



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cybernation

→ **Motivation/Definition/Vorgehensweise**

Prof. Dr. (TU NN)

Norbert Pohlmann

*Professor für Cyber-Sicherheit und
Leiter des Instituts für Internet-Sicherheit - if(is)*

*Vorstandsvorsitzender des Bundesverbands IT-Sicherheit - TeleTrusT
Vorstandsmitglied des Verbands der Internetwirtschaft - eco*

if(is)
internet-sicherheit.

Cyber-Sicherheitslage

→ Motivation Cybernation

- *Die Cyber-Sicherheitsprobleme werden immer größer*
- **IT-Systeme** und **-Infrastrukturen** sind **nicht sicher genug konzipiert, aufgebaut, konfiguriert** und **upgedatete**, um den Angriffen intelligenter Hacker erfolgreich entgegenzuwirken.
- **Weitere Herausforderungen mit der fortschreitenden Digitalisierung:**
 - *IT-Systeme und -Infrastrukturen werden immer komplexer (Steigerung der Abhängigkeiten... mehr Software/Schwachstellen ... Supply-Chain...)*
 - **Angriffsfläche wird größer**
 - *Die Methoden der Angreifer werden ausgefeilter*
 - **Kriminelles-Ökosystems → mehr Angriffe**
 - *Angriffsziele werden kontinuierlich lukrativer (Digitalisierung)*
 - **mehr digitale Werte**

Digitalisierung

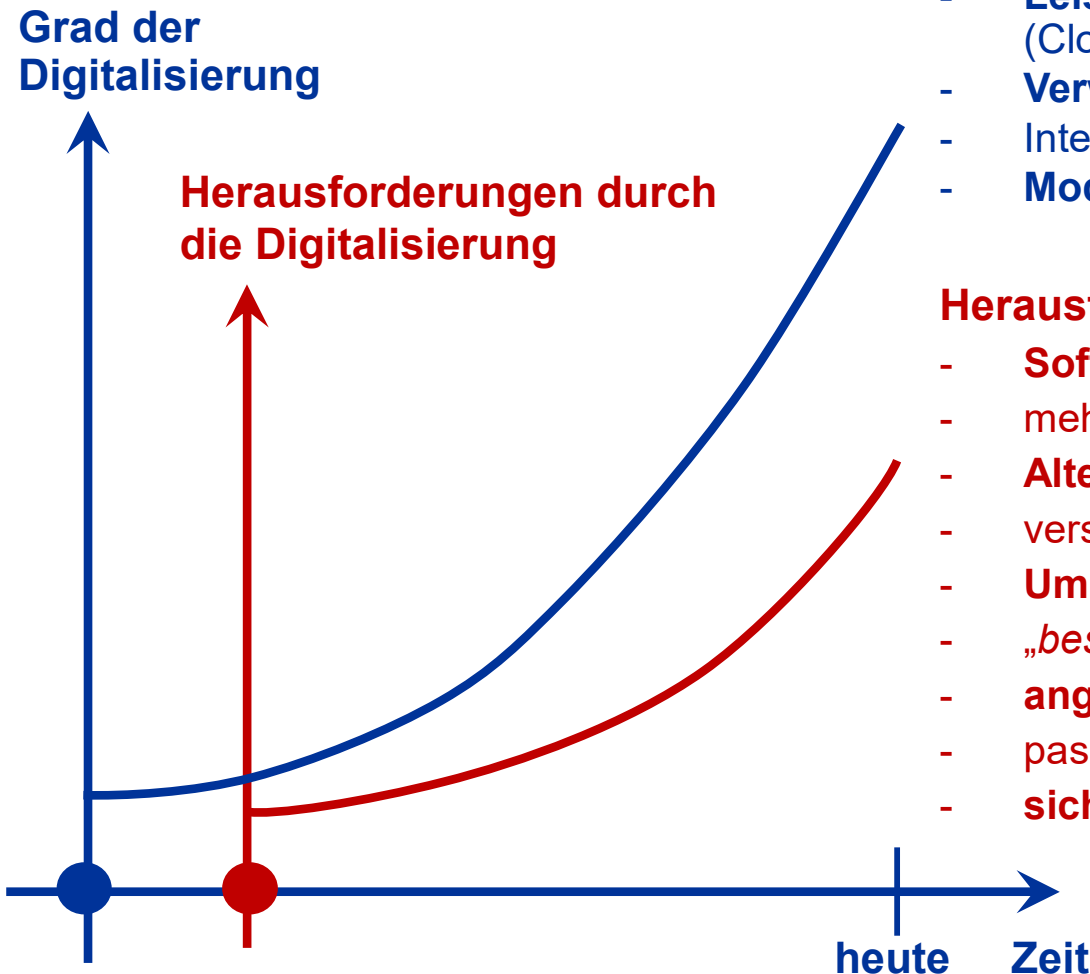
→ Die Basis für eine Cybernation

Erfolgsfaktoren der Digitalisierung (Beispiele)

- **Kommunikationsinfrastruktur** (5/6G, Glasfaser, „NFC“ ...)
- **Smarterheit der Endgeräte** (Watch, Phone, Book/Pad, IoT ...)
- **Leistungsfähigkeit zentraler IT-Systeme** (Cloud, Edge-Computing, Hyperscaler ...)
- **Verwendung von KI** (ML, LLM ...)
- **Integration in IT-Prozesse und IT-Systeme** (echtzeitorientiert+)
- **Moderne Benutzerschnittstellen** (Sprache, Gestik ...)

Herausforderungen Cyber-Sicherheit (Beispiele)

- **Softwarequalität** verbessern
- mehr Schutz vor Malware, unsichere Webseiten ...
- **Alternativen zu Passwörtern (MFA)** einführen
- verschlüsselte E-Mails, Kommunikation umsetzen
- **Umgang mit der Komplexität der IT-Systeme** managen ...
- „bessere“ IT-Sicherheitsarchitekturen motivieren
- **angemessene Verfügbarkeit** schaffen
- passenden Level IT-Sicherheit („Stand der Technik“) nutzen
- **sichere Hardware** (Sicherheitsmodule in IT-Systemen)



- Eine **Cybernation** ist ein **souveräner Staat**, der die **Möglichkeiten** und das **Potenzial** der **digitalen Technologien**
 - *umfassend*,
 - *sicher* und
 - *vertrauenswürdig*ausschöpft.
- Das **Ziel** ist, die **Digitalisierung im Sinne der Gesellschaft** engagiert umzusetzen, um die **wirtschaftliche Leistungsfähigkeit** sowie die **Effektivität** der öffentlichen Dienstleistungen zu maximieren.
- Eine **Cybernation** bietet eine **sehr gute Voraussetzung** für eine **souveräne, sichere und vertrauenswürdige digitale Zukunft**.

- Wir brauchen **robuste Cyber-Sicherheitsmechanismen** auf der Basis des „**Stand der Technik**“, um uns **wirkungsvoll** gegen immer intelligentere Angriffe zu schützen.
- Alle relevanten **Cyber-Sicherheitsbedürfnisse** müssen im Cyberraum **garantiert** werden (*Vertraulichkeit, Integrität, Verfügbarkeit ...*).
- Die Cybernation muss **erhebliche Ressourcen** (*15-20 % der IT-Ausgaben*) in die Stärkung ihrer **Cyber-Sicherheit** investieren, um sich
 - **gegen Cyber-Sicherheitsrisiken zu schützen,**
 - **um Schäden zu vermeiden.**
- Dadurch kann das **Vertrauen** aller Beteiligten **in die Digitalisierung** gestärkt und so eine **notwendige Akzeptanz** erreicht werden.

- Das **Cyber-Sicherheitsniveau** muss **substanziell erhöht** werden, um uns deutlich wirkungsvoller zu schützen.
- **Technologiekompetenz** muss weiter **aufgebaut** werden, um **souveräner**, sicherer und vertrauenswürdiger agieren zu können.
- Vorhandenes **Know-how** muss **effizient gebündelt** werden, um *nicht-hilfreiche* Doppelarbeit zu vermeiden.
- Es muss ein **aktives Cyber-Ökosystem** etabliert werden, um erfolgreich und souverän wirken zu können (*Technik, Recht und Investitionen*).
- Alle **Cyber-Sicherheitsakteure** aus Wirtschaft, Wissenschaft und Staat in Deutschland müssen **eng zusammenarbeiten** und **gemeinsam handeln**.
- Wir brauchen ein gemeinsames und umfangreiches **Cyber-Sicherheitslagebild**, um schnell und gezielt aktiv zu werden.
- Die **Cyber-Resilienz** muss **wesentlich gesteigert** werden, um die Stärkung der Widerstandskraft aller IT-Systeme und IT-Infrastruktur zu gewährleisten.

Cybernation

→ Vorgehensweise

- Nur durch eine
 - **enge Zusammenarbeit** aller wichtigen Akteure,
 - die Motivation und Realisierung **passender Innovation** und
 - **gemeinsame** und **feste Entschlossenheit**

kann Deutschland eine wirkungsvolle Cybernation werden und die digitale Zukunft *souverän, sicher, vertrauenswürdig* und *erfolgreich* gestalten.

- Dazu brauchen wir **gemeinsame Ziele** und **ein Kommittent** zwischen den **wichtigen Akteuren**.
- Die Idee ist vorhanden, nur die **Umsetzung muss jetzt motiviert werden**.

Gemeinsame Umsetzung von E-Mail-Sicherheit

- **Verschlüsselung**, um die Vertraulichkeit von E-Mails zu gewährleisten
- **Digitale Signatur**, um
 - die Verbindlichkeit von Businessabläufen zu gewährleisten *und*
 - ***Spear-Phishing- von echten E-Mails unterscheiden zu können***
- **Umsetzung / Aktivitäten**
 - Gemeinsam Ziele sowie den Umsetzungszeitpunkt definieren
 - Einfache Dienste und Technologien kollektiv motivieren
 - Aufklärung vereint durchführen, um die Umsetzung zu fördern
 - ...

Weitere Themen: Zero Trust,

***Angebot von zentralen sicheren Cloud-Anwendungen für kleine Unternehmen,
Ressourcen-optimierte Aufteilung der notwendigen IT-Sicherheitsaktivitäten ...***



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cybernation

→ **Motivation/Definition/Vorgehensweise**

*Gemeinsam für eine souveräne, sichere und
vertrauenswürdige digitale Zukunft*

Prof. Dr. (TU NN)

Norbert Pohlmann

Professor für Cyber-Sicherheit

Leiter des Instituts für Internet-Sicherheit - if(is)

Vorstandsmitglied des Verbands der Internetwirtschaft - eco

Vorstandsvorsitzender des Bundesverbands IT-Sicherheit - TeleTrusT

if(is)
internet-sicherheit.

Wir empfehlen

- **Cyber-Sicherheit**

Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019
<https://norbert-pohlmann.com/cyber-sicherheit/>



- **7. Sinn im Internet (Cyberschutzraum)**

<https://www.youtube.com/cyberschutzraum>



- **Master Internet-Sicherheit**

<https://it-sicherheit.de/master-studieren/>



Besuchen und abonnieren Sie uns :-)

WWW

<https://www.internet-sicherheit.de>

Facebook

<https://www.facebook.com/Internet.Sicherheit.ifis>

Twitter

https://twitter.com/_ifis

<https://twitter.com/ProfPohlmann>

YouTube

<https://www.youtube.com/user/InternetSicherheitDE/>

Prof. Norbert Pohlmann

<https://norbert-pohlmann.com/>

Quellen Bildmaterial

Eingebettete Piktogramme:

- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
<https://www.it-sicherheit.de/>

- N. Pohlmann, S. Schmidt: „Der Virtuelle IT-Sicherheitsberater – Künstliche Intelligenz (KI) ergänzt statische Anomalien-Erkennung und signaturbasierte Intrusion Detection“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 05/2009
- D. Petersen, N. Pohlmann: "Ideales Internet-Frühwarnsystem", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 02/2011
- M. Fourné, D. Petersen, N. Pohlmann: "Attack-Test and Verification Systems, Steps Towards Verifiable Anomaly Detection". In Proceedings der INFORMATIK 2013 - Informatik angepasst an Mensch, Organisation und Umwelt, Hrsg.: Matthias Horbach, GI, Bonn 2013
- U. Coester, N. Pohlmann: „Verlieren wir schleichend die Kontrolle über unser Handeln? Autonomie hat oberste Priorität“, BI-SPEKTRUM Fachzeitschrift für Business Intelligence und Data Warehousing, 05-2015
- U. Coester, N. Pohlmann: „Ethik und künstliche Intelligenz – Wer macht die Spielregeln für die KI?“, IT & Production – Zeitschrift für erfolgreiche Produktion, TeDo Verlag, 2019
- N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit – Diskussionsgrundlage für den Digitalgipfel 2018“
<https://norbert-pohlmann.com/app/uploads/2018/12/Künstliche-Intelligenz-und-Cybersicherheit-Diskussionsgrundlage-für-den-Digitalgipfel-2018-Prof.-Norbert-Pohlmann.pdf>
- N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit - Unausgegoren aber notwendig“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2019
- U. Coester, N. Pohlmann: „Wie können wir der KI vertrauen? - Mechanismus für gute Ergebnisse“, IT & Production – Zeitschrift für erfolgreiche Produktion, Technik-Dokumentations-Verlag, Ausgabe 2020/21
- D. Adler, N. Demir, N. Pohlmann: „Angriffe auf die Künstliche Intelligenz – Bedrohungen und Schutzmaßnahmen“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 1/2023
- P. Farwick, Pohlmann: „Chancen und Risiken von ChatGPT – Vom angemessenen Umgang mit künstlicher Sprachintelligenz“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 4/2023
- N. Pohlmann: Lehrbuch „Cyber-Sicherheit“, Springer Vieweg Verlag, Wiesbaden 2022
Druckausgabe (ISBN 978-3-658-36242-3) und eBook (ISBN 978-3-658-36243-0).

Weitere Artikel siehe: <https://norbert-pohlmann.com/artikel/>



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Institut für Internet-Sicherheit

→ Vorstellung und Übersicht

Prof. Dr. (TU NN)

Norbert Pohlmann

*Professor für Cyber-Sicherheit und
Leiter des Instituts für Internet-Sicherheit - if(is)*

*Vorstandsvorsitzender des Bundesverbands IT-Sicherheit - TeleTrusT
Vorstandsmitglied des Verbands der Internetwirtschaft - eco*

if(is)
internet-sicherheit.

Berufliche Erfahrungen: Unternehmer im Bereich IT-Sicherheit

- Geschäftsführender Gesellschafter der **KryptoKom GmbH (1988-1999)**
- Vorstandsmitglied der **Utimaco Safeware AG (1999-2003)**

Hauptamtliche Tätigkeiten: seit 2003

- **Informatikprofessor** für Informationssicherheit *und*
- Geschäftsführender **Direktor des Instituts für Internet-Sicherheit – if(is)** an der Westfälische Hochschule

Ehrenämter:

- Vorstandsvorsitzender des **Bundesverbands IT-Sicherheit – TeleTrust**
- Vorstandsmitglied des eco – **Verband der Internetwirtschaft e.V.**
- Vorstandsmitglied **EuroCloud Deutschland_eco e.V.**
- Mitglied des wissenschaftlichen Beirates der **GDD**
- Mitglied im Lenkungskreis Initiative „**IT-Sicherheit in der Wirtschaft**“ des BMWi
- Mitglied der Advisory Group der European Union Agency for Cybersecurity – **ENISA**
- ...

Institut für Internet-Sicherheit

→ Übersicht

- Das Institut für Internet-Sicherheit - if(is) ist eine Fachbereich übergreifende, **wissenschaftliche Einrichtung der Westfälischen Hochschule**, im Fachbereich Informatik
- Gründung: 2005
- Wir haben uns zu dem **führenden Institut für Internet-Sicherheit** entwickelt!
- Seit WS10/11: **Master** „Internet-Sicherheit“
- Ca. 50 Mitarbeiter
- Unser **Ziel** ist es, einen Mehrwert an **Vertrauenswürdigkeit** und **Sicherheit** im Internet herzustellen.



Zahlen des if(is)

→ Übersicht



Forschungsschwerpunkte im

Internet Frühwarnsysteme



(Internet-)Kennzahlen-Sys.



KI + Cyber-Sicherheit



Zahlungssysteme und
Banktransaktionen



Blockchain

Identity Management



IoT Security



Gesundheitswesen

Vertrauenswürdige IT-Systeme



Smart City, -Car, -Traffic

Cloud, Fog, Edge Computing



Mobile Security



Botnetz-Erkennung



Vertrauenswürdigkeit