Jahresthema 2023 „Gemeinsam: Was und welche Werte halten unsere Gesellschaft zusammen?“

Dritter Vortrag des Jahres 2023 am 9. Oktober 2023 in der Hanns-Seidel-Stiftung, München

PROF. DR. WOLFGANG HOMMEL,
UNIVERSITÄT DER BUNDESWEHR, MÜNCHEN

CYBER DEFENCE.
INDIVIDUELLE, GESAMTSTAATLICHE UND EUROPÄISCHE AUFGABE

Das Thema ist komplex wegen der viele Abhängigkeiten.

- Ausgehend vom Begriff „Cyber“ – was bedeutet das?
  Cyber ist eigentlich eine Vorsilbe, ein Wortbildungselement mit der Bedeutung „im Internet befindlich, das Internet betreffend“.[1]
- Es geht um Kommunikation! Und zwar Kommunikation von Menschen und Maschinen:

  Es ist bei der Kommunikation zu unterscheiden, ob die Nachricht sofort oder verzögert übermittelt wird;
  gewünscht wird immer die sofortige Übermittlung.

  Dann gibt es noch die Unterscheidung, wie viele andere erreicht werden sollen.

  Und letzte Unterscheidung ist, von wem die Kommunikation zu verwenden ist: von einigen wenigen Auserwählten und Privilegierten oder von jedem.

  Meilensteine der Kommunikation:

  > Es begann mit (direkter) mündlicher Kommunikation, dem persönlichen Gespräch, dann folgten Boten, die mündliche oder schriftliche Nachrichten übermittelten, die Post 1490 und erste Zeitungen um 1600 – dies alles verzögert in der Übermittlung im Gegensatz zum persönlichen Gespräch.
  >
  > Dann folgten Telegrafen- (um 1840) und Telefonnetze (um 1880), Amateurfunk (um 1900) und Radio- (1920) und Fernsehrundfunk (1935).
  >
  > Botennachrichten, Zeitungen, Radio und Fernsehen kommen nur von ausgewählten Absendern, während die Empfängerzahl bei den beiden erstgenannten Medien begrenzter ist als bei den letztgenannten.

[1] cyber- – Wiktionary; während der Duden „Cyber“ mit „die von Computern erzeugte virtuelle Scheinwelt betreffend“ übersetzt, siehe cyber- ▶ Rechtschreibung, Bedeutung, Definition, Herkunft | Duden.

Als neueste Medien der Kommunikation folgten in den 1980er Jahren die (kommerziellen) Mobilfunknetze und das seit den 1990er Jahren populäre Internet, auch hier ist wieder Unterscheidungskriterium die (nur beim Internet sehr hohe) Anzahl der Empfänger.

Es geht jeweils um die Übertragung von Daten (Texte, Videos) und Sprache „für alle von überall“ an Einzelne, Gruppen oder die weltweite Öffentlichkeit.

Eingeschränkt wird die Kommunikation durch Zensurbemühungen; auch in Europa: in der EU ist „Russia Today“ nicht mehr (direkt) zugänglich.

Die technischen Möglichkeiten sind faszinierend, *Stichwort „globales Dorf“:*

- Internet als Kommunikationsmedium: Menschen kommunizieren mit Menschen
  - mittels Computer (PC, Notebook, Tablet, Smartphone…)
  - entweder synchron durch Internet-Telefonie, Videokonferenz, Chat-Nachrichten…
  - oder asynchron per E-Mail, Diskussionsforum, gemeinsames Arbeiten an einem Dokument
  - und für beliebige Zwecke wie Kontaktpflege, Informationsaustausch, Geschäftsbeziehungen
- Internet als kommerzielle Plattform: Menschen kommunizieren mit Computern
  - beispielsweise über den Abruf von Daten (Zeitung/News/Social Media, Streaming von Musik oder Videos)
  - oder über Nutzung teilautomatisierter Dienste wie Online-Banking oder Online-Shopping

  Hierfür wird die Internetinfrastruktur immer weiter ausgebaut.
- Internet der Dinge (Internet of Things, IoT), es kommunizieren Computer mit Computern:
  - industrielle Steuerungsanlagen mit Sensoren und Aktoren[2]
  - automatisierter Handel an den Börsen
  - Smart Home: es schaltet die Heizung ein, sobald (das Smartphone) ein(es) Familienmitglied(s) auf dem Heimweg ist
  - Cyber bedeutet auch, dass Geräte vernetzt sind - eventuell sogar weltweit

Warum „Cyber Defence“?

