren (Spionage), Informationen zu manipulieren, Informationsflüsse zu beeinträchtigen oder Systeme zu zerstören. Umgekehrt gehört zum Cyberkrieg die Bereitstellung und Aufrechterhaltung der eigenen Kommunikations- und Kommandostrukturen sowie die Abwehr gegnerischer Angriffe auf eigene Systeme. Entsprechend umfassen defensive Operationen die Maßnahmen, die ergriffen werden, um unbefugte Aktivitäten in den IT-Systemen und Computernetzwerken (einer Regierung) zu schützen, zu überwachen, zu analysieren, aufzudecken und darauf zu reagieren.

Da sich informationstechnische Angriffe wesentlich von konventionellen unterscheiden, macht das Aufkommen der Cyberkriegsführung es erforderlich, dass Politik, Strategien, Konzepte, Doktrinen, Verfahren sowie Fähigkeiten und Personalstruktur umgestaltet werden. Tätigkeiten, die klassisch Geheim- und Nachrichtendiensten zugeordnet sind, werden jetzt ebenfalls vom Militär praktiziert. Entsprechend sind diese Teile des Militärs oft den Geheim- und Nachrichtendiensten des Landes nahe stehend oder assoziiert. Das United Nations Institute for Disarmament Research hat bereits 2013 fast 100 Staaten identifiziert, welche sich innerhalb des Militärs für informationstechnische Kriegsführung rüsteten.[1]

Im Folgenden sollen die drei wichtigsten bekannten Manöver beleuchtet werden, die regelmäßig und in wechselnder Zusammensetzung von der NATO durchgeführt werden. Bei allen drei sind die Übungsszenarien fiktiv und finden in einer auf Europa basierenden Geografie statt. Des Weiteren handelt es sich um sogenannte *Multi-level Exercises*, bei denen unterschiedliche Schichten trainiert werden: Strategie, operative Ebene, Taktik und technische Ebene. In der Übung *Cyber Coalition* werden v. a. Entscheidungsstrukturen geübt, bei *Locked Shields* hingegen versuchen mehrere Teams Cyberangriffe abzuwehren, wohingegen bei dem Übungszyklus *Crossed Swords* offensive Cyber-Operationen zur Unterstützung von Spezialkräften geübt werden. Darüber/darunter liegende Schichten oder Teile davon werden simuliert.

Bei den technischen Manövern gibt es fünf Teams. Das rote Team greift an. Das blaue Team verteidigt. Darüber hinaus gibt es das weiße Team, welches die Übung leitet und verwaltet, das gelbe Team, welches für die Situationserfassung zuständig ist, und das grüne Team, welches die technische Infrastruktur entwickelt und verwaltet.

Cyber Coalition

Seit 2008 findet jährlich im November das Manöver *Cyber Coalition*[2] statt. Es wird als die wichtigste Cyber-Übung der NATO, als Flaggschiff der kollektiven Cyberverteidigungsübung der NATO und eine der größten Übungen dieser Art weltweit beworben. Das Manöver dauert drei Tage.

Cyber Coalition ist eine kollektive Übung, d. h. die Teilnehmer:innen arbeiten gemeinsam auf ein bestimmtes Ziel hin, um Probleme zu lösen oder bestimmte Aufgaben zu erfüllen, anstatt miteinander zu konkurrieren. Das Manöver soll die Strategieplanung auf operationaler und taktischer Ebene sowie deren Umsetzung durch die NATO und seine Mitglieder trainieren.

Die Übung wird vom Allied Command Transformation[3] unter der Leitung des Militärausschusses – und damit formal auf der höchsten Ebene der militärischen Hierarchie – geplant und durchgeführt.

