Funkkolleg 2016/2017

Sicherheit

Zusatzmaterial zur Sendung 20: **Cyber-War – neue Herausforderungen für die Bundeswehr**

vhs Die Volkshochschulen in Hessen

TECHNISCHE UNIVERSITÄT DARMSTADT

HESSEN Hessisches Kultusministerium

hr iNFO

Zusatzmaterial zur Folge 20
Cyber-War – neue Herausforderungen für die Bundeswehr

Livestream und Podcast: www.hr-inforadio.de

Interessierte Hörerinnen und Hörer finden auf dieser Seite weiterführende Informationen zu den einzelnen Sendungsthemen als Zusatzmaterial. Die Materialien wurden zum Zugriffszeitpunkt 18.04.2017 erstellt von:
Markus Stegeman, Fachgebiet Wirtschaftsinformatik | Software Business & Information Management, Technische Universität Darmstadt

Inhalt

1. Forschungsstudien

„Der Cyberkrieg ist längst hier“

Im Interview mit dem „Zukunftsinstitut“ spricht die renommierte Cyberwar-Expertin Dr. Myriam Dunn Cavelty über echte und fiktive Cyberkriege, die Rolle des Militärs und die Zukunft von Sicherheit. Sie ist stellvertretende Leiterin für Forschung und Lehre am Center for Security Studies der ETH Zürich. Sie publiziert regelmäßig in internationalen Fachzeitschriften und ist Autorin und Herausgeberin mehrerer Bücher zu Themen rund um Sicherheit im Informationszeitalter.

Neben wichtigen Erkenntnissen ihrer Forschungsarbeit ist auch ihre persönliche Einschätzung zu bestimmten Aspekten von Cyberwar Teil des Interviews. So stellt sie beispielsweise klar, dass ernstzunehmende Fachexperten eine kriegerische Auseinandersetzung, die ausschließlich im virtuellen Raum stattfindet und schwerwiegende Konsequenzen für die Bevölkerung nach sich ziehen würde, heutzutage für höchst unwahrscheinlich halten.

Quelle: Dunn Cavelty, Myriam; Papasabbas, Lena: “Der Cyberkrieg ist längst hier”, Cyber (In)Security, November 2015

Link: https://www.zukunftsinstitut.de/artikel/05-cyber-insecurity/05-experts-insights/der-cyberkrieg-ist-laengst-hier/

2. Industrienahe Studien

Die digitale Gewalt im Internet ist längst ein Weltkrieg

Der ehemalige US-Präsident Barack Obama kündigte Ende 2016 Vergeltung für russische Hackerangriffe im amerikanischen Wahlkampf an. Seit 2010 haben die USA eine eigenständige Kommandoebene für die elektronische Kriegsführung, das USCYBERCOM. Dessen Aufgabe: die überlebenswichtige Infrastruktur der USA vor digitalen Attacken zu schützen, selbst Angriffswaffen und -strategien zu entwickeln und insgesamt die militärisch-technologische Überlegenheit der Amerikaner in diesem Bereich zu sichern.

Was die Cyberkrieger genau können, ist geheim. Denn anders als militärische Hardware, die auf Truppenparaden gezeigt wird, haben Cyberwaffen oft ein Verfallsdatum. Wenn sie einmal eingesetzt wurden, sind sie weitgehend entwertet, weil die andere Seite dann weiß, wie sie sich gegen Ausforschung oder Sabotage schützen kann.

Im Internet kämpft längst jeder gegen jeden. Dieser Artikel liefert eine Übersicht der mächtigsten Akteure und Strategien.

Quelle: Böhmer, Daniel-Dylan; Erling, Johnny; Mühlmann, Sophie; Wergin, Clemens; Yaron, Gil; Yücel, Deniz: Die digitale Gewalt im Internet ist längst ein Weltkrieg, WELT Online, 17.12.2016

Link: https://www.welt.de/politik/ausland/article160381327/Die-digitale-Gewalt-im-Internet-ist-laengst-ein-Weltkrieg.html

3. Sonstiges

3.1. Literatur

Cyberwar – Grundlagen, Methoden, Beispiele

Die Diskussionen um die Computer- und Internetsicherheit haben in den letzten Monaten an Intensität zugenommen und der Cyberspace wird wegen der zunehmenden Bedeutung des Internets und der Informationstechnologie inzwischen als fünfte militärische Dimension neben Boden, See, Luftraum und Weltall betrachtet.

Die folgende Arbeit unternimmt eine aktuelle Bestandsaufnahme und geht auf die theoretischen und praktischen Probleme des Cyberwars ein. Es wird zudem ein aktueller Überblick über Cyberwar-Aktivitäten seit 1998 gegeben und die Sicherheitsarchitektur im Cyberspace vorgestellt. Abschließend werden exemplarisch die Cyberwar-Strategien der USA, Chinas, Russlands und auch die Cyberpolitik der Europäischen und Afrikanischen Union besprochen.

Quelle: Saalbach, Klaus-Peter: Cyberwar. Grundagen-Methoden-Beispiele. Universität Osnabrück, 07.09.2016

Link: http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-grundlagen-geschichte-methoden.pdf

Als weiterführende Literatur empfehlen wir:

- Ammann, Thomas; Aust, Stefan: Digitale Diktatur. Totalüberwachung, Datenmissbrauch, Cyberkrieg. Ullstein Verlag, Berlin, 2016

3.2. Video/Audio

Cyberwar – 7 Dinge, die Sie wissen sollten

Computer steuern unser Leben. Sie vermitteln Telefongespräche und zahlen uns Geld am Automaten aus. Sie steuern Atomkraftwerke und Kläranlagen. Unsere digitalisierte Gesellschaft birgt damit Risiken: Stromausfälle oder sich selbst zerstörende Industrieanlagen sind so gefährlich wie ein bewaffneter Konflikt.

