Technische Universität Chemnitz
Philosophische Fakultät
Institut für Politikwissenschaft
Professur Internationale Politik
Dozent: Jakob Kullik, M.A.
Referenten: Lucas Hums, Hubertus Leo Weigel

SoSe 2021
03.05.2021

Globales Internet, Netzpolitik und Cybersicherheit

1 Globales Internet

Zentrale Datenansammlungen und komplexe Service-Plattformen

- Probleme:
  - → Starke Bindung an Oligopole
  - → Hacks / Leaks sind verheerender als bei Dezentralisierten Plattformen
- Lösung: stark integrierte Service Plattformen vermeiden, dezentralisierte Dienste

Kritische Daten liegen bei außereuropäischen Unternehmen

- Problem: Starke Abhängigkeit von USA und China,
- Ziel: Kontrolle über Daten zurückholen
- Lösungsansätze:
  - → Langfristige Investition in eigene europäische Infrastruktur
  - → lokale Unternehmen unterstützen um, auf dem zersplitterten europäischen Markt bestehen zu können

2 Formen von Cyberangriffen:

Diese Phänomene verschwimmen oft und sind eher als Überblick und für Rechtsprechung interessant.

Hacktivismus

Das nicht-profitorientierte Nutzen von Hacking-Tools (z.B. [D]DoS-Attacken) für Protest- bzw. Propagandazwecke, Ziel ist hohe Aufmerksamkeit: dafür werden aus ideologischen Gründen gestohlene vertrauliche/persönliche Daten oder Passwörter veröffentlicht.

Internetaktivismus

Nutzung von sozialen Medien und des Internets als Diskussions-, Kommunikations- und Informationsmittel z.B. zur Planung von Aktionen. Dabei werden keine Hacking-Tools genutzt. Themen von Netzaktivisten sind demokratische Nutzung und Gestaltung des Internets, gleichberechtigter Zugang zum Netz, Urheberrechtsproblematiken und der Kampf gegen Zensur.

Cyberkriminalität

Cyber-Attacken gegen Privatpersonen oder Unternehmen mit Ziel des persönlichen Profits, die dabei eingesetzten Mittel sind vielfältig. Dabei wird in Cyberkriminalität im engeren Sinne: also Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung

von Daten- oder Kommunikationstechnik begangen werden und Cyberkriminalität im weiteren Sinne: dabei handelt es sich um herkömmliche Straftaten bei denen Daten- oder Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung genutzt werden.

Cyberspionage

Informationsraub von öffentlichen Stellen, der sowohl profitorientiert als auch nicht-profitorientiert motiviert sein kann. Es kann in intrusiv, d.h. das einfache „Abhören" einer (verschlüsselten) Nachricht und nicht-intrusiv; also dem Informationsraub durch das Einsetzen von Cyberangriffen, unterschieden werden.

Cyberterrorismus

Das Nutzen des Internets zu Propaganda- und Radikalisierungs- und Rekrutierungszwecken und Cyberangriffen mit dem Ziel materielle oder physische Schäden zu verursachen.

Cyberkrieg

Cyber-Attacken zur Nutzung staatlicher Kriegsführung, wobei mindestens eine der am Konflikt beteiligten Parteien ein staatlicher Akteur sein muss.

3 Cyber-Außen- und Sicherheitspolitik EU

3.1 Akteure

- EU-Agentur für Netz- und Informationssicherheit (ENISA)
- Europäisches Zentrum zur Bekämpfung der Cyberkriminalität (EC3) welches zu Europol gehört
- EU-Zentrum für Informationsgewinnung und -analyse (INTCEN)
- Abteilung Aufklärung des Militärstabs der EU (EUMS INT) und sein Lagezentrum (SITROOM)
- IT-Notfallteam für die Organe und Stellen der EU (CERT-EU)
- Europäischen Kommission

3.2 Cyberdiplomatie

Vier Pfeiler der EU-Cybersicherheit:

1. Schaffung von Instrumenten zur wirksamen Täterverfolgung
2. IT-Produkte und -Dienstleistungen durch Marktanreize sicherer machen, Nutzer in die Lage versetzen, fundierte Kaufentscheidungen zu treffen, Vereinheitlichung verschiedener Zertifizierungssysteme zur Vervollständigung eines digitalen Binnenmarkts
3. Standardisierung militärischer Systeme (elek. Ausrüstung -> Sprach-, Datenkommunikation, Software), Schaffung eines „Cyber-Schengenraumes"
4. Bilaterale Cyberdialoge zwischen EU und Regierungen der Mitglieder

Oktober 2017 Diplomatischer Reaktionsrahmen:

- Cyberwerkzeugkasten = Festlegung gemeinsamer diplomatischer Konsequenzen bei Angriff
- Eindämmung unmittelbare/langfristiger Bedrohungen erleichtern
- Hilfe Einwirkung auf Verhalten Tätern/potentieller Angreifer

Fünf Kategorien von Maßnahmen:

- Prävention: durch Aufbau von Cyberdialogen mit Drittstaaten und Regionalinstitutionen wird versucht, das Verhalten und die Positionierung der Dialogpartner zu beeinflussen
- Kooperation: im Konfliktfall arbeiten von einer Cyberattacke betroffene Staaten zusammen, sofern eine EU-Delegation im betroffenen Land vorhanden ist
- Stabilisierung: Beschlüsse der EU müssen mit Mitgliedsstaaten abgestimmt sein, sofern keine schnelle Reaktion nötig ist und eine Abstimmung nicht möglich ist
- Restriktionen: Rat kann mit Einstimmigkeit Sanktionen gegen Vertreter bestimmter Regierungen, Staatsunternehmen oder Personen verhängen, wenn Rechtmäßigkeitsvoraussetzungen erfüllt sind und im Einklang mit den GASP-Zielen stehen
- Völkerrechtskonforme Reaktionen: Solidaritäts- und Beistandsklausel aus dem Vertrag von Lissabon können auch bei schwerwiegenden Cyberangriffen angewandt werden

Dual-Use-Verordnung Mai 2009:

- Regelung gemeinsamer Genehmigungspflichten aller Mitgliedsstaaten für Ausfuhr, Vermittlung, Durchfuhr von Dual-Use-Gütern
- Dezember 2019 Aktualisierung

3.3 Probleme

- Einstimmungserfordernis im Rahmen der GSVP/GASP
  - → Verschiedene Interessen/Prioritäten der Mitgliedsstaaten
  - → Unterschiedliche technische Entwicklung der einzelnen Mitgliedsstaaten
- Mitgliedsstaaten müssen Anstrengungen zur Stärkung der Sicherheit im digitalen Rauem erhöhen
- Streitfrage wann aktive Verteidigung wie z.B. Hackbacks gerechtfertigt sind und wie die Kompetenzen verteilt werden sowohl auf nationaler wie europäischer Ebene
- Cyberdiplomatie nur wirksam, wenn sie europäische und globale Dimensionen mit einbezieht und geschlossen von allen Mitgliedsstaaten angewandt wird

4 Deutsche Cybersicherheit

4.1 Akteure:

Cyber-SR	Berät 3 mal Jährlich über Trends und langfristige Handlungsnotwendigkeiten. Veröffentlicht regelmäßig Impulspapiere → BMI, BKAmt, AA, BMVg, BMWi, BMJV, BMF & BMBF; ggf BfV &
BSI	Zentraler Sicherheitsdienstleister des Bundes. Aufgabe: IT-Sicherheit des Bundes sicherstellen. Berät auch Länder. Gehört zum BMI.
BND	Auslandsnachrichtendienst. Erfasst alle Angriffe von außen-/sicherheitspolitischer Bedeutung, z.B. Spionage oder Sabotage. Gehört zum BKAmt.