- Essentielle, komplexe Infrastruktur:
  - Selbstgemachte, fast vollständige Abhängigkeit vom Internet innerhalb von 30 Jahren in praktisch allen Bereichen entstanden (Zahlungsverkehr, Logistikprozesse etc.)

[2] Ein Aktor setzt elektrische Signale in mechanische Bewegungen oder andere nichtelektrische Größen um, siehe Aktor - Lexikon der Physik (spektrum.de)

- Flächendeckende Digitalisierung als strategisches Ziel (siehe z. B. dt. Gesundheitswesen)
- Benötigt Strom, Vernetzung (über Verkabelung oder Funk) und Geräte (Stichwort „digitale Souveränität“)
- Infrastruktur hierfür muss stabil am Netz sein, denn es betrifft so gut wie alle Bereiche, sie sind davon abhängig
- Problematisch ist/kann werden, dass die Geräte meist in Fernost gefertigt werden, während die Lizenzen für die Software aus Nordamerika stammen.

- Menschen
  - können im Internet z. B. potentielle Opfer einer Vielzahl von Betrügern werden
  - müssen z. B. den Wahrheitsgehalt beliebiger ungefilterter Informationen beurteilen können
  - können u. U. durch „Cyberangriff“ dazu gebracht werden, anders zu agieren als gewünscht
  - denn: Kommunikation zwischen Computern ist zu komplex, um alles zu bedenken.

Schutz der Kommunikationsinfrastruktur

- Zwei Beispiele für die Bedeutung dieses Schutzes:
  - Erhebliche Störungen des Zugverkehrs im Oktober 2022
  - und des Flugverkehrs im Februar 2023
  durch absichtliche[3] oder versehentliche[4] Beschädigung *einzelner* Glasfaserkabel
- Der Schutz dieser Infrastruktur ist lebenswichtig:
  - vor Zufall wie dem Ausfall eines Routers: Redundanz
    Redundanz bedeutet die Sicherstellung der Verfügbarkeit technischer Einrichtungen durch Bereitstellung eines Ersatzsystems[5].
  - vor regional begrenzten Katastrophen wie im Ahrtal 2021
    - sofortige Hilfsmaßnahmen nötig,
    - aber die provisorische Wiederherstellung der flächendeckenden Stromversorgung dauert Wochen
    - Internet: nur punktuelle Versorgung über Satellit
  - Krieg mit gezielter Kommunikationseinschränkung
    - bedeutet systematische Störung oder Zerstörung von Energieerzeugung/-transport, Datennetzen und Rechenzentren, Satelliten…

[3] Siehe Sabotage an Bahn-Kabeln legt Zugverkehr stundenlang lahm | rbb24.

[4] Siehe IT-Probleme bei der Lufthansa - Flugverkehr beeinträchtigt | tagesschau.de

[5] NETZWERKREDUNDANZ: 7 FAKTOREN FÜR EIN GUTES NETZWERKDESIGN | COMPUTER WEEKLY ODER AUCH REDUNDANZ - MODULARITÄT - SKALIERBARKEIT (BUND.DE)

- Lösungsansatz Redundanz?
  - Kopien wichtiger Daten an verschiedenen Orten
  - Bevorratung technischer Komponenten teuer und durch Innovationszyklen kaum sinnvoll
  - Problem der Lieferkette: Mangel an europäischen Herstellern, z. T. lange Lieferzeiten durch fragile Lieferketten
- Beispiele:
  - Steckenbleiben eines Frachters im Suezkanal[6]
  - Lockdown in China[7]
  -> massive Beeinflussung der internationalen Lieferketten

Schutz der Menschen

- Themenbereich gefälschte Informationen (Fake News etc.):
  - Desinformationskampagnen, z. B.:
    - Kriegsberichterstattung
    - Beeinflussen demokratischer Prozesse/Verschwörungstheorien
    - Radikalisieren von Zielgruppen/Diskreditieren von Minderheiten
  - Kombination u. a. aus
    - KI-gestützter Erzeugung von (manipulierten) Texten, Bildern, Sprache und Videos
    - automatischer Übersetzung in Fremdsprachen/Herkunft v. a. aus dem Ausland
    - schneller Verbreitung incl. Kopien über das Internet
    - und dem Echokammer-Effekt (aufgrund der Vorlieben des Nutzers werden Stil, Stichworte und Zielgruppe vorgegeben)
  - Beispiele: gefälschte Fotos von Putins Kniefall vor Xi Jinping oder Papst Franziskus in Daunenjacke[8]
- Gegenmaßnahmen?
  - Zensur
  - seriöse „Faktenchecks“
  - „Awareness“: kritisches Reflektieren, „gesunder Menschenverstand“
  - Gegenmaßnahmen sind schwierig und langsamer als Fake News

Schutz von Computern, Software und Daten

- Nach Hackerangriffen z. B. auf Kliniken dauert es Monate, die IT-Infrastruktur wiederaufzubauen.
  In Medienberichten über Hackerangriffe wird meist ein Foto des betroffenen Betriebes gezeigt, weil ein Hackerangriff nicht bildlich darstellbar ist – außer als schwarzer Bildschirm.

---

[6] Siehe Containerfrachter "Ever Given" - Lehren aus der Havarie im Suezkanal (deutschlandfunk.de) und Containerschiff im Suezkanal: Nicht der letzte Schock für die Lieferketten | ZEIT ONLINE

[7] Z. B. Lockdowns lassen Chinas Wirtschaft abstürzen – DW – 16.05.2022 oder Lockdown in China: Die Auswirkungen für die Industrie (produktion.de) (Juli 2022).

[8] KI-Fake: Warum das Papst-Foto nicht nur witzig ist - ZDFheute

- Herausforderungen hierbei:
  - jede Software aufgrund der inhärenten Komplexität kleine Fehler und Tausende von Sicherheitslücken enthält.
  - fehlendes Know-how, Fachkräftemangel bei sicherheitsfokussierten Informatikern und der Druck, mit neuen (IT-) Produkten schnellstmöglich auf den Markt zu kommen
  –> eine umsatzorientierte Priorisierung von Funktionalität („Features“) und Time-to-Market[9] anstatt (als Regel) Einbau von IT-Sicherheit
- Lösungsansätze?
  - zunehmende Regulierung: Verpflichtung von Herstellern und Betreibern zu z. B. Security-by-Design[10] und garantierter Verfügbarkeit für Software- und Security-Updates über einen längeren Zeitraum
  - spezialisierte Aus- und Weiterbildung von Fachkräften

Schuldzuweisung bei Angriffen (Attribuierung)?

- „Das Internet hat keine Grenzen“ vs. „Der Überbringer schlechter Nachrichten wird geköpft“:
  Angriffe zurückzuverfolgen ist schwer bis unmöglich, weil die Angriffe nie direkt, sondern über viele Stationen erfolgen und meistens wird nur der letzte Angreifer erkannt werden kann – wo genau der Angreifer sitzt, ist nicht zu ermitteln.
- Praktische Grenzen von „aktiver Cyberabwehr“ und „Hackbacks“: sind aus diesem Grund schwer möglich

Verteidigung im Vergleich

- Konventioneller militärischer Konflikt:
  - begrenzte Ressourcen auf beiden Seiten
  - Verteidigerposition kann Truppenbewegungen des Angreifers berücksichtigen
  - Kombattanten/Kämpfer sind konventionsgemäß als solche erkennbar[11]
  - Verteidiger können und dürfen sich wehren
  - Erfahrungswerte vorhanden aufgrund langer Historie
- Cyber-Angriff:
  - auch flankierend zu konventionellem Angriff
  - Asymmetrie zum Vorteil des Angreifers (u. a. Automatisierung)
  - Angriffsziele werden erst kurzfristig bekannt
  - eine Sicherheitslücke reicht, Abwehr ist schwer
  - Angriffe auch von/durch Zivilisten möglich
  - Position der Angreifer unbekannt, nicht lokalisierbar für einen „Hackback“

---

[9] Time-to-Market • Definition | Gabler Wirtschaftslexikon

[10] Security by Design - _erklärt | TÜV NORD (tuev-nord.de)

[11] Regeln des Krieges: Humanitäres Völkerrecht (bmvg.de)

- noch sehr begrenzte Erfahrungswerte

Exemplarische Maßnahmen und Pläne pro Ebene

- Individuell:
  - verantwortungsvoller Umgang mit der Technologie
  - Sensibilisierung der Menschen im eigenen Zuständigkeitsbereich
- Gesamtstaatlich:
  - Koordination der ressortübergreifenden Zusammenarbeit (in Bayern z. B. ist das BSI (Bundesamt für Sicherheit in der Informationstechnik)[12] neben dem LSI (Landesamt für Sicherheit in der Informationstechnik)[13] tätig) – Abstimmung untereinander?
  - rechtliche Rahmenbedingungen: Motivation schaffen, Mindestanforderungen und Grenzen festlegen
  - Bildung und Beratung
- Europäische Union:
  - länderübergreifende (auch zivil-militärische) Zusammenarbeit ist enger als national, Ausbildung/Standardisierung/Zertifizierung
  - Cyber Defence und technologische Souveränität als Ziele erkannt
  - zahlreiche Regulierungen
  - Beispiel: Aufbau eines Lagebildzentrums, CIDCC (Cyber and Information Domain Coordination Centre), bis 2026 (Deutschland, Frankreich, Niederlande, Ungarn)[14]

CODE[15] – exemplarische Aktivitäten des Forschungsinstituts an der Universität der Bundeswehr München

- Aktive Vernetzung von Bundeswehr, Behörden, Industrie und Wissenschaft
  - u. a. Mitgestaltung des Nationalen Koordinationszentrums für Cybersicherheit, NKCS[16]
- Aus- und Weiterbildung
  - u. a. Studiengang Cyber-Sicherheit für angehende Offiziere und zivile Studierende von Behörden
  - Cyber-Range: multinationale militärische Cyber-Übungen, Angebote für Cyber-Reserve und Behörden
- Forschungsprojekte (Auswahl)
  - Steigern der IT-Sicherheit in Krankenhäusern
  - Identifikation von Desinformationskampagnen durch Social Media

---

[12] BSI - Auftrag (bund.de)

[13] Über das LSI - Landesamt für Sicherheit in der Informationstechnik (bayern.de)

[14] Europäisches Verteidigungsprojekt für Cybersicherheit – Das CIDCC (bundeswehr.de)

[15] Über uns — code (unibw.de)

[16] Nationales Koordinierungszentrum für Cybersicherheit (NKCS) — code (unibw.de)

Mining[17]
- Erkennen des Einschleusens von Schadfunktionen in Open Source Software
- Aufbau von Quantenkommunikationsnetzen zur Absicherung der Behördenkommunikation
- sichere Kommunikationsprotokolle und Softwareentwicklung im Sektor Luftfahrt
- sichere Infrastruktur für die Steuerung elektrischer Netze für die zukünftige Energieversorgung
- Nutzen batteriebetriebener Low-Power-Wide-Area-Networks für die Kommunikation in Krisengebieten

EVA DITTRICH, ASS. JUR.

WEITERFÜHRENDE INFORMATIONEN:

- ÜBER DEN VORTRAGENDEN: UNIV.-PROF. DR. RER. NAT. WOLFGANG HOMMEL — CODE (UNIBW.DE) UND
- SOFTWARE SECURITY — SOFTWARE-SECURITY (UNIBW.DE)
- MARTIN VOGT, SOCIAL MEDIA MINING IN DER PRAXIS, WIST 2-3, 2021, S.23-29, WIS02-21 0001 (BECK.DE)
- WEBSITE BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: WWW.BSI.BUND.DE
- BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, 2018: REDUNDANZ - MODULARITÄT - SKALIERBARKEIT (BUND.DE)
- WEBSITE LANDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: LANDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK - LANDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BAYERN.DE)

(ALLE INTERNETQUELLEN ZULETZT EINGESEHEN AM 27.11.2023)

[17] Wis02-21 0001 (beck.de)