Ein Projekt von

PH Wien BMBF

ORF 1 RADIO ÖSTERREICH 1

Cyberwar

Das Internet als Kampfgebiet

Ö1 Radiokolleg / Teil 1 - 4
Gestaltung: Mariann Unterluggauer
Sendedatum: 8.-11. September 2014
Länge: je ca. 13 min

Inhaltsübersicht

Teil 1: Was ist ein Cyberwar?

Begriff Cyber-Krieg, Cyber-War | Definition von Krieg: zwei Armeen kämpfen | Carl Philipp Gottlieb von Clausewitz | Stefan Schumacher, Magdeburger Institut für Friedensforschung | erkennbarer Feind ist abhanden gekommen | Sir Michael Howard, Militärstratege | Notstand | Martin Libicki, Rand Corporation | Veröffentlichung der Pentagon-Papiere, Ende des Vietnamkriegs | Edward Snowden, NSA | Krieg in Computernetzwerken | Attribution: Tatsachenzuschreibung | Wer hat den Angriff ausgeführt? | Indizienbeweis | Ziel: Informationen, Spionage | 2007: Israelische Hacker im Radarsystem der syrischen Luftabwehr | 2010: Stuxnet, Steuerung iranischer Zentrifugen | 2012: Hack in staatlicher saudischer Ölfirma | 6 Monate später: Cyberangriff von Nordkorea auf Computer in Südkorea | Falschspiel, schwer feststellbarer Angreifer | Schwieriges Ende eines Cyberkriegs | Matthias Kettemann, Goethe Universität Frankfurt | „Konflikt“ statt „Krieg“ | Genfer Konvention | Völkerrechtlich kann es einen Cyberwar nicht geben | Space War, Satelliten | Notstand im Internet? | Cyberwar kann zu einem gewaltsam geführten Krieg werden.

Teil 2: Cybercrime oder Cyberwar?

Verunsicherung | Thomas Rid, King‘s College in London | Kriminalität ist meist unpolitisch, ein Krieg politisch | Identität verschleiert, zur Schau gestellt | Spionage, Sabotage, umstürzlerische Tätigkeiten – Propaganda | Slim Amamou, tunesischer Aktivist | kontrolliere die Geschichte, die Ressourcen | Untergrabung der Autorität | Krim | Auswirkungen von Propaganda | Software-Roboter, die E-Mails verschicken | Aufmerksamkeit ist eine Ressource | Zeit gewinnen | Minister liest die Zeitung | soziales Netzwerkmodell zur Durchführung von Propaganda | vage Aussagen | Passwörter werden nicht über Telefon abgefragt | Regierungen selbst können Schadsoftware verfassen: „BKA Trojaner“ | Ransomware | Alexander Seger, Europarat | Wie müssen Gesetzte beschaffen sein? | Reinhard Posch, Chief Cyber Security Officer | Aufbringen der Schadsoftware über das Netz in Deutschland erlaubt, in Österreich nicht | Eindeutigkeit des Ziels nicht gegeben | Budapester Konvention 2001 | „Cybercrime Convention Committee” des Europarats | Vertragsparteien gewinnen | USA dabei | Russland und China nicht | Regeln verbannt „schlechtes Verhalten“, Kriminalisierung von Cyberkriminalität | es gibt noch keine Normen | „Datenverkehr der kurzen Wege“ | Geldüberweisungen | Wegzoll

Teil 3: Macht der Daten – Grundrechte oder Strafverfolgung

Vorratsdatenspeicher | David Irvine, australischer Inlandsgeheimdienst | 2014, Luxemburg | Grundrechte zum Schutz personenbezogener Daten | verhältnismäßig, notwendig | Christoph, Forschungsinstitut „Zentrum für digitale Menschenrechte" | Beschwerde gegen die Vorratsdatenspeicherung beim Europäischen Gerichtshof | Grundsatz der Verhältnismäßigkeit | Wirksamkeit | Alexander Seger, Europarat | Convention on Cybercrime 2001, 42 Staaten ratifizierten | Dokumentation von Verletzungen | Problem ist schwierig geworden | Attacken gegen Computer | Beweise | Recht auf freie Meinungsäußerung, Recht auf Privatheit | Ziele mit anderen Mitteln erreichbar | Terrorismusbekämpfung als Freibrief | permanenter Ausnahmezustand | Souverän ist, wer über den Ausnahmezustand bestimmt | Matthias Kettemann, Goethe Universität Frankfurt | Menschenrechte – wir brauchen Internet dafür | Pressefreiheit, Meinungsfreiheit | 1997: OSZE, Institut für die Freiheit der Medien, Leiterin: Dunja Mijatovic | alte und neue Demokratien | Beschränkungen lösen keine Probleme | Humanitäres Völkerrecht, Genfer Konvention, Europäische Menschenrechtskonvention | nationale Gesetzgebungen | Aufgabe der Medien | Information und Debatte | Aufklärung, Kontext | Zugang zu Informationen | Spekulation, Öffentlichkeit kann die Entscheidungen der Regierungen nicht mehr kontrollieren | Aufdecker sind gefährdet | Name and Shame | Open Journalism, OSZE

Teil 4: Wer kontrolliert das Internet?

Kontrolle des Internets | Macht über Informationen | Strafverfolgungsbehörden, Geheimdienste, Militärs | Reinhard Posch, Chief Information Officer der Österreichischen Bundesregierung | Nationalstaaten | Hardware aus Fernost, Software aus USA | Sicherheitsübungen | Bewusstsein | 70% IT-gesteuerte Geräte sind in Deutschland nicht gesichert | Funktionalität | Dinge für ein bequemeres Leben | Abhängigkeit vom System | Louis Pouzin, Computerwissenschaftler | Paketvermittelte Datenübertragung | Internet Governance | Militärs, Computernetzwerke als Kriegsgebiet | 1996 Wassenaar Arrangement, Leiter: Philip Griffiths, neuseeländischer Botschafter | Überwachungssoftware | Datenfluss garantieren, Datenfluss kontrollieren | Dual-Use Liste | Roger Cucchietti, Senior Officer im Sekretariat Wassenaar Arrangement | Verschlüsselungssoftware | Multi-Stake-Holder | ICANN steht für "Internet Corporation for Assigned Names and Numbers" | staatlich, technisch zentriert | Entwicklungsländer | China | all das ist sehr kompliziert | man muss aber politische Entscheidungen treffen: Bildung, Kommerz, Kommunikation | manche Länder machten eigenes Netzwerk | Mittlerer Osten, Länder mit Geld | 2005: China