An der Übung sind zahlreiche NATO-Einrichtungen beteiligt, darunter das NATO Cyberspace Operation Centre und die NATO-Kommunikations- und Informationsagentur (NCIA), welche für die gemeinsame Standardisierung und Beschaffung von IT-Komponenten und -Dienstleistungen zuständig. Eine zentrale Rolle nimmt auch das im estländischen Tallinn ansässige NATO-Exzellenzzentrum für gemeinsame Cyberabwehr (Cooperative Cyber Defence Centre of Excellence, CCDCOE) ein.[4] Unterstützt werden sie von Akteuren aus der Industrie und der Wissenschaft. Sie finden im Cyber Security Exercise and Training Centre CR14 in Tallinn statt. Dieses stellt die Infrastruktur (virtuelle Umgebung), um die (technischen) Szenarien zu erproben. Über virtuelle Netze (VPN) nehmen die Teilnehmer:innen und die örtlichen

Aaron Lye

Aaron Lye hat an der Universität Bremen Informatik studiert und dort auch Ende 2021 seine Promotion abgeschlossen. Er ist seit Jahren beim FIfF aktiv.

Ausbilder:innen aus ihren jeweiligen Staaten und Einrichtungen an der Übung teil, eine kleine Übungssteuerungsgruppe kommt in Estland zusammen, um die Übung durchzuführen.

In den letzten Jahren waren jeweils 700 bis 1.000 Menschen beteiligt. 2021 nahmen rund 1.000 Teilnehmer:innen aus 25 NATO-Mitgliedstaaten, vier Partnerstaaten und der Europäischen Union (EU) teil, darunter insbesondere der EU-Militärstab und das Computer Emergency Response Team für die EU.

Ziel der Übung ist es, neue Taktiken, Techniken und Verfahren zu prüfen. Das bedeutet, erstens die Zusammenarbeit zwischen NATO-Gremien, NATO-Verbündeten und Partnerstaaten als auch Behörden zu verbessern; zweitens die Verbesserung der Fähigkeit des Bündnisses zur Durchführung von sogenannten Cyberspace-Operationen für militärische und zivile Stellen durch die Entwicklung eines Lagebewusstseins, den Austausch von Informationen und die Bewältigung von Angriffen; drittens die Bereitstellung einer Plattform zur Ermittlung von Fähigkeitslücken und Ausbildungsanforderungen sowie zur Validierung von Verfahren der Cyber-Kriegsführung.

Mithilfe von Szenarien und Handlungsabläufen (u. a. Angriffe auf kritische Infrastrukturen, Eindringen in Netzwerke, Spionage, Insider-Bedrohungen, Exfiltration und Datenmanipulation) soll das Manöver die Koordinierung, die Zusammenarbeit und den Informationsaustausch innerhalb der NATO verbessern. Das Manöver umfasst mehrere gleichzeitige Cyberangriffe auf die NATO und NATO-Mitgliedstaaten. Das Übungsszenario konzentriert sich auf eine fiktive Insel – Icebergen genannt – im Nordatlantik und umfasst eine Reihe realistischer Szenarien. Zu den Szenarien 2021 gehörten ein Cyberangriff auf Gasversorgungspipelines, ein Cyberangriff, der die Verlegung von Truppen und die Logistik stört, und ein pandemiebezogener Ransomware-Angriff, bei dem Impfstoffdaten gestohlen und Impfprogramme gefährdet werden.

Das Training von Malware-Analyse, Netzwerk- und Computer-Forensik, also die Analyse der Urheber, Techniken und Taktiken der Angriffe, ist eher nebensächlich und nur ein kleiner Teil des Manövers. Es gibt zwar unterschiedliche Angriffe und Malware, die analysiert und abgewehrt werden sollen, das technische Personal soll aber vor allem Berichte für die operationelle Ebene produzieren.

Locked Shields

Seit 2010 veranstaltet die NATO jährlich im April in Tallinn die Echtzeit-Netzwerkverteidigungsübung *Locked Shields*[5]. Diese Übung dauert zwei Tage.

Während *Cyber Coalition* primär kollaborativ ausgerichtet ist, ist dieses Manöver kompetitiv konzipiert. Nur ein (verteidigendes) blaues Team kann gewinnen. Die Übung ist als Wettbewerbsspiel aufgebaut, bei dem die verteidigenden Teams auf der Grundlage ihrer Leistung bewertet werden. Obwohl die Teams miteinander konkurrieren, ist die Übung so angelegt, dass sie die Teams ermutigt, Informationen auszutauschen und so weit wie möglich zusammenzuarbeiten.

Anfangs war es eine ausschließlich technische Übung. Mittlerweile handelt es sich ebenfalls um ein Multi-Level Exercise, welches ebenfalls die operative Ebene einbezieht (allerdings liegt der Fokus nach wie vor auf der technischen Ebene).

Locked Shields 2021 wurde vom CCDCOE in Zusammenarbeit u. a. mit der NCIA, dem estnischen Verteidigungsministerium, den estnischen Streitkräften, dem NATO-Exzellenzzentrum für Strategische Kommunikation (Strategic Communications Centre of Excellence, STRATCOM COE), der Europäischen Verteidigungsagentur (EDA), dem US Federal Bureau of Investigation (FBI) sowie dem europäischen Kompetenzzentrum für die Bekämpfung hybrider Bedrohungen ausgerichtet. Hinzu kamen zahlreiche Industriepartner (siehe Kasten).

Industriepartner bei *Locked Shields 2021*:

Arctic Security, Atech, Avibras, BHC Laboratory, Bittium, Bolt, Bytelife, Cisco, Clarified Security, Cyber Test Systems, Cybernetica, Elisa, Ericsson, Foundation CR14, GuardTime, Iptron, Microsoft, openvpn, PaloAlto networks, Sentinel, Siemens, SpaceIT, STM, Stamus Networks, Synopsys, SUTD iTrust Singapore, TalTech, Threod Systems, VTT Technical Research Centre of Finland

Die Übung findet im Hilton-Hotel in Tallinn statt. Des Weiteren werden die zu verteidigenden Systeme visuell oder modellhaft aufbereitet. Beides dient dazu, die Übung für Politiker:innen, Entscheider:innen und Sponsoren ansprechend zu machen.

Das CCDCOE stellt Personal für das weiße, gelbe, grüne sowie das offensive rote Team. NATO-Staaten, Partner, aber auch das NATO Computer Incident Response Capability stellen die blauen Teams. Zu den Teilnehmer:innen gehören Sicherheitsexpert:innen, die nationale IT-Systeme schützen, sowie politische Beamte und Rechtsberater:innen von NATO-Verbündeten und Partnern. Während sich die Organisatoren der Übung vor Ort treffen, haben die teilnehmenden blauen Teams via VPN Zugang zu den Übungsnetzen.

Die Teilnehmer:innenzahl erhöhte sich alle zwei bis drei Jahre signifikant (2012: 200, 2015: 400, 2018: 1000, 2021: 2000). Die Anzahl der teilnehmenden Staaten belief sich bis 2015 auf ca. 17, die zusammen mit 12 blauen Teams antraten. 2016 waren es schon 26 Staaten und 20 blaue Teams und ab 2018 fast 30 Staaten mit 22 blauen Teams.

Die blauen Teams haben die Aufgabe, die Netze und Dienste eines fiktiven Landes – Berylia – unter großem Druck aufrechtzuerhalten. Dazu gehören die Bewältigung und Meldung unterschiedlicher Angriffe auf eine Vielzahl von Systemen, die Lösung forensischer Herausforderungen sowie die Reaktion auf rechtliche, mediale und szenarienbedingte Einwirkungen. Umgesetzt wird das anhand von einem großen virtualisierten Netzwerk und einem fiktiven Szenario inkl. der simulierten Infrastruktur des fiktiven Inselstaats Berylia im Nordatlantik. Das Fachpersonal der Verteidiger wird mit einer Vielzahl von Angriffen herausgefordert und an Grenzen bzw. zum Scheitern gebracht, damit diese aus Fehlern lernen und extreme Situationen und damit auch übliche Angriffe abwehren können. 2500 Cyberangriffe pro Team werden simuliert. Die Anzahl der zu schützenden virtuellen Sys-

teme wurde entsprechend der Teilnehmer:innenzahl angepasst: 2017 waren es noch 3000 Systeme, 2018 schon 4000 und 2021 5000. Die Übung bezieht reguläre Unternehmens-IT, kritische Infrastruktur und militärische Systeme mit ein. Realistische Netzwerke, Systeme und Angriffsmethoden bildeten die technische Umgebung.

