

«Cyber ...»

Der Begriff «Cyber» ist heute aus dem öffentlichen Diskurs nicht mehr wegzudenken. Kaum ein Tag vergeht, da die mediale Welt nicht über Cyberkriminalität, Cyberkrieg, Cyber Defence, Cybermobbing, über den Cyberspace oder eben über Cyber Security berichtet.

Das Wort «Cyber» stammt ursprünglich aus dem Griechischen und kann etwa mit «Steuerung» übersetzt werden. 1948 hat der amerikanische Mathematiker Norbert Wiener das Buch mit dem Titel «Cybernetics or Control and Communication in the Animal and the Machine» veröffentlicht, und damit die Wissenschaft der «Kybernetik» begründet – einer Forschungsrichtung, welche Systeme verschiedenster Art (wie biologische, technische oder soziologische Systeme) auf selbsttätige Regelungs- und Steuerungsmechanismen hin untersucht. Daraus entwickelten sich in der Folge zahlreiche angewandte Spezialdisziplinen wie etwa die Robotik, die Biomechatronik oder auch die Managementkybernetik.

«Cyber» geht also auf «Cybernetics» zurück und wird heute oft verwendet, wenn Bezug auf eine künstliche Realität resp. Virtualität genommen werden soll. Cybergeld ist dementsprechend virtuelles Geld. Der Begriff «Cyberspace» hat seinen Ursprung in der 1982 erschienen Science-Fiction Kurzgeschichte «Burning Chrome» von William Gibson, in der er eine künstliche, vom Computer geschaffene Welt beschreibt. Heute bezeichnet der «kybernetische Raum» – oder eben der «Cyberspace» – eine «virtuelle Welt», respektive «mittels Computern erzeugte räumlich anmutende oder gestaltete Bedienungs-, Arbeits-, Kommunikations- und Erlebnisumgebungen» (Zitat Wikipedia [1]). Der Cyberspace ist der Aktionsraum digitaler Identitäten (resp. Entitäten). Vielfach steht «Cyberspace» aber auch ganz einfach stellvertretend für «Internet».

Zu den Begriffen «Cyber Security» und «Information Security» gibt es unterschiedliche Definitionen und Beschreibungen. Einige Beispiele sind hier aufgeführt:

Cyber Security

1. Das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) schreibt auf seiner Webseite zum Thema «Cyber-Sicherheit»:

Die illegale Nutzung von digitalen Technologien ist eine Herausforderung des 21. Jahrhunderts. Der Cyber-Raum wird vermehrt für kriminelle, machtpolitische und nachrichtendienstliche Zwecke missbraucht. Angriffe über digitale Netzwerke auf Infrastrukturen wie Stromversorgung und Telekommunikation können ein Land destabilisieren. Die Schweiz geht mit der Nationalen Strategie zum Schutz vor Cyber-Risiken gegen Bedrohungen aus dem virtuellen Raum vor.

Störungen, Manipulationen, Sabotagen und gezielte Angriffe über elektronische Netzwerke gehören zu den Cyber-Risiken. Diese sind Begleiterscheinungen der Informationsgesellschaft. (...)

<https://www.eda.admin.ch/eda/de/home/aussenpolitik/sicherheitspolitik/neue-sicherheitspolitische-herausforderungen/cyber-sicherheit.html> (online, 14.11.2017)

2. Definition des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Deutschland:

Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik.

Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html (online, 14.11.2017)

3. Definition gemäss Glossary of Key Information Security Terms (NISTIR 7298, Revision 2) des National Institute of Standard and Technology (NIST) in den USA:

The ability to protect or defend the use of cyberspace from cyber attacks.

<http://dx.doi.org/10.6028/NIST.IR.7298r2> (online, 16.01.2018)

Definition von «cyberspace»

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

<http://dx.doi.org/10.6028/NIST.IR.7298r2> (online, 16.01.2018)

Definition von «cyber attack»

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

<http://dx.doi.org/10.6028/NIST.IR.7298r2> (online, 16.01.2018)

Information Security

1. Definition gemäss ISO/IEC 27000:2016, Information technology — Security techniques — Information security management systems — Overview and vocabulary

2.33

Information security

preservation of confidentiality (2.12), integrity (2.40) and availability (2.9) of information

Note 1 to entry: In addition, other properties, such as authenticity (2.8), accountability, non-repudiation (2.54), and reliability (2.62) can also be involved.

2. Definition gemäss Glossary of Key Information Security Terms (NISTIR 7298, Revision 2) des National Institute of Standard and Technology (NIST) in den USA:

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

<http://dx.doi.org/10.6028/NIST.IR.7298r2> (online, 16.01.2018)

Information Security versus Cyber Security

Die Frage nach der Verwandtschaft respektive nach dem Unterschied dieser beiden Begriffe wird oft gestellt, und sie wird ebenso oft unterschiedlich beantwortet. Häufig werden die beiden Begriffe einfach als Synonyme bezeichnet. Wer nach den beiden Begriffen recherchiert, wird jedoch rasch feststellen, dass es auch differenziertere Betrachtungsweisen gibt. So kann man z.B. in [2] nachlesen:

«These terms are often misused, because they are nearly synonymous. Both information security and cyber security are defined as the practice of defending information from unauthorised access, use, modification or disruption. The only difference between the two disciplines is in the form of the data. While cyber security refers only to electronic security, information security is a broader term that encompasses all data, both physical and digital.»

Information Security wird also als umfassende Obermenge bezeichnet und Cyber Security als Teilmenge davon, was die folgende Darstellung illustriert.



Abbildung 1: Information Security versus Cyber Security [2]

Noch differenzierter betrachten Rossouw von Solms und Johan van Niekerk das Thema in ihrem Dokument «From information security to cyber security». [3] Sie argumentieren, dass Cyber Security auch Aspekte umfasst, die Information Security nicht berücksichtigt. Um dies aufzuzeigen, erläutern sie Bedrohungen, die nicht zu einer Verletzung der Grundziele der Informationssicherheit, wie Vertraulichkeit, Integrität und Verfügbarkeit führen. Solchen Bedrohungen, die sie als «cyber security threats» bezeichnen, muss mit Massnahmen der Cyber Security begegnet werden. Beispiele für solche Bedrohungen sind:

- Cyber bullying: Gemeint ist Cybermobbing oder Internetmobbing, also die Verleumdung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Unternehmen mithilfe elektronischer

Kommunikationsmittel. Dabei wird weder die Vertraulichkeit, noch die Integrität oder die Verfügbarkeit von Informationen beeinträchtigt. Angriffsziel sind Menschen oder Unternehmen, denen Schaden zugefügt wird.

- Home automation: Kühlschränke, Heizungen, Stores, TV-Geräte oder Kaffeemaschinen können heute über webbasierte Interfaces via Internet gesteuert werden resp. kommunizieren darüber miteinander (Internet of Things). Angreifer können diese Geräte via Internet stören oder missbrauchen. Hier sind die Geräte das Ziel des Angreifers. Das Verfälschen von Informationen ist dabei Mittel zum Zweck.
- Digital media: Durch das illegale Teilen von digitalen Inhalten gehen der Unterhaltungsbranche jedes Jahr grosse Beträge verloren. Auch hier sind aber nicht Vertraulichkeit, Integrität oder Verfügbarkeit der Inhalte betroffen. Betroffen sind die Besitzer der Rechte an den Inhalten. Darüber hinaus wird das Wertesystem der Gesellschaft in Frage gestellt.
- Cyber terrorism: Cyber-Terroristen können heute über den Cyberspace kritische Infrastrukturen (Elektrizitäts- und Wasserversorgung, Telekommunikationsnetze, Transportinfrastrukturen etc.) angreifen. Solche Angriffe zielen weder direkt auf Informationen noch auf einen individuellen Besitzer dieser Informationen vielmehr wird die Bevölkerung eines Landes angegriffen.