Bundeswehr	Im Cyber- und Informationsraum (mobil) im Außland und Inland kämpfen.
ZITiS	Zentrale Anlaufstelle und Dienstleister vom Bund für technische Probleme.
CERT‘s	Computer-Notfallteam und Anlaufstelle für alle Bundesbehörden im Falle eines sicherheitsrelevanten IT-Vorfalls

4.2 Cyberkriminalität in Deutschland:

- Professionalität global vernetzter, international agierender Täter steigt stetig an
- Cyberkriminelle arbeiten arbeitsteilig und höchst organisiert
  - → Zusammenarbeit erfolgt anonym und über Foren im Darknet
- Anstieg Cyberkriminalität im engeren Sinne um 15,4% auf ca. 100.500 Fälle

4.3 Probleme

- Deutschland Teil Amerikanisch-Chinesischen Datenmonopols
  - → Wesentliche Infrastrukturen und Dienstleistungen von außereuropäischen Anbietern bereitgestellt
  - → Wenige große Akteure (Amazon, Microsoft, Apple, Huawei, Alibaba)
- Unvollendeter digitaler Binnenmarkt
- Vorwiegend regulatorische Reaktionen auf digitale Bedrohungen
- Zu viele Akteure die an deutscher Cybersicherheitspolitik beteiligt sind
  fünf Bundesministerien (Inneres, Wirtschaft, Verkehr, Äußeres, Verteidigung), 40 Behörden
- Bundeswehr schlecht für digitale Kriegsführung gerüstet

4.4 Mögliche Lösungsansätze:

- Reduzierung Behörden, mehr Kompetenzen für bestehende
  z.B. Aufbau eigenes Ministerium, Verantwortungsbereich Spionageabwehr/Wirtschaftsschutz von BfV zu BND
- Offensive Gegenreaktionen (z.B. Hackbacks) als Maßnahme erleichtern und nicht durch zu viele Regulationen einschränken
- Strategische Investition in konkurrenzfähige IT-Unternehmen
- Schaffung gemeinsamer Datennetze/-zentren auf europäischer Ebene
  - → Deutschland kommt als größte Volkswirtschaft in der EU Schlüsselrolle zu
  - → Behauptung Werte der EU im digitalen Raum ermöglicht durch Kontrolle eigener Datennetze
- Abhängigkeit von geschlossenen Systemen reduzieren
  - → Auf gemeinsame offene Software setzen
  - → Qualität von Open-Source-Software sicherstellen
- Defensive Sicherheitsmaßnahmen ausbauen
  - → Dezentrale statt zentrale Systeme
  - → Ende-zu-Ende-Verschlüsselung zum Standard machen
- Wirken von Geheimdiensten einschränken
  - → Unabhängige und evidenzbasierte Sicherheits- und Geheimdienstpolitik

Quellen:

1. Al-Ani, Ayad (2019): Algorithmische Schlachten, in: Internationale Politik, Januar/Februar 2019 (1), S. 100-104.
2. Bendiek, Annegret (2018): Die EU als Friedensmacht in der internationalen Cyberdiplomatie, Stiftung Wissenschaft und Politik, SWP-Aktuell Nr. 22, März 2018.
3. Bundeskriminalamt (2020): Cybercrime Bundeslagebild 2019, 30. September 2020, URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/C6ybercrime/cybercrimeBundeslagebild2019.html (letzter Zugriff: 23.03.2021).
4. Bundeskriminalamt (2015): Hacktivisten. Abschlussbericht zum Projektteil der Hellfeldbeforschung, 20. Februar 2015, URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015HacktivistenProjektteilHellfeldbeforschung.pdf?__blob=publicationFile&v=5 (letzter Zugriff: 02.05.2021).
5. Herpig, Sven / Bredenbrock, Clara (2021): Cybersicherheitspolitik in Deutschland. Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum, Stiftung Neue Verantwortung, 01.04.2021.
6. Kullik, Jakob (2021): Deutschlands Cybersicherheitsstrategie im nächsten Jahrzehnt: Sicherheitspolitische Selbstbehauptung in der amerikanisch-chinesischen Digitalweltordnung, Arbeitspapier Nr. 2/2021, Bundesakademie für Sicherheitspolitik
7. Neuman, Linus (2014): Effektive IT-Sicherheit fördern, 07.03.2014, URL: https://ccc.de/system/uploads/149/original/StellungnahmeDigitaleAgenda.pdf, (letzter Zugriff: 02.05.2021).
8. Werkner, Ines-Jacqueline/Schörnig, Niklas (Hrsg.) (2019): Cyberwar – die Digitalisierung der Kriegsführung: Fragen zur Gewalt. Wiesbaden: Springer.