In dieser Ausgabe der Sendung „Quarks & Co“ des WDR werden die wichtigsten Aspekte von Cyberwar erklärt und zusammengefasst.

Link: http://www1.wdr.de/mediathek/video/sendungen/quarks-und-co/video-cyberwar---dinge-die-sie-wissen-sollten--100.html

Cyberwar – das digitale Schlachtfeld

Wirtschafts- und Bankenspionage, Manipulationen von militärischen und staatlichen Kommunikationsmedien, Fremdsteuerungen oder gar Zerstörungen von Computersystemen - Gert Scobel diskutiert in seiner Sendung (3sat) mit Sandro Gaycken, Robin Geiß und Felix Lindner über bekannt gewordene Cyberattacken und militärische Transformationen der neuen Kriegsführung.

Link: https://www.zdf.de/wissen/scobel/cyberwar-das-digitale-schlachtfeld-104.html

3.3. Zeitschriften

Pentagon sucht nach Superwaffe für den Cyberwar

Die Superwaffe für den brachialen Cyberwar ist seit langem bekannt. Und sie hängt direkt mit der Erfindung des Computers und der Entwicklung der Atombombe zusammen, denn die ultimative Bedrohung einer hochgradig vernetzten Gesellschaft mit allen ihren elektrischen Geräten ist die Explosion einer Atombombe hoch in der Luft.

Die Strahlung einer solchen EMP-Bombe würde Menschen und Leben nicht schädigen, aber einen massiven und plötzlichen hochfrequenten, elektromagnetischen Impuls ausstrahlen, der in weitem Umkreis alles lahmlegt, was am Stromnetz hängt, also einen Großteil der Infrastruktur und der Geräte, die für eine moderne Gesellschaft unerlässlich sind, Smart Cities und Smart Homes, alle Fahrzeuge sowieso, wären insbesondere davon betroffen.

Quelle: Rötzer, Florian: Pentagon sucht nach Superwaffe für den Cyberwar, HEISE Online 25.02.2017

Link: https://www.heise.de/tp/features/Pentagon-sucht-nach-Superwaffe-fuer-den-Cyberwar-3629536.html

Flugzeug-Absturz oder Atomunfall für Hacker technisch kein Problem mehr

Sowohl Russland als auch China bedrohen den Vorsprung des Westens im Bereich innovativer Militärtechnik. Die ist umso bedrohlicher, wenn man die möglichen Folgen von Cyber-Angriffen betrachtet. Ein Flugzeug abstürzen zu lassen oder ein Atomkraftwerk zu sabotieren sei für Hacker kein Problem mehr, warnt ein Experte.

Quelle: Lüdeke, Ulf: China und Russland auf dem Vormarsch. Cyberwar-Experte: Flugzeug-Absturz oder Atomunfall für Hacker technisch kein Problem mehr, FOCUS Online, 11.02.2016

Link: http://www.focus.de/politik/china-und-russland-auf-dem-vormarsch-cyberwar-experte-flugzeug-absturz-oder-atomunfall-fuer-hacker-technisch-kein-problem-mehr_id_5277973.html

4.500 Hackerangriffe pro Tag auf die Bundeswehr

Die Bundeswehr muss nach Angaben von Verteidigungsministerin Ursula von der Leyen jeden Tag 4.500 Hackerangriffe abwehren. "Viele dieser Angriffe sind automatisiert. Da versucht ein Computernetzwerk automatisch durch unsere Firewalls zu gelangen", sagte die CDU-Politikerin der Welt am Sonntag. Gefährlicher seien aber "die maßgeschneiderten Angriffe, sogenannte APTs – Advanced Persistent Threats". Hinter einigen dieser komplexen und fortwährenden Attacken vermuten die deutschen Geheimdienste staatliche Akteure.

Präventivschläge gegen die Angreifer schloss von der Leyen aus. "Da ist die Gesetzeslage eindeutig", sagte sie. Darüber hinaus sei der Angreifer schwierig auszumachen.

Quelle: ZEIT Online: 4.500 Hackerangriffe pro Tag auf die Bundeswehr, 17.04.2017

Link: http://www.zeit.de/politik/deutschland/2017-04/ursula-von-der-leyen-bundeswehr-cyberangriffe-abwehr

4. Personen

Urusla von der Leyen (CDU) war von 2005 bis 2009 Familienministerin, von 2009 bis 2013 Arbeitsministerin und ist seit Dezember 2013 Bundesverteidigungsministerin. Um einer der Großaufgaben der Landesverteidigung – Das Internet und die Digitalisierung des gesamten Lebens – gerecht zu werden, hat sie im vergangenen Jahr den Aufbau einer Cyberarmee angeordnet.

„Wir wollen uns beim Thema Cyber besser aufstellen“, sagte Leyen. Konkret heißt das: In den nächsten fünf Jahren soll neben Heer, Marine, Luftwaffe, Streitkräftebasis und Sanität eine neue Abteilung „Cyber- und Informationsraum“ entstehen – mit 13.500 Soldaten und Zivilisten, die aus bestehenden Einheiten zusammengeführt werden, mit Abteilungsleiter und eigenem Inspekteur als „Cyberkommandeur“. Fehlt nur noch die eigene Uniform – aber die soll es nicht geben.

Quelle: Birnbaum, Robert: Bundeswehr rüstet auf für den Cyber-Krieg, Der Tagesspiegel, 26.04.2016

Link: http://www.tagesspiegel.de/politik/ursula-von-der-leyen-bundeswehr-ruestet-auf-fuer-den-cyber-krieg/13505394.html