Um in *Locked Shields* erfolgreich zu sein, müssen die konkurrierenden Teams sowohl technische als auch soziale Fähigkeiten beherrschen, d. h. sie müssen in der Lage sein, mit Medien- und Rechtsanfragen umzugehen und gleichzeitig Angriffe abzuwehren.

Die Systeme und Aufgaben haben sich über die Jahre gewandelt und an Komplexität gewonnen. Bis 2014 bestand die Übung aus klassischen Client-seitigen Angriffen und aus Angriffen auf die Server via Exploits.

Neue Elemente im Jahr 2015 waren industrielle Steuerungssysteme (ICS/SCADA Systeme) und Windows 8 und 10 Betriebssysteme sowie ein Element von „aktiver Verteidigung". Des Weiteren war eine Aufgabe, die Kontrolle über ein von Feinden übernommenes unbemanntes Luftfahrzeug (Unmanned Aerial Vehicle, UAV) zurückzuerlangen. Dabei standen die Teams unter Zeitdruck, da das bespielte Szenario lautete, dass die Drohne über einer Stadt kreise und nach drei Stunden aufgrund von Treibstoffmangel abstürzen werde. Zusätzlich zu technischen und forensischen Herausforderungen wurden Medien und rechtliche Fragestellungen erstmals Bestandteil der Übung.

Im Jahr 2017 hatten die blauen Teams die Aufgabe, die Dienste und Netze eines Luftwaffenstützpunkts des fiktiven Landes aufrechtzuerhalten, der dem Übungsszenario zufolge schweren Angriffen ausgesetzt war. Neben den Angriffen auf militärische Kommando- und Kontrollsysteme und andere operative Infrastrukturen waren Angriffe auf die Kontrollsysteme für ein von Siemens simuliertes Stromnetz sowie simulierte UAVs Teil der Übung. Die Übung ermöglichte den Umgang mit der simulierten Situation, in der ein unbekanntes Flugzeug über das Land fliegt. Die Flugdaten waren gefälscht bzw. simuliert und wurden vom roten Team in das System eingespeist.

Des Weiteren war die Übung in dem Jahr zum ersten Mal eine Multi-Layer Exercise. Während IT-Expert:innen die Verteidigung von Computernetzwerken und die Bewältigung rechtlicher und forensischer Herausforderungen trainierten, übten politische Entscheidungsträger ihre Entscheidungsverfahren. Insbesondere ging es darum, wie ein einzelner Staat auf einen Cyberangriff reagieren sollte und wie man Entscheidungen aus rechtlicher und diplomatischer Sicht treffen kann.

2018 wurde die Situation um die Verteidigung eines 4G-Mobilfunknetzes für die öffentliche Sicherheit sowie einer SPS-gesteuerten Wasseraufbereitungsanlage erweitert. 2019 waren neben diesen beiden auch maritime Überwachungssensoren Teil der Übung.

2021 enthielt die Übung neben neuen Systemen (Stromnetze, Satellitensteuerung, Luftverteidigung, Wasseraufbereitung, mobile und militärische Kommunikationsnetzwerke) auch mehrere neue Herausforderungen für den Bereich der strategischen Entscheidungsfindung. Auch der Finanzdienstleistungssektor wurde als Angriffsfläche für feindliche Angriffe hervorgehoben. Die Übung untersuchte, wie neu entstehende Technologien, wie z. B. Deepfakes, zukünftige Konflikte beeinflussen werden.

Crossed Swords

Seit 2014 findet jährlich in Riga die Übung *Crossed Swords*[6] statt. Diese technische und praxisnahe Übung dauert drei Tage und legt den Fokus auf das Training von Penetrations-Tester:innen und Expert:innen für digitale Forensik. Diese sollen lernen, besser mit verschiedenen Angriffsvektoren umzugehen, und offensive Fähigkeiten trainieren. Seit 2017 richtet sich das Training ebenfalls an Spezialkräfte und es wurden kinetische Elemente eingebettet. Nach und nach hat sich *Crossed Swords* von einem rein technischen Red-Teaming-Workshop zu einem Manöver entwickelt, bei dem verschiedene technische Fähigkeiten mit kinetischer Gewalt kombiniert werden. 2018 wurde die Übung in Umfang und Komplexität erheblich ausgeweitet und erstreckte sich über mehrere geografische Gebiete, wobei Anbieter kritischer Informationsinfrastrukturen einbezogen wurden.

Das Manöver wird seit 2016 ebenfalls vom CCDCOE organisiert. Im Gegensatz zu den anderen zwei Übungen findet *Crossed Swords* in Präsenz statt und ist wesentlich kleiner als die beiden anderen Manöver. Allerdings ist auch dieses über die Jahre gewachsen, und immer mehr NATO-Staaten nahmen daran teil: 2018 waren es ca. 80 Partizipierende aus 15, 2019 ca. 100 Partizipierende aus 21 und 2020 ca. 120 Partizipierende aus 26 Staaten.

Ziel der Übung ist das Erlernen von Fähigkeiten, IT-Systeme zu infiltrieren (client side targeting, web based attacks, malware and system exploitation, network and service based attacks). Neben klassischen Computer-Netzwerk-Operationen behandeln die Übungen auch Untersuchung und Angriffe auf Systeme, die oft für Automatisierung und industrielle Steuerung genutzt werden.

Zu den Übungszielen gehört aber auch die erfolgreiche Durchführung von verdeckten Angriffen und Ablenkung (deceptions) sowie die Zusammenarbeit, die es den Teilnehmer:innen ermöglicht, bereichsübergreifende Synergien zu nutzen und informationstechnische Angriffe in militärische Taktiken zu integrieren, um informationstechnische mit kinetischen Angriffen zu kombinieren. Dabei liegt der Fokus allerdings nach wie vor auf der technischen Ebene. Seit 2020 beinhaltet die Übung auch ein Führungsmodul.

Des Weiteren trainiert *Crossed Swords* die digitale Forensik (die Sammlung und Auswertung von Informationen). Die Analyse von Informationen dient auch der technischen Zuordnung (Attribution) sowie der Identifizierung bösartiger Aktivitäten. Auch was gemeinhin als *Hack-back* bekannt ist, also das Aufspüren und Infiltrieren von Systemen, von denen ein Angriff ausgeht, wird ebenfalls geübt (responsive cyber defense and adversarial information system infiltration).

Zur Verfügung stehen 200 virtuelle und physikalische IT-Systeme. Anzugreifende Ziele (siehe Kasten, siehe Blumbergs-Ottis-Vaarandi (2019), Fn 6) waren das Steuerungssystem einer

Bunkertür, ein Alarmsystem, IP-Kameras, Steuerungssysteme eines Stromnetzes, unbemannte Luft-, Wasser- und Bodenfahrzeuge, eine Eisenbahnkontrollstation, das Steuerungs- und Verfolgungssystem eines Schiffes sowie ein militärisches Funkkommunikationsnetz und die Basisstationen eines zivilen Mobilfunknetzes.

2018 wurden beispielsweise Mobilfunktechnologien zur Identifizierung einer Zielperson, Drohnenüberwachung und 5G-Sensoren zur Erfassung seines Standorts und zum Sammeln weiterer Informationen eingesetzt. 2019 wurden mehrere kinetische und Cyber-Operationen gleichzeitig durchgeführt, darunter Angriffe auf industrielle Kontrollsysteme, physische Sicherheitssysteme, UAVs und maritime Überwachungssysteme. Ein neues Element waren die unbemannten Bodenfahrzeuge (UGV), die informationstechnisch angegriffen werden sollten.

Anzugreifende Ziele bei Crossed Swords bis 2019:

Bunkertür: Steuersystem, das eine Reihe von miteinander verbundenen, von Siemens entwickelten S7-1200 basierten PROFINET IO-Geräten verwendet. Das rote Team muss das Kommunikationsprotokoll rekonstruieren, um die Befehle zur Steuerung der Bunkertür über das Netzwerk einzugeben.

Alarmsystem: Geschützte Räumlichkeiten durch das Paradox-Alarmsystem, das durch Analyse des verwendeten Busprotokolls und Erfassung und Dekodierung des PIN-Codes über das Netzwerk angesprochen werden muss.

CCTV-IP-Kamera: Das rote Team muss die Schwachstellen in der Webschnittstelle der IP-basierten Überwachungskamera finden und ausnutzen, um die vollständige Kontrolle über das Netzwerk zu erlangen.

Verteiltes Stromnetz: Die industrielle Ethernet-Protokollserie IEC-60870-5-104 und eine von Martem hergestellten Remote-Terminal-Unit wird zur Verwaltung und Überwachung des Stromnetzes verwendet. Das rote Team muss das Protokoll rekonstruieren und Befehle über das Netzwerk injizieren, um die Energieversorgung zu steuern.

Unbemanntes Luftfahrzeug (UAV): Die von Threod hergestellten UAVs, die das geschützte Gebiet überfliegen, müssen ins Visier genommen werden, um die Kontrolle über sie zu erlangen.

Unbemanntes Bodenfahrzeug (UGV): Die von Milrem entwickelten UGVs dienen als vom Gegner kontrollierte Panzertruppe und das rote Team hat die Aufgabe, die vollständige Kontrolle über sie zu übernehmen, indem entweder die verwendeten Netzwerkprotokolle oder die steuernde Workstation angegriffen werden.

Maritime Navigation: Das Steuerungs- und Verfolgungssystem eines Schiffes, das auf dem maritimen AIS-Protokoll (Automatic Identification System) basiert, wird vom roten Team angriffen, um die Kontrolle über das Schiff zu erlangen und gefälschte Marine-Tracks zu injizieren.

Funkkommunikationsnetz: Das Harris-basierte militärische Datennetz muss vom roten Team durch Extraktion der Verschlüsselungsschlüssel infiltriert werden.

Basisstationen des Mobilfunknetzes: Das rote Team muss die vom Betreiber LMT (Latvian Mobile Telephone) bereitgestellten Basisstationen, die mit dem tatsächlichen Mobilfunknetz verbunden sind, infiltrieren und die abgefangene Kommunikation analysieren, um den Nachrichtenaustausch (SMS) eines gegnerischen Agenten zu entschlüsseln und seinen physischen Standort zu bestimmen, damit Spezialkräfte zugreifen können.

Eisenbahnkontrollstation: Ein System, das auf einer von Siemens entwickelten S7-1200 SPS mit s7comm+ Protokoll basiert, steuert das simulierte Eisenbahnnetz. Das rote Team hat die Aufgabe, die Kontrolle über die Eisenbahnkontrollstationen zu erlangen, um den Zug zu stoppen oder entgleisen zu lassen.

Fazit

Das Ausspähen und Nutzen von Sicherheitslücken im Vorfeld und bei geheimdienstlichen Operationen und militärischen Auseinandersetzungen ist längst Alltag. Durch das Bekanntwerden der Operation Olympic Games (gemeinhin als Stuxnet bekannt) ist auch seit 2010 eine neue Qualität von geheimdienstlich-militärischen Cyberangriffen bekannt. In diversen Manövern trainieren Armeen (und Geheimdienste) den Cyberkrieg. Insgesamt wird deutlich, dass Cyber-Operationen in großem Maßstab vorbereitet und seit 2008 systematisch im Manöver geübt werden. Da informationstechnische Angriffe in der Regel wesentlich kostengünstiger sind als konventionelle Angriffe und ihre Attribution äußerst schwierig ist, ist die Schwelle niedrig, diese Angriffe durchzuführen. Entsprechend sind diese Manöver Brandbeschleuniger für aktuelle und bevorstehende Konflikte. Eine internationale Ächtung dieser Angriffe ist dringend notwendig, erscheint aber aktuell unwahrscheinlich.

Anmerkungen

1 *United Nations Institute for Disarmament Research (UNIDIR) (2013): The Cyber Index – International Security Trends and Realities. Genf.*

2 *Selbstdarstellung des Manövers Cyber Coalition siehe https://www.act.nato.int/cyber-coalition*

3 *Das Allied Command Transformation (ACT) ist neben dem Allied Command Operations eines der beiden strategischen Hauptquartiere der NATO. Es ist zuständig für die Analyse von Herausforderungen und Chancen, die sich aus der Innovation und der Aufrechterhaltung eines technologischen Vorsprungs im Kampf ergeben, sowie die Entwicklung von Verfahren und Technologien, welche der NATO-Kriegsführung nutzen, durch ein großes Netz aus Industrie, Hochschulen, militärischen und zivilen Stellen in den NATO-Staaten, in NATO-Agenturen und NATO-Exzellenzzentren.*

4 *Das NATO Cooperative Cyber Defence Centre of Excellence (CCD-COE) ist eines von 21 akkreditierten Centre of Excellence der NATO mit Sitz in Tallinn in Estland. Das Zentrum wurde 2008 gegründet und als internationale militärische Organisation akkreditiert. Es ist eine Wissensdrehscheibe, Denkfabrik und Ausbildungseinrichtung. Kernaufgaben sind interdisziplinäre angewandte Forschung und Entwicklung*

sowie Beratungen, Schulungen und Übungen im Bereich der Cybersicherheit. Zur Rolle der NATO-Exzellenzzentren siehe u. a.: Christopher Schwitanski: Nato-Exzellenzzentren – Planen für den nächsten Krieg, IMI-Studie 2016/06.

5 *Selbstdarstellung des Manövers Locked Shields siehe https://ccdcoe.org/exercises/locked-shields/. Weitere Informationen sind den jährlichen Stellungnahmen des CCDCOE sowie den After Action Reports (https://ccdcoe.org/library/publications) zu finden.*

6 *Selbstdarstellung des Manövers Crossed Swords siehe https://ccdcoe.org/exercises/crossed-swords/. Details siehe Blumbergs-Ottis-Vaarandi (2019): Crossed Swords: A Cyber Team Red Oriented Technical Exercise. Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019: University of Coimbra, Portugal, 4-5 July 2019.*

CC BY

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in Fairer Honig

Beginnen wir am besten mit dem Koalitionsvertrag der Bundesampel. Bezüglich der sozial-ökologischen Transformation ist auffallend die EU im Blick: EU-Handelsabkommen sollen verbindliche Klauseln enthalten, die Menschenrechte, soziale und ökologische Standards schützen. Ein *effektives* Lieferkettengesetz soll auf EU-Ebene vorangetrieben werden, bei unveränderter Umsetzung und ggf. Verbesserung der deutschen Variante. EU-Vorschläge zum Importverbot von Produkten aus Zwangsarbeit sollen unterstützt werden.

Und mindestens beim letzten Punkt sind wir auch bei der Elektronik angekommen. China ist in den Medien, im Jahr des Tigers, mit Olympia, Schulterschluss mit Putin und eben der Zwangsarbeit der muslimischen Uiguren [illegible] Intel hatte seine Zulieferer Anfan[illegible] sich aus der Provinz zurückzuzieh[illegible] gesetz sieht für Unternehmen ein[illegible] nicht nur sowieso bei direkten Auftragnehmern, sondern auch tiefer in der Lieferkette, wenn es *substanzielle* Hinweise auf Menschenrechtsverletzungen gibt. Die liegen hier offensichtlich vor. Und China ist in Sachen IT und Elektronik überall in der Lieferkette, vom Zusammenschrauben bis zu den Rohstoffen. Etwas dumm für das zentrale Anliegen der Energiewende vielleicht, dass ausgerechnet für Solarzellen nun konkrete Nachweise von Zwangsarbeit im Westen Chinas vorliegen.

Diese werden aus Quarzsand gefertigt, bislang nicht gerade als einer jener Transitionsrohstoffe im Gespräch. Es gibt ihn sprichwörtlich wie Sand am Meer, ganz anders als beim Lithium in den Akkus der vielen noch kommenden E-Autos und sowieso auch unserer mobilen IT: Das baut man zum einen oft im Meer ab, es kommt in Salzseen angereichert vor. Zum anderen ist es knapp und wird immer teurer. Bolivien versucht seit Jahren daraus Gewinn zu schlagen, wird aber nicht produktionsreif, wie jüngst resümiert wurde. Sie wollen es bis zur Batterie alleine hinbekommen, also ohne Ausbeutung durch etablierte Rohstoffindustrie, was eine wichtige Voraussetzung für die nationale Entwicklung ist. Die Multis orientieren sich daher lieber gen Argentinien. Die Regierung ist da offener für fremdes Know-how, Kapital und Knebelverträge, ja, wenn nicht die indigene Bevölkerung sich dem entgegenstellen würde, um ihre Wasserversorgung zu retten. In Serbien jedenfalls hat Rio Tinto im Januar aufgrund lokaler Proteste aufgegeben, Lithium zu fördern. Ein anderer Transitionsrohstoff, ebenfalls für die Batterien, ist Kobalt aus dem Kongo mittels Kinderarbeit, ein lange bekannter Zusammenhang, was die IT-Hersteller nur zögerlich akzeptierten. Eine Klage indes gegen u. a. Apple und Microsoft in dieser Sache ist im November abgewiesen worden: Man könne ob der Komplexität der Handelsbeziehungen keinen einzelnen [illegible]nnen.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

[illegible]jekte? Fairphone hatte im Herbst [illegible]4 ihres Smartphones veröffentlicht, das im Dezember nun die TCO-Zertifizierung erhalten hat und im Januar die vom Blauen Engel. Enttäuschend ist vielleicht, dass sie sich aus optischen Gründen gegen Recycling-Alu im Gehäuse entschieden haben, immerhin nun aber auf der Suche nach fairem Aluminium sind. Neu aus Fairnesssicht ist der Ausbau des Unterstützungsprogramms in Ruanda für den Abbau von Wolfram für den Vibrationsalarm, und das Fairtrade-Gold, das schon die Leiterplatten enthalten, ist nun auch in den Bauteilen des Herstellers Hirose, wie im Dezember verraten wurde. Vermutlich in Steckkontakten, leider wird das nicht verraten. Das Tragische an der vorbildlichen Modularität des Fairphones ist, dass sie mehr Steckkontakte benötigt, in denen typischerweise Gold ist, was sich negativ auf die Sozial- und Ökobilanz auswirkt. Nun ist es immerhin fair. Fairer jedenfalls als das immerhin konfliktfreie Zinn, über das eine sehr lesenswerte Artikelserie beim Onlinemagazin *Das Lamm* erschien, mit deutlich geäußerten Zweifeln an der sozialen Wirksamkeit dieser Maßnahme. Auch sonst wird dort nicht an Zweifeln gespart: Viele Angestellte seien enttäuscht gegangen, weil der neue Geldgeber nur auf die Zahlen schaue.

Sebastian Jekutsch

Sebastian Jekutsch ist Sprecher der AG Faire Computer des FIfF. Wer sich für die Quellen oder das Thema überhaupt interessiert, kann gerne Kontakt aufnehmen per *sebastian.jekutsch@fiff.de*.