DiDaT Feinplanung für den Vulnerabilitätsraum 07

Cybercrime / Cyber Security

Eike Albrecht (BTU), Andriy Panchenko (BTU), Dirk Labudde (HS Mittweida), Dirk Marx (BTU), Dr. Heralt Hug (Leipzig/Cottbus), , Larissa Kätker (BTU), Marcel Mönch (BTU); Practice: Haiying Wu (Huawei), Dirk Nagel (Vodafone), Veselko Hagen (BTU), Bernhard Brocher (StA Cottbus), Hinrich Völcker (Deutsch Bank)

1. Gegenstand, Ziele und Leitfrage

Das Forschungsprojekt DiDaT (Laufzeit 11/2019 bis 10/2021) beinhaltet sieben Arbeitsgruppen als dementsprechende Vulnerabilitätsräume (VRs). Diese Teilbereiche des Gesamtprojektes spiegeln gesellschaftliche und funktionale Forschungsschwerpunkte wider. Dabei wird ein den VR bestimmender thematischer Rahmen und theoretische Struktur so aufgestellt, dass mit Hilfe einer Leitfrage transdisziplinäre Forschung möglich wird.

Ein solcher Forschungsprozess kennzeichnet sich durch die Erstellung der Materialien Grob- und Feinplan und dem Weißbuch. Im Rahmen der hier vorliegenden Feinplanung werden die Arbeitsschritte *Vulnerabilitäten*, *Unseens* und deren *Mechanismen* sowie *robuste soziale Orientierungen* als Ergebnisse angestrebt. Vertiefungsforschung und eine Td-Lab-Anwendung ermöglichen einen besseren Überblick und tieferen Einblick zu unerwünschten Nebenfolgen, den Rebounds und verbessern damit das Erkennen von Unseens.

Die vorliegende Ausarbeitung ist daher die Grundlage für das Erkennen spezieller Herausforderungen im Bereich von Cybercrime und Cyber Security. Die Nutzung digitaler Systeme im *Cyberspace* führt zu Straftaten, dadurch, dass dieser Raum es überhaupt erst ermöglicht solche Taten zu begehen und aufgrund von Entpersonalisierung möglicherweis dazu einlädt. Dies stellt eine zunehmende Herausforderung für die öffentliche Sicherheit und Ordnung dar (Falk 2017; Lentner 2019). Der Cyberspace (das Internet) muss heute schon alleine aufgrund seiner immensen Bedeutung für Wirtschaf und Gesellschaft geschützt werden. Solche Schutzmaßnahmen können jedoch von Kriminellen missbraucht werden, wie es z.B. bei Verschlüsselungssystemen so genutzt wird, um den rechtmäßigen Benutzer auszuschließen. Dolose (arglistig, trügerisch) Handlungen (nach Siepermann 2017) und alle anderen unrechtmäßigen Handlungen im *Cyberspace* erfordern im Rahmen der Zuordnung *Cybercrime und Cyber Security*[1] spe-

[1] *Cybercrime* umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden (BKA, 2018). *Cyber Security* befasst sich mit 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 (BSI, 2019). *Cybersafety* bedeutet Internetsicherheit und

zielle Antworten auf Fragen, die wegen der Dynamik im Internet teils noch gar nicht gestellt sind (Goeken u. Fröhlich 2018). Insofern ist Prävention eine äußerst ernst zu nehmende Aufgabe, die nur in Verbünden gute Erfolge erbringen kann. Dabei spielen Kooperationen zwischen Akteure, die unsichere und auffällige Daten im Rahmen ihres Geschäftsmodelles nutzen, die zentrale Rolle. Infrastruktur und Datenmanagement sowie die Geschäftsabwicklungen der Banken sind dabei weitere konkrete Beispiel, die im Rahmen dieses VRs bearbeitet werden. Aber auch Repression mit den Mitteln des Strafrechts und der Strafverfolgung sind notwendig.

Hervorzuheben ist hier ferner das Phänomen *«Darknet»*, welches sich auf der einen Seite als „zunehmende Bedrohung" darstellt, weil die klassische Kriminalität, wie z. B. Waffen- und Drogenhandel, partiell in den Cyberspace als virtuellen und somit versteckten Raum verlagert wird. Auf der anderen Seite bietet das Darknet auch Schutz vor staatlicher Repression, beispielsweise in nicht so demokratischen Systemen.

Ganz generell ist hervorzuheben, dass neue Anforderungen an die Datensicherheit und hier gerade auch durch die Einführung von externen Cloud-Computing und einen damit erhöhten Datentransfer, gestellt werden. Dies gilt gerade vor dem Hintergrund der zunehmend globalisiert erfolgenden Datenspeicherung, ohne dass ein bestimmter Heimatstaat mit seinen Gesetzen und Institutionen noch zuständig wäre.

Der Einsatz neuer Technologien bedingt daher rechtlicher Anpassungen auf nationaler und auch internationaler[2] Ebene. Neue Gesetze – politische Situationen –, angepasste Organisationsstrukturen und geänderte Verhaltensweisen, verbunden mit dem Ziel, die *Resilienz* der Gesellschaft und des Staates gegen die nachteiligen Auswirkungen der Digitalisierung zu erhöhen. Dabei ist es erforderlich, «*socially robust strategies*»[3] im Rahmen dieses Teilprojektes durch die Identifizierung von Vulnerabilitäten zu entwickeln. Dieser dynamische Prozess hat Auswirkungen in den folgenden **Hauptbereichen** und wirkt regulatorisch oder bestrafend. Vorschriften zur Vorratsdatenspeicherung unter Einbeziehung Dritter und einer darauf folgend weitergehenden Analyse, wie es z.B. von **Banken** erwartete wird, die im Rahmen einer (Daten-)Massendatenanalyse Ihre Kundendaten so auswerten, das z.B. eine Verfolgung und Unterbindung von Geldwäsche auch gelingen kann.

Eine Neuorganisation der Strafverfolgungsbehörden, die aufgrund der digitalen Herausforderungen sowohl vor rechtlichen als auch forensischen neuen Herausforderungen stehen.[4] Wie aber kann sich Computer- und Systemnutzung durch *Digitalität* von Manipulationen, Korruption bis hin zur Sabotage kritischer Infrastrukturen und anderer krimineller Aktivitäten im Cyberspace abgrenzen?

Digitale **Infrastrukturanbieter**, die den Ausbau der Hardware sicherstellen und die digitalen Serviceanbieter, die **Provider**, die die Software

---

wird im Rahmen dieser Arbeit unter Cyber Security subsummiert. Denn Cybersafety scheint begrifflich eine private Internetnutzung anzusprechen und nicht eine professionelle, so wie es Cyber Security eher zugeordnet wird. Diese Begriffsabgrenzung ist unscharf und führt dazu, dass Cybersafety als Begriff eines alltäglichen Sprachgebrauchs verwandt wird und somit inhaltlich mit Cyber Security gleichgesetzt werden kann und aus Gründen der Klarheit auch muss.

[2] Cybercrime Convention Budapest 2001 (Übereinkommen über Computerkriminalität) – erste internationale Vereinbarung über mittels Internet oder sonstiger Computer begangener Straftaten: https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185 (abgerufen am 16.11.2019)

[3] DiDaT Newsletter 01, Februar 2019, www.iass-potsdam.de (abgerufen am 05.05.2019)

[4] https://www.computerweekly.com/de/definition/Computerkriminalitaet-Cybercrime

und Datenflusstechnik zur Verfügung stellen, bilden zwei weitere Hauptbereiche ab.

Es geht somit im Weiteren unter Einbeziehung dieser vier Hauptbereiche darum, dass unbeabsichtigte Nebenwirkungen (sog. *Unseens*; abgeleitet von: unintended side effects[2]) als *Nebeneffekte* zu erkennen und zu akzeptieren. Dazu gehört eine bewusste, gesellschaftlich ausgehandelte Akzeptanz von nachteiligen Auswirkungen, z.B., wenn die positiven Folgen überwiegen, oder die nachteiligen nicht sehr schwerwiegend sind. Technologische Entwicklungsgeschwindigkeiten, die zu temporären und lukrativen Markterfolgen führen, werden durch den Markt reguliert. Anreize dazu, hohe Geschäftsrisiken einzugehen, erfahren somit einen weiteren Check.

Eine solch *profitable* Ambivalenz erfordert die Abwägung zwischen verschiedenen Rechtsgütern wie Freiheit vs. Sicherheit und Gesellschaftskonzepten, Selbstverantwortlichkeit vs. staatlich-gesellschaftlich organisiertem Schutz sowie einer Gewichtung/Regulierung des gesellschaftlichen- und unternehmerischen Verhaltens. Eine Basis zur Aushandlung von Akzeptanz, vor allem vor dem Hintergrund nicht vorhersehbarer und nicht gewollter Nebeneffekte, scheint es transparent so noch nicht zu geben. Es geht eher um Zufälligkeit, wobei die staatliche Regulierung der Privatwirtschaft regelmäßig hinterherhinkt, wie das regelmäßig bei neuen Technologien zu beobachten ist und Motive für den Erfolg, der im Internet im Verborgenen stattfindet, manipulative Freiheiten noch selbstverständlicher werden lässt (Scholz 2019).

Cybercrime-Angriffe auf digitale Infrastrukturen und Daten sind regelmäßig strafbar, aber schwer nachweisbar. Denn *digitale Spuren* können flüchtig sein und werden nicht in allen Fällen mit dem für den klassischen Strafrechtsbereich geltenden Beweisanforderungen (siehe hierzu Miebach 2016) belegbar sein. Ein Lösungsansatz ist, hier Kompetenz und Technologie bei speziell für Cybercrime zuständiger Ermittlungsarbeit und Staatsanwaltschaften zu schaffen. Beispielhaft seien hier die Schwerpunktstaatsanwaltschaften für Cybercrime in Brandenburg (StA Cottbus), wobei es aber auch ganz andere Modelle gibt, beispielsweise im Vorarlberg, wo die organisatorische Antwort auf diese neuen Herausforderungen ein anderes Modell präferiert. Gegenwärtig stellen sich Strafverfolgungsbehörden dem sich dynamisch ändernden Kriminalitätsphänomen „Cybercrime“ durch unterschiedliche organisatorische Antworten in den verschiedenen Bundesländern.

Ausgehend von einer Analyse der Vulnerabilitäten werden positive und negative Options- und Handlungsräume betrachtet, die soziale- und technische Innovationen (transdisziplinärer Prozess) für einen verantwortungsvollen Umgang mit *digitalen Daten* zu *Cybercrime* und *Cyber Security ermöglichen.*

Die **Leitfrage** dieses VRs lautet daher: *Ist der derzeitige Rechts- und Organisationsrahmen geeignet, in verhältnismäßiger Weise die Gesellschaft auf die gegenwärtigen und absehbaren zukünftigen Herausforderungen der Digitalisierung vorzubereiten?*

Definitionsraum

1. *«Cybercrime»* umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime

im engeren Sinne)[5] oder die mittels dieser Informationstechnik begangen werden (Computerkriminalität). Aktuell verbreitete Erscheinungsformen von Cybercrime sind gekennzeichnet durch die Infektion und Manipulation von Computersystemen mit Schadsoftware, z.B. um persönliche Daten und Zugangsberechtigungen des Nutzers abzugreifen und missbräuchlich nutzen zu können (Identitätsdiebstahl), darauf befindliche Daten/Dateien des Nutzers mittels sog. Ransomware zu verschlüsseln, um "Lösegeld" zu erpressen, sie "fernsteuern" zu können, in sog. Botnetzen zusammenzuschalten und für weitere kriminelle Handlungen einzusetzen.[6]

Zusammengefasst lassen sich die o.g. Definitionsräume zu Cybercrime wie folgt ausformulieren: «Cybercrime im **engeren Sinne** sind Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder Daten richten» und «Cybercrime im **weiteren Sinne** sind Straftaten, die mittels Informationstechnik begangen werden»[7]. Die letztgenannten Delikte sollen im Rahmen der vorliegenden Analyse und Bearbeitung allenfalls sekundär behandelt werden, geht es doch bei ihnen um althergebrachte Straftaten, die lediglich unter Nutzung neuer technischer Möglichkeiten begangen werden. Somit sind unter den Begriff Cybercrime viele Delikte subsumierbar. Klassische Straftaten nach dem Strafgesetzbuch unterscheiden sich von solchen Delikten jedoch (teils gravierend) dahingehend, als dass durch die Begehung von Cybercrime-Delikten im globalen Netz (kaum wahrnehmbare) Landesgrenzen überwunden werden und sich dadurch anders gelagerte Problemstellungen im Zusammenhang mit der Strafverfolgung des Täters ergeben können.

Tabelle 1: Grundlage für die Verfolgung von Cybercrime im engeren Sinne nach dem Strafgesetzbuch[8]

Straftatbestände	Inhalt (Kurzbeschreibung, Quelle Hagen)
§ 202a StGB Ausspähen von Daten	Das unbefugte Verschaffen eines Zugangs zu Daten, die nicht für den Täter bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung.
§ 202b StGB Abfangen von Daten	Das unbefugte Verschaffen von Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Anwendung von technischen Mitteln.
§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten	Das Vorbereiten einer o. g. Straftat durch das Herstellen, Verschaffen oder Zugänglichmachen von Passwörtern, Sicherheitscodes oder Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist.
§ 202d StGB Datenhehlerei	Das sich oder einem anderen Verschaffen, Überlassen, Verbreiten oder Zugänglichmachen von nicht allgemein zugänglichen und durch einen anderen aus einer rechtswidrigen Tat erlangten Daten mit der Absicht, sich oder einen Dritten zu bereichern oder einen anderen zu schädigten.
§ 263a StGB Computerbetrug	Das Schädigen des Vermögens eines Andern durch Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf. Des Weiteren das

[5] „Cybercrime im engeren Sinne bezieht sich gemäß dem Deutschen BKA auf spezielle Phänomene und Ausprägungen dieser Kriminalitätsform, bei denen Elemente der elektronischen Datenverarbeitung (EDV) wesentlich für die Tatausführung sind.“: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2011.pdf;jsessionid=A914451065D1D0C8E5F1ED18FDFDEA9A.live0612?__blob=publicationFile&v=3

[6] , o. J.

[7] Differenzierung des BKA im Bundeslagebild 2016 zur Thematik „Cybercrime im engeren und im weiteren Sinne“

[8] BKA, Cybercrime – Handlungsempfehlungen für die Wirtschaft

	Vorbereiten einer solchen Tat durch Herstellung, Verschaffung, Veräußerung, Verwahrung oder Überlassung eines Computerprogramms, dessen Zweck die Begehung einer solchen Tat ist.
§ 269 StGB Fälschung beweiserheblicher Daten	Das Speichern oder Verändern beweiserheblicher Daten zur Täuschung im Rechtsverkehr, sodass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder das Gebrauchen solcher Daten.
§ 303a StGB Datenveränderung	Das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten.
§ 303b StGB **Computersabotage**	Das erhebliche Stören einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch 3. Begehung einer Datenveränderung (§ 303a), 3. Eingabe oder Übermittlung von Daten in der Absicht, einem anderen einen Nachteil zuzufügen, 3. Zerstörung, Beschädigung, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers.

2. *«Cyber-Raum»* Sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik mit darauf basierender Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen.[9]
3. *«DarkNet»*: Anonyme Verbindungen, die nicht öffentlich zugänglich und somit z.B. nicht von normalen Suchmaschinen auffindbar sind. Der Begriff wird häufig als Synonym für das Tor-Netzwerk verwendet[10], das Verbindungsdaten anonymisiert[11]. Der virtuelle Raum wird häufig für den Handel mit illegalen Waren (z. B. Falschgeld, Betäubungsmittel, Waffen, usw.) genutzt.[12]

Ziel

Die Datenerhebung und -analyse (Datenzugriff, Datenauswertung) auf den Ebenen von Anwendern, Providern oder der Strafverfolgung (am Beispiel einer „Schwerpunktstaatsanwaltschaft“, konkret in Cottbus) machen Herausforderungen in dreierlei Bereichen der Verwendung digitaler Daten und deren Auswertungen soweit kenntlich, dass folgende Forderungen Arbeitsvoraussetzungen für diesen VR sind. **(Arbeitsvoraussetzung 1)** *Die* Qualität der Ausbildung der „spezialisierten“ Staatsanwälte und Cybercrime-Ermittler (z. B. BKA, LKAs) in digitaler Forensik muss schnell erhöht und dynamisiert werden, zum einen um tatsächlich krimineller Aktivität mindestens auf Augenhöhe begegnen zur können, aber auch, um das Risiko der Nutzung elektronischer Systeme zu reduzieren.

(Arbeitsvoraussetzung 2) Ebenso muss das Spektrum aus Wissen zu Veränderungen der Tatorte, beispielsweise in Bezug auf hinterlassene Spuren und der Tathergänge im Cyberspace musterhaft und schnell vergleichbar dokumentiert werden. **(Arbeitsvoraussetzung 3)** Bewegungen im DarkNet müssen kurzer Zeit forensisch sicher analysiert werden können. **(Arbeitsvoraussetzung 4)** Um das zu ermöglichen, müssen Aufgaben zur Cybercrimeabwehr zwischen systemrelevanten Unternehmen so verteilt werden, dass Wissen, Erstzugang, Manpower und Legitimation Eingang in die Forschung finden. Forschungsvertiefende Ansätze dieses VR`s zur Tatüberführung aufgrund digitaler forensisch begutachteter Spuren, sichern belastbare Beweise für die Verwendung einer Gesamtanalyse. Der Einsatz von systemrelevante Unternehmen, etwas von Internet- und Mobil-

[9] Bundesamt für Sicherheit in der Informationstechnik, o. J.
[10] Vgl. *Golem Media GmbH*, o. J.
[11] Vgl. *Wikimedia Foundation Inc.*, o. J.
[12] Vgl. *Bundeskriminalamt*, 2018, S. 25.

funkprovidern, aber auch Banken und Versicherungen bei der Unterstützung staatlicher Ermittlungs-, aber auch für präventiver Zwecke, der derzeit keiner erkennbaren Systematik folgt, müsste auf der Grundlage eines gesellschaftlichen Aushandlungsprozesses zumindest öffentlich diskutiert werden.

Die bisherige Interpretation aller digitaler Spuren führt zu einer Tathergangseinschätzung durch die Staatsanwaltschaft, die nur mit hohem Aufwand oder mit zu geringem Erfolg hergestellt werden kann.

In verschiedenen Lagebildern, Studien und Veröffentlichungen wird auf Folgen aus Cybercrime-Delikten hingewiesen. DiDaT soll die Plattform bieten, um zu untersuchen, welche nicht intendierten Nebeneffekte mit solchen Delikten einhergehen.

Zentral ist im VR07 eine Analyse des «Kampfes» gegen Cybercrime unter besonderer Berücksichtigung der Verfälschung und missbräuchlichen Nutzung von *digitalen Daten*, der Manipulationen und der missbräuchlichen Nutzungen im Zusammenspiel der hierbei durch das System notwendig verknüpften Teilnehmer, wie sie in der Stakeholder-X-Tabelle genannt werden.

Im Rahmen der **Feinplanung** wird als erster Teilschritt die organisationsrechtliche Frage der Errichtung spezialisierter Schwerpunktbehörden am Beispiel der Schwerpunktstaatsanwaltschaft für Internetkriminalität im Land Brandenburg (StA Cottbus) der ganz anders organisierten Staatsanwaltschaft im Bundesland Vorarlberg analysiert und einer Beantwortung zugeführt.

Dabei sind die folgenden analytischen Schwerpunkte zu untersuchen:

(Arbeitsvoraussetzung 5) Neuordnung von Organisationsstrukturen innerhalb der Staatsanwaltschaft und ihrer Instrumentarien zur Strafverfolgung in Kooperation auch mit anderen behördlichen Akteuren.

(Arbeitsvoraussetzung 6) Die Analyse und kritische Beurteilung geltenden Rechtes sowie Neubeurteilung des geltenden Rechts als Voraussetzung für die Strafverfolgung in Deutschland und der EU.

(Arbeitsvoraussetzung 7) Ausbildung zur Anwendung und Durchsetzung des Rechts auf den unterschiedlichen Ebenen der Staatsanwaltschaft und deren Organisationsstrukturen «*Regulation*» und darauf basierend den *Gegenstand* als Anwendung so erkennen zu können, dass Handlungsempfehlungen als Arbeitsvorgaben zur Lokalisierung und Verfolgung von Cybercrime möglich werden. Durch Überführung von z.B. Handlungsempfehlungen zur *«Cyber Security»* wird eine Prävention insoweit möglich, dass zentrale Wirtschafts- und Finanzakteure, wie die Stakeholder Deutsche Bank, Vodafone und Huawei eine relevante Aufgabe bei der Abwehr von Cybercrime zugewiesen bekommen. Darüber hinaus tragen sie im Rahmen der System relevanten Kooperation (oder auch des Zwanges mit der Staatsanwaltschaft) dazu bei, durch gegenseitiges Feedback und fortwährendes Lernen ein *Handlungsspektrum* zu entwickeln in dem gemeinsame Anwendungen genutzt werden können. Zudem wird es den Unternehmungen ermöglicht, vorhandene und auch nur mögliche Vulnerabilitäten dabei selber zu erkennen, sodass man sich in die Lage versetzt sieht, konkrete Optionen zur Verbesserung des eigenen Geschäftsbereichs anzuwenden.[13] Lt. einem Bericht von Risk Based Security,

[13] „Das BSI publiziert in unregelmäßigen Abständen verschiedene Dokumente mit Hinweisen zu Themen der Cyber-Sicherheit. Dabei handelt es sich beispielsweise um Konfigurationsempfehlungen für Software-Produkte, Analysen von häufig verwendeten Angriffsmustern oder Hilfsmittel zur Detektion von Angriffen auf die eigene Organisation.“ https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/empfehlungen_node.html;jsessionid=C6EF59FA3225F81A6BD9C50259090FF2.1_cid341 (abgerufen am 23.10.2019)

der sich mit Vulnerabilitäten aus dem ersten Halbjahr 2019 befasst, wurden 34 % der bekannten Vulnerabilitäten bis zum 23.08.2019 nicht behoben.[14] Cyber Security und Cybercrime stehen in gegenseitiger Wechselwirkung, da Cyber Security sich grundsätzlich und regelmäßig im Vorfeld mit der Thematik «Unseen» befasst. Cyber Security kann somit Grundlage für die Strafbarkeit von Delikten im Cyberspace sein und kann darüber hinaus Hilfsmittel zur Verfolgung von Cybercrime-Delikten bereitstelle.

Box 1: Grundsaterörterung zur Datenverwendung

1. Grundsätzliche Fragestellungen – Einstellung zum Cybercrime
   - Warum wird Cybercrime akzeptiert?
   - Gelernte «evolutionäre» Hilflosigkeit? (Bedeutung: Nichts oder sehr wenig über das Problem oder die Problemlösung wissen?)
   - Die Mehrheit ist davon überzeugt, dass „Cyberkriminelle“ nicht der Strafverfolgung zugeführt werden bzw. werden können
   - Cyberkriminelle sind gesichtslos, anonym, da diese oftmals aus anderen Ländern kommen bzw. von dort aus operieren
2. Recht – Rechtsgrundlagen (National und EU) – fehlende Rechtsgrundlagen, Beweismittel
   - Aktuelles Recht (National und EU)
   - Nationale Priorität in Bezug auf Cybercrime?!
   - Strafbarkeit einzelner Delikte
   - (Straf-) Gesetze beinhalten einen Schutzzweck. Dies können die menschliche Gesundheit, das Vermögen, aber auch die Sicherheit digitaler Infrastrukturen und Systeme sein. Wird dies auf den „Cyberspace“ übertragen, dann spräche man von den Computern/Servern/IoT (Internet of Things), die verletzlich sind oder sein könnten (also geschützte Rechtsgüter sein können?).
   - Großes Problem:
     - Verlust von Beweismaterial im Cyberspace – meist nur temporär verfügbar (auch Cloud)
   - Wo ist der Tatort? Ist das Delikt dort (geografischer Tatort) auch mit Strafe geahndet – subsidiäre Strafverfolgung (Erhebung des Kriteriums des deliktischen Schwerpunkts)?
   - Mangelndes Unrechtsbewusstsein
   - Cybercrime – konventionelle Straftaten:
     - Wirtschaftskriminalität
     - Waffen-, Drogen- und Menschenhandel
     - Im Internet organisierter politischer Extremismus
     - Das Verbreiten illegaler Inhalte im Netz
   - Haftungsdilemma:
     - Apple Malware
     - Provider

[14] Halbjahresbericht: https://www.riskbasedsecurity.com

2. Welche nicht intendierten, unbeabsichtigten Nebenfolgen sind von Interesