Sicherheit als staatliche Aufgabe?

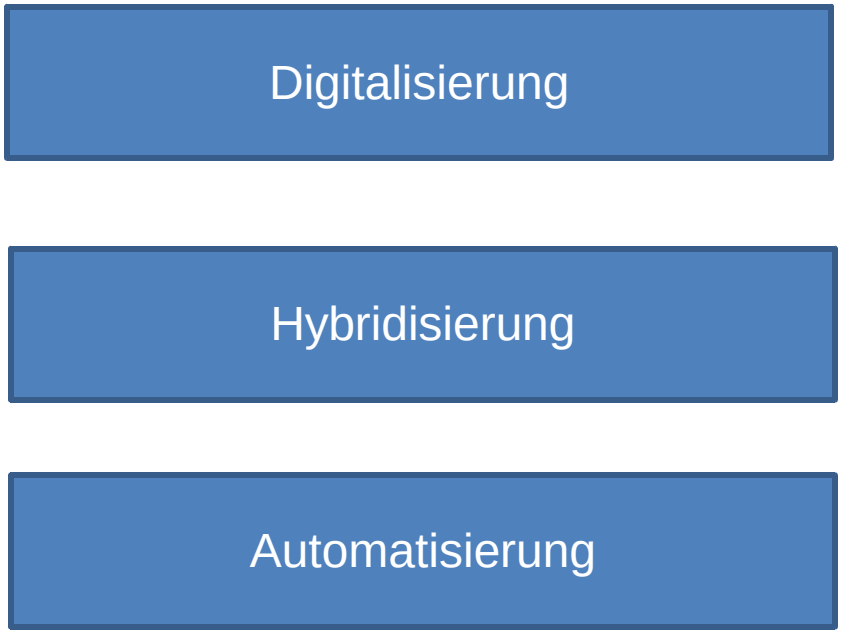
Zum Stand der Bürgerrechte im Cyberraum

Berlin, 20. Juli 2016

- thematische Einordnung
- **(Cyber)Sicherheit & Datenschutz**
- Gefährdungen & ihre Begegnung:
- Dt. Cyber-Sicherheitsstrategie, KRITIS,
- Cyberkriminalität und Cyberpolicing
- **Big Data**
- Bürgerrechte & Cyber-Sicherheit
- Das Internet ist eine gute Sache

Das Internet ist eine gute Sache!

Einordnung



Sicherheit im Cyberraum

Begriffe

Was heißt Sicherheit ?

Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.

Begriffe

Was heißt IT-Sicherheit ?

- Datenschutz
- Datensicherheit (Schutz von Daten vor Verlust, Verfälschung etc.)
- Netzwerksicherheit (Schutz von Netzen)
- Computersicherheit (Schutz vor Ausfall bzw. Schaden)

Begriffe

Was heißt Cybersicherheit ?

Cybersicherheit erweitert das Konzept der IT-Sicherheit auf den Cyberraum. Auch die Schutzbedürfigkeit der Kommunikation, von Anwendungen, von Prozessen oder von verarbeiteten Informationen werden berücksichtigt.*

* Definition des BSI

Schutzziele

Zwei Zielfelder:

- Schutz von Bürgerinnen und Bürgern (i.S.v. Bürgerrechten),

- Vermeidung von Angriffen (Sabotage, Spionage, Missbrauch, Betrug, Diebstahl), Risiken, Schäden

Datenschutz im Cyberraum

Rahmenbedingungen für einen modernen Datenschutz

Selbstbestimmung

privacy

Spezifizierungen sind notwendig!

- Verwendung und Daten und Informationen grundsätzlich erlauben
- Anonymisierungsgebot
- Förderung von Verschlüsselung
- Zweckbindung
- Verknüpfung von Informationen als Verbotsprinzip (Scoring-Verbot)
- Verbesserung des Selbst-Datenschutzes (Ampeln, Geschäftsbed.)
- Sanktionierung bei Datenschutzverletzungen (zivilrechtlich)
- „Recht auf Vergessen“ (auch von Datenspuren)
- Kontoführung
- Stärkung der Datenschutzbehörden (Aufsichtsfunktion)

Das Internet ist eine gute Sache…

...aber die Missbrauchspotenziale steigen!

Gefährdungen

Gefährdungen können durch nicht-technische Lücken Schwachstellen entstehen:

- Cyber-Kriminalität
- physische Sicherheitslöcher
- Arbeitsweisen
- …

… aber auch durch technische Lücken und Schwachstellen

- Netzwerkinfrastruktur
- Betriebssysteme
- Firewalls
- mobile Systeme
- …

Gefährdungen

205 Tage brauchen Experten, um Lücken zu erkennen und zu schließen.

32 Tage beträgt die Reaktionszeit zum Schließen einer Lücke.

69% aller Firmen/Organisationen waren schon betroffen.

100% der Opfer hatten aktuelle Firewall-Einstellungen und Virensignaturen.

3.5 Mio € betragen die durchschnittlichen Kosten zum Schließen einer Lücke

Quelle: Mandiant (2015)

Dt. Cyber-Sicherheitsstrategie

Deutsche Cyber-Sicherheitsstrategie 2011

Ziel der Bundesregierung ist es, einen signifikanten Beitrag für einen sicheren Cyber-Raum zu leisten.

Handlungsfelder

- Schutz kritischer Informationsinfrastrukturen
- Sichere IT-Systeme in Deutschland
- Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
- Nationales Cyber-Abwehrzentrum
- Nationaler Cybersicherheitsrat
- Wirksame Kriminalitätsbekämpfung auch im Cyber-Raum
- Effektives Zusammenwirken für Cyber-Sicherheit international
- Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie
- Personalentwicklung der Bundesbehörden
- Instrumentarium zur Abwehr von Cyber-Angriffen

…**2016 in neuer Fassung (Ressortabstimmung läuft)**

Kritische Infrastrukturen

IT-Sicherheitsgesetz und kritische Infrastrukturen

Nach dem IT-Sicherheitsgesetz sollen Betreiber besonders gefährdeter Infrastrukturen verpflichtet werden, Ihre Netze besser vor Hacker-Angriffen zu schützen. Neben der dann obligatorischen Meldung von IT-Sicherheitsvorfällen werden zudem Mindeststandards für die IT-Sicherheit bei den Betreibern solcher IT-Infrastrukturen branchenweit festgelegt.*

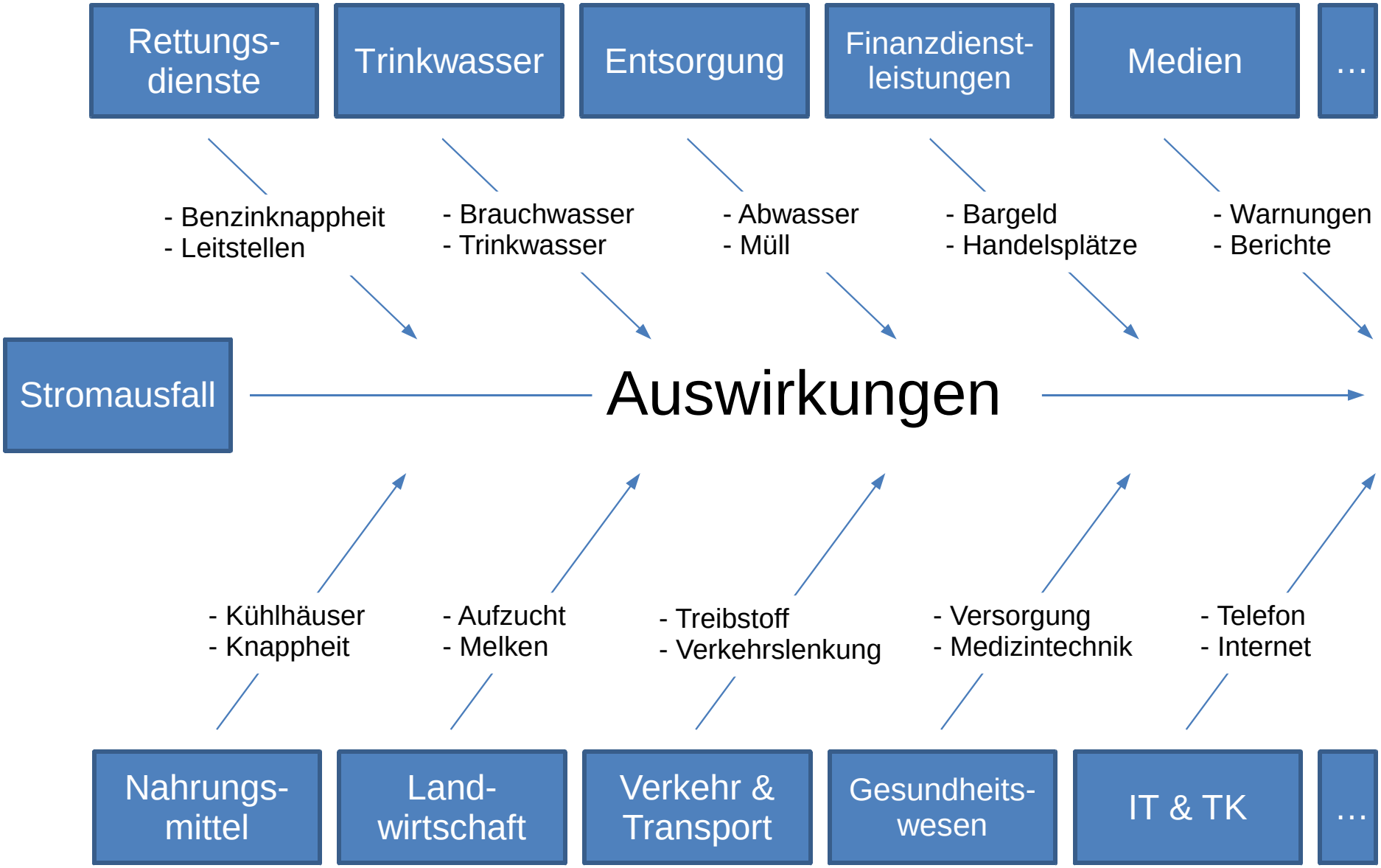
* http://www.secupedia.info/wiki/IT-Sicherheitsgesetz#ixzz434Z7rueL

Energie	Transport & Verkehr	Medien	Wasser
Finanzwesen	Gesundheit	IuK	Ernährung

Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung
- nachhaltig wirkende **Versorgungsengpässe**,
- erhebliche **Störungen der öffentlichen Sicherheit**
- oder andere **dramatische Folgen** eintreten würden.*

***BMI Strategie KRITIS, 2009**

Beispiel Stromausfall



Cyberkriminalität

Definition*

Cyberkriminalität umfasst die Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten.

C. umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden.

* Definition des BKA

Quelle: Köppen 2015

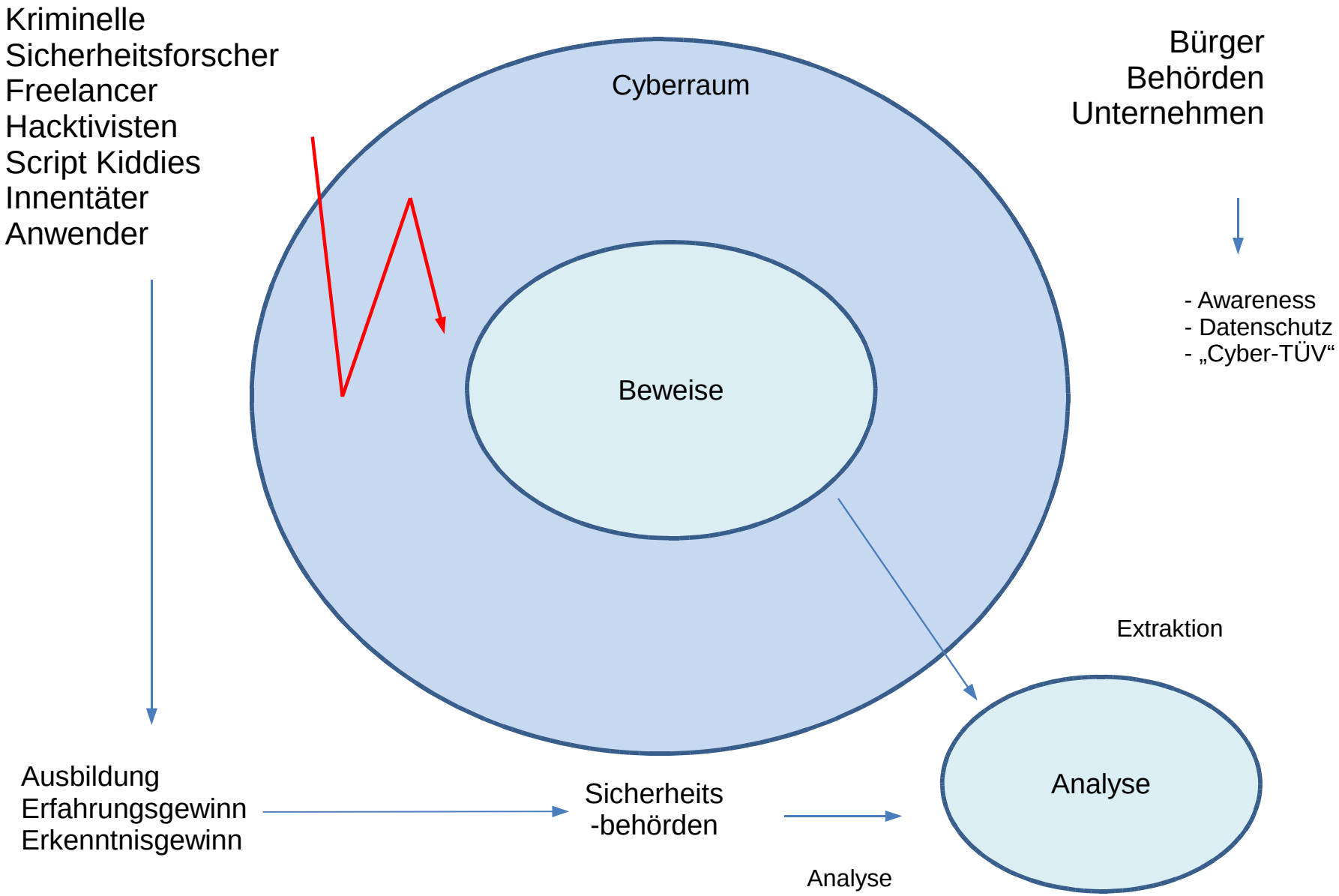
Häufigkeit (1/2)

Häufigkeit (2/2)

Quelle: Kochheim 2015

Akteure

Akteure


Kriminelle
Sicherheitsforscher
Freelancer
Hacktivisten
Script Kiddies
Innentäter
Anwender
Cyberraum
Beweise
Bürger
Behörden
Unternehmen
- Awareness
- Datenschutz
- „Cyber-TÜV“
Extraktion
Analyse
Ausbildung
Erfahrungsgewinn
Erkenntnisgewinn
Sicherheits
-behörden
Analyse

Vorgehensweisen

Vorgehensweisen Cyberkriminalität *

Quellen

Hacking

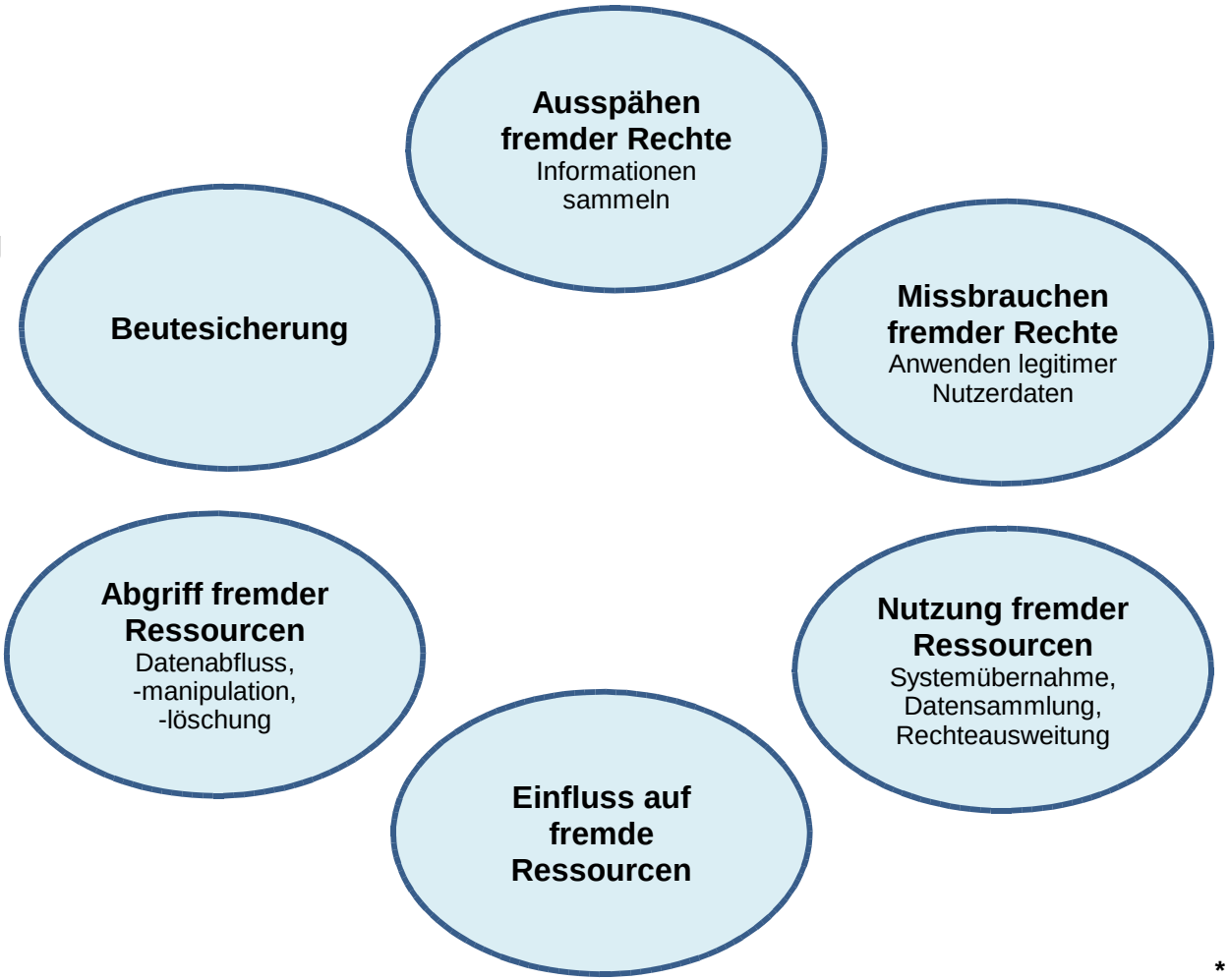
Social Engineering

Malware

technische Unterstützung

strategische Unterstützung

Etappen und Ziele



Logistik

Kommunikation

Steuerung

Know How und Werkzeuge

Infrastruktur und Tarnung

Beuterealisierung

*** nach Kochheim (2015)**

Formen und Methoden der Cyberkriminalität

Phishing	Ausspähen von Kontozugangsdaten und ihr missbräuchlicher Einsatz zugunsten eines Täters
Skimming	Ausspähen der Zahlungskarten und Autorisierungsdaten bei der Nutzung von Geldausgabeautomaten (auch Gebrauch gefälschter Karten)
Malware	Kl. Computerprogramme mit beabsichtigten schädlichen Wirkungen (Viren, Würmer, Trojaner, Keylogger, Spyware)
Identitätsdiebstahl	Missbrauch einzelner, fremder Identitätsmerkmale bis hin zur vollständigen Übernahme fremder Identitäten
Carding	Ausspähen von Kreditkarten- und Kontozugangsdaten, der Handel mit ihnen und ihr Missbrauch bei Geschäften im Warenhandel
Finanzagent	Geldwäscher, der sein Konto zum Empfang von ertrogenden Zahlungen zur Verfügung stellt und weiterleitet (Male Account)

Ausgewählte Ermittlungshandlungen

klassische Ermittlungen:

- personale Beweismittel
  - … Zeugen
  - … fachkundige Zeugen
  - … Sachverständige
- Sachmittelbeweise

verdeckte Ermittlungen:

- Rasterfahndung
- Postbeschlagnahme
- Überwachung Telekommunikation
- Großer Lauschangriff
- Kleiner Lauschangriff
- Bildaufnahmen
- Verdeckte Ermittler
- IMSI-Catcher
- polizeiliche Beobachtung
- Observation
- Verkehrsdatenabfragen vom Provider
  - … Endgerät
  - … Standortdaten
  - … wegen TK-Straftaten
  - … nicht vom Provider
- Schleppnetzfahndung
- Informant
- Vertrauensperson
- nicht offen ermittelnder Beamter

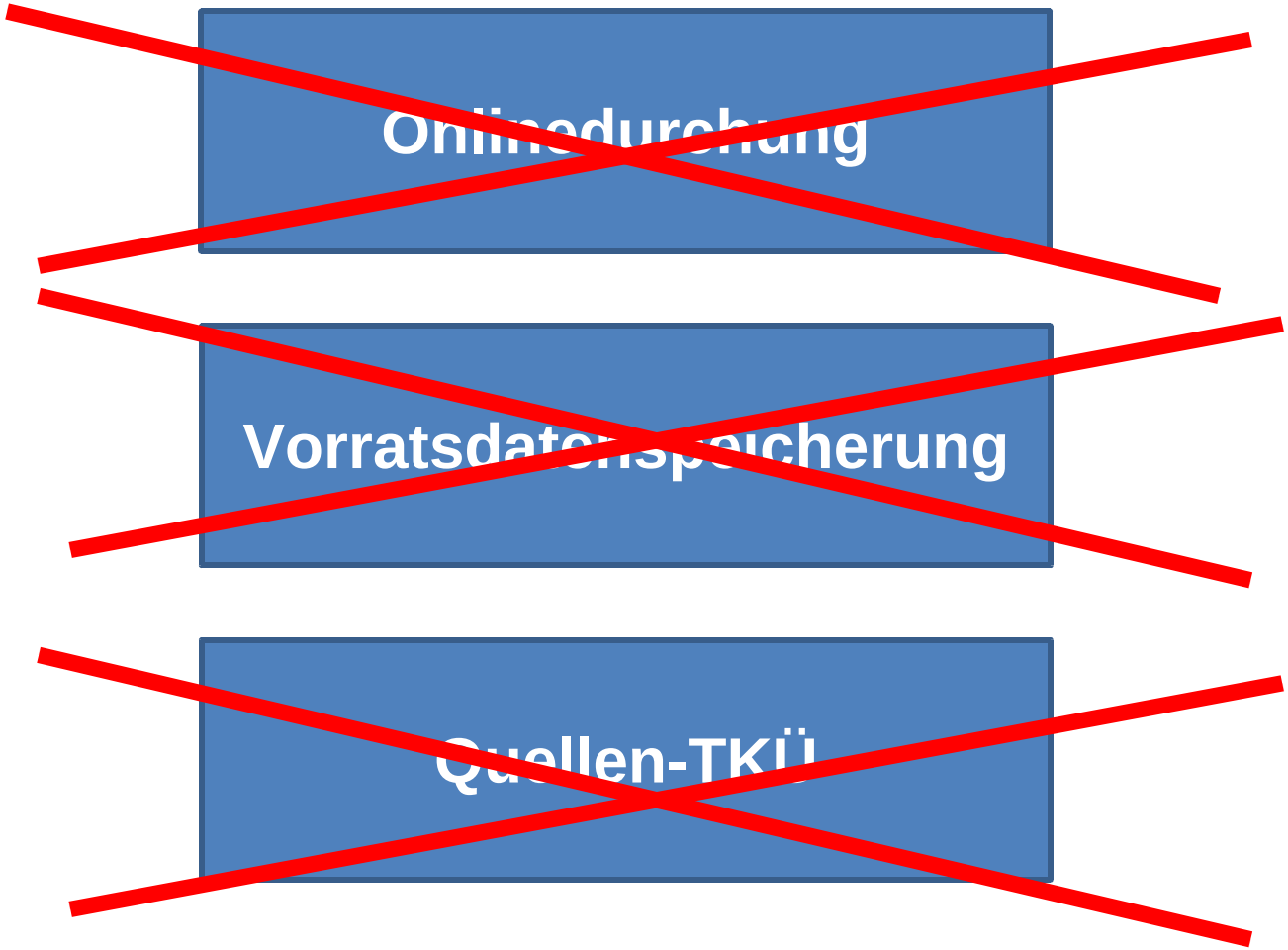
weitere Ermittlungshandlungen

Onlinedurchung

Vorratsdatenspeicherung

Quellen-TKÜ

weitere Ermittlungshandlungen



neue Ermittlungshandlungen

(mit möglichen negativen Auswirkungen auf Bürgerrechte)

neue Ermittlungshandlungen

Predictive Policing

„vorausschauende Polizeiarbeit“:

- Prognose von Zeiten und Örtlichkeiten mit erhöhtem Kriminalitätsrisiko
- Identifizierung von Personen, die zukünftig Straftaten begehen könnten
- Erstellung von Profilen, die wahrscheinliche Täter mit vergangenen Taten abgleichen
- Prognose von Gruppen, die eine erhöhtes Viktimisierungsrisiko haben

Ziel: Einsatzkräfte zu einem Zeitpunkt an potenziellen Tatorten haben, an denen mutmaßlich Straftaten stattfinden.

Methode:

Big Data bezeichnet *strukturierte und unstrukturierte* Datenmengen, die zu groß oder zu komplex sind oder sich zu schnell ändern, um sie mit manuellen und klassischen Methoden zu speichern und auszuwerten.
Unter Big Data werden auch **Verfahren,** Algorithmen oder Technologien verstanden, die geeignet sind, Big Data-Datenbestände zu durchsuchen, zu analysieren und auszuwerten.

Kritische Würdigung Cyberpolicing

Big Data-basierte (Personalisierungs-)Verfahren für die Täter- oder Opferidentifikation erhöhen das Risiko von logischen bzw. statistischen Fehlschlüssen:

Bsp.: Die Datenanalyse folgt dem einfachen Prinzip, dass sich Dinge wiederholen: „Wenn Y nach X auftritt, wird Y immer wieder nach X auftreten“ – ein einfacher Kausalzusammenhang existiert allerdings oft und insbesondere bei sozialen Phänomenen meist nicht.

Big Data-basierte Personalisierungsverfahren erhöhen das Risiko der Vulnerabilität von Individuen und missachten vorsätzlich das Recht auf Privacy und informationelle Selbstbestimmung:

Bsp.: Aus einem Text-Mining von Beiträgen sozialer Netzwerke, Bewegungsdaten des Telefons, Aufenthalt in bestimmten Raum-Zeit-Punkten, amtlichen Daten zu Herkunft, der elektronischen Auswertung von Gesundheitsdaten etc. wird ein statistischer Scoring-Wert ermittelt, der die Wahrscheinlichkeit möglichen strafbaren Handelns errechnet.

Big Data-basierte Personalisierungsverfahren können zu zunehmender Diskriminierung führen:

Bsp.: „Wenn Versicherungsprämien von der Ernährung abhängig gemacht werden, dann zahlen Juden, Moslems, Christen und Frauen unterschiedliche Tarife“

neue Behörden

(mit möglichen negativen Auswirkungen auf Bürgerrechte)

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITIS)

- geplante neue Behörde zur Entschlüsselung von kryptierter Kommunikation.
- ZITIS soll keine operativen Befugnisse erhalten
- ZITIS soll ausgewählten Sicherheitsbehörden beratend bzw. unterstützend zur Verfügung stehen.
- Gründung per Einrichtungserlass
- bis 2022 400 Mitarbeiterinnen und Mitarbeiter

Quelle: http://www.sueddeutsche.de/digital/sicherheitspolitik-neue-behoerde-soll-fuer-regierung-verschluesselte-kommunikation-knacken-1.3047884-2

Und wie steht es
um die Bürgerrechte?

Das Internet ist eine gute Sache!

Allerdings gilt im Cyberraum auch:

Das Streben nach Sicherheit un Informationen ist immer mehrseitig und muss sich an Grund- und Bürgerrechten orientieren.

Jedem Bürger muss ein selbstbestimmter Umgang mit sicherheitstechnischen Funktionen ermöglicht werden.

Eine Aushandlung von Sicherheitsanforderungen und Schutzanforderungen muss zwischen allen Beteiligten ermöglicht sein.

(Konzept mehrseitiger Sicherheit)

Big Data & Digitalisierung ermöglichen viel,

aber:

Das Internet ist offen, frei und für jeden Anwender
(natürliche und juristische Personen!) nutzbar zu halten.

Das Internet muss widerstandsfähig gegenüber Störungen sein.

Der Manipulation von Informationen ist zu begegnen.

Der Beeinträchtigung freier Meinungsäußerung ist entgegenzuwirken.

Es muss rechtsstaatlich zugehen!

Regelungsbedarf:

Umgang mit Schwächen in Software.

Gewährleistung von Behörden und Verwaltung,
dass an der Einhaltung von Gesetzen zur
Integrität, Vertraulichkeit und Verfügbarkeit
von Informationen gelegen ist.

bessere parlamentarische Kontrolle über
die Analyseverfahren, Such- und Empfehlungsalgorhytmen,
die Polizei, Dienste, Behörden und Verwaltung einsetzen.
(rechtsstaatliche Verfahren)

Für Big Data existiert ein Ehrenkodex

Man darf durch die Arbeit mit Daten & Informationen und den Einsichten, die sie gewähren, **Dritten keinen Schaden zuführen**.

Man darf Daten & Informationen nur so verwenden, dass die Ergebnisse **die friedliche Koexistenz des Menschen unterstützen**.

Verwende Daten nur so, um **Menschen in Not zu helfen**.

Verwende Daten, um die **Natur zu** schützen und die Umweltverschmutzung zu reduzieren.

Verwenden Daten, um Diskriminierung und Intoleranz zu **beseitigen** und ein faires Zusammenleben zu ermöglichen.

Das Internet ist eine gute Sache..

..aber wen interessiert das?

Was

ENDE