Diese Beispiele zeigen, dass neben Informationen auch andere Werte geschützt werden müssen: Menschen, intelligente Geräte, die Interessen der Gesellschaft (z.B. ihr Wertesystem) oder die kritischen Infrastrukturen eines Landes. Vor diesem Hintergrund wird Cyber Security zu einer Erweiterung von Information Security. Sie schützt nicht nur Informationen und Systeme, die Informationen verarbeiten, sondern auch die Ressourcen, die wir in einer «Cyberumwelt» nutzen und sogar gesellschaftliche Werte. Die folgende Abbildung illustriert diesen Sachverhalt.

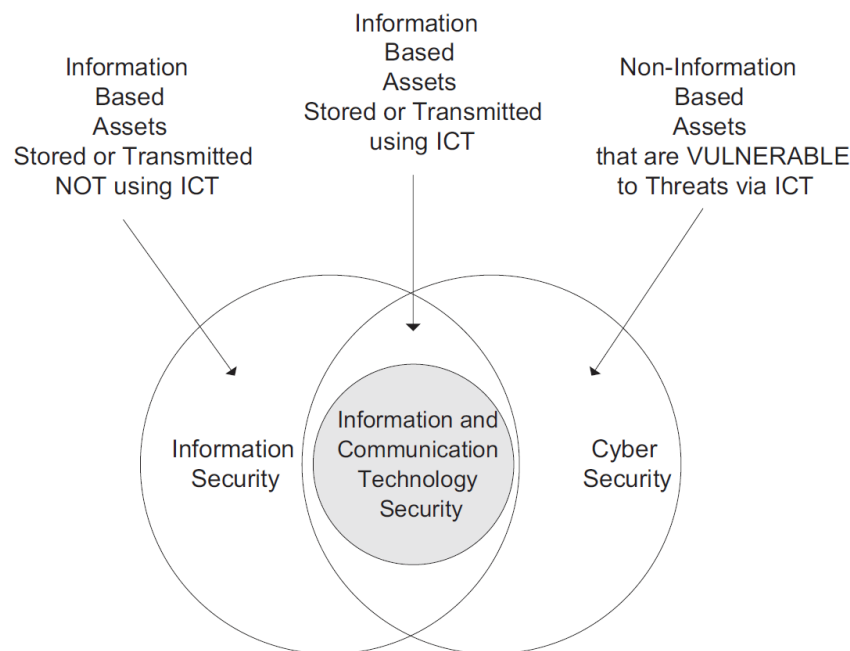


Abbildung 2: Information Security versus Cyber Security [3]

Fazit: Beide oben aufgeführte Sichtweisen haben ihre argumentative Berechtigung. Die zweite von Rossouw und van Niekerk gefällt aber besser, weil sie die raschen Veränderungen unserer sozialen und technologischen Umwelt und deren weitreichenden Auswirkungen besser widerspiegelt. Die zugehörigen Stichworte lauten «Social Networks», «Digitalisierung», «Internet of Things», «Cyber Physical Systems» oder «Industrie 4.0».

Bezug zu den CAS Information Security

Die Weiterbildungen in Informationssicherheit des Departements Informatik der Hochschule Luzern decken sowohl die klassischen Themen der Information Security ab als auch die neuen Themen aus dem Kontext der Cyber Security. Letztere sind schwerpunktmässig im CAS Information Security – Advanced zu finden.

Literaturverzeichnis

- [1] <https://de.wikipedia.org/wiki/Cyberspace> (online, 16.01.2018)
- [2] <https://www.legalfutures.co.uk/associate-news/data-protection-vs-information-security-vs-cyber-security> (online, 16.01.2018)
- [3] Von Solms R., Van Niekerk J. From information security to cyber security. Computers & Security 2013; 38:97-102. <http://dx.doi.org/10.1016/j.cose.2013.04.004> (online, 16.01.2018)