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

Fragen und Antworten

Teil 1: Was ist ein Cyberwar

1. Wo ist der Unterschied zwischen einem Krieg (engl.: „war“) und einem Cyberwar?

Krieg: Armeen und Staaten kämpfen gegeneinander, ein Krieg hat Beginn und Ende, als Ziel/Folge: die Bildung eines neuen Staates oder der Gewinn von Land.
Cyberwar: Ein erkennbarer Feind ist abhanden gekommen. Im Internet kann kein Krieg erklärt werden; man kann auch kaum einen Notstand ausrufen. Kritiker sprechen auch daher lieber nicht von Cyberwar, sondern von Konflikt. Er kann – anders als ein Krieg – völkerrechtlich nicht legitim geführt werden.

2. Was ist ein Notstand?

Die Verfügung drastischer Maßnahmen innerhalb eines Staates, wenn die Ordnung nicht hergestellt bzw. gesichert werden kann. Die Öffentliche Gewalt kann dabei ihre Bindung an Gesetz und Recht einschränken.

3. Wie bzw. warum wurde der Vietnam-Krieg beendet?

Maßgeblich war die Veröffentlichung der „Pentagon-Papiere“ (geheime Papiere des US-Verteidigungs-ministeriums, die eine gezielte Irreführung der Bevölkerung durch den Präsidenten belegte) in den 1970-er Jahren.

4. Welche Beispiele gibt es für Cyberwar?

2007: Israelische Hacker dringen in die Computersysteme der syrischen Luftabwehr ein.
2010: Stuxnet: Die Steuerung von iranischen Zentrifugen wurde verändert.
2012: Saudische Ölfirma wurde gehackt; Nordkorea verübte Cyberangriffe auf südkoreanische Einrichtungen.

5. Kann ein Cyberwar beendet werden?

Das Schwieriige ist, dass nicht klar ist, wer der Feind ist, wer die Schadsoftware in einem Computer installiert hat – daher kann man mit ihm nicht Frieden schließen. Der Angriff kann von einer anderen Stelle gestartet worden sein.

Ein Projekt von

PH Wien BMBF

ORF 1 RADIO ÖSTERREICH 1

Teil 2: Cybercrime oder Cyberwar

1. Wo ist der Unterschied zwischen Cybercrime und Cyberwar?

Kriminalität ist meist „unpolitisch“, die Identität soll verschleiert werden. Ein Krieg dagegen ist immer „politisch“, die Identität der Soldaten wird gezeigt.
Es gibt aber auch eine Grauzone, in der diese Definitionen verschwimmen.

2. Warum ist Zeitgewinn bei einem Cyberwar von Vorteil?

Es gilt das Motto: „Kontrolliere die Geschichte, die Informationen.“ Falschinformationen und Propaganda helfen, den Gegner von einer Idee zu überzeugen, Zeit ist dazu notwendig.

3. Was versteht man unter „Schadsoftware?“

Sie wird auf dem Computer des Gegners installiert, sie führt Aufgaben aus, verschickt z.B. E-Mails unter falscher Identität oder zeichnet Ton, Bild oder Tastenanschläge auf. Regierungen behaupten, es gäbe auch „gute Schadsoftware“, wie z.B. den Bundeskriminalamt-Trojaner der Deutschen Bundesregierung.

4. Was versteht man unter Ransomware?

Ransomware sind Schadprogramme, mit denen Benutzer erpresst werden. Es wird dabei die Kontrolle über den Computer übernommen, oder es werden die Daten verschlüsselt bis ein Lösegeld bezahlt wird.

5. Gibt es im Internet eine Kontrolle über den Weg, den die Daten nehmen?

Im Allgemeinen nicht, es wird aber immer wieder der Wunsch danach formuliert, dass Daten nicht den Umweg über ein anderes Land nehmen sollen – zum Beispiel bei Banküberweisungen.

Ein Projekt von

PH Wien BMBF

ORF 1 RADIO ÖSTERREICH 1

Teil 3: Macht der Daten – Grundrechte oder Strafverfolgung

1. Was versteht man unter Vorratsdatenspeicherung?

Die Speicherung personenbezogener Daten durch staatliche Einrichtungen, ohne dass ein aktueller Anlass dafür besteht. Für Kritiker ist das ein nicht zu akzeptierender Eingriff in die Grundrechte von Menschen.

2. Wer hat Interesse an Vorratsdatenspeicherung?

Regierungen, Geheimdienste, Strafverfolgungsbehörden. Die Gründe werden von diesen Einrichtungen aber nur vage diskutiert und kommuniziert – sagen Kritiker.

3. Welche Grundrechte gibt es im Bereich der Informationsvermittlung?

Es gibt Sicherheits- und Freiheitsrechte: Recht auf freie Meinungsäußerung, Recht auf Privatheit, Recht auf Bildung, Recht auf Arbeit, Recht auf Information, Recht auf Teilnahme am Gemeinwesen: Menschenrecht „auf Internet“.

4. Welche „Konventionen“ gibt es im Zusammenhang mit Krieg und Menschenrechten?

Humanitäres Völkerrecht, Genfer Konvention, Europäische Menschenrechtskonvention, Charta der Grundrechte der Europäischen Union, etc.

5. Was machen Aufdecker?

Menschen, die Zugang zu Informationen haben, veröffentlichen diese, um sie zugänglich zu machen.

Ein Projekt von

PH Wien BMBF

ORF 1 RADIO ÖSTERREICH 1

Teil 4: Wer kontrolliert das Internet

1. Welche Rolle hat eine Strafverfolgungsbehörde?

Sie stellt Rechtsübertritte (Straftaten) fest und „verfolgt sie“.

2. Warum haben im Internet Nationalstaaten nicht mehr die Hoheit über Strafverfolgung?

Die Computerindustrie übernimmt immer mehr die Macht über Informationen – Hardware aus Fernost, Software aus den USA. Digitale Sicherheitsvorkehrungen können nicht mehr von Nationalstaaten kontrolliert werden.

3. Warum sind IT-gesteuerte Geräte im Gebrauch durchaus problematisch?

Sie sind nicht vor dem Hintergrund der Sicherheit gebaut, sondern vor dem Hintergrund der Funktionalität. „Autos und Kaffeemaschinen“ werden dafür zunehmend mit Sensoren ausgestattet.

4. Was versteht man unter Dual-Use Gütern?

Das sind Geräte und das ist Software mit „doppeltem Zweck“. Ihr Einsatz ist sowohl für zivile als auch für militärische Zwecke möglich. Überwachungs- oder Verschlüsselungssoftware würde unter diese Definition fallen. Sie kann den Betrieb der Daten im Internet sicherstellen, sie kann ihn aber auch kontrollieren.

5. Wer kontrolliert das Internet?

ICANN: „Internet Corporation for Assigned Names and Numbers“, eine staatlich-technisch-zentrierte Vereinigung von „Multi-Stake-Holder“: Staaten, Firmen, Lobbyisten. Es sind aber auch Staaten selbst, die eigene Netze zunehmend selbst betreiben und kontrollieren, z.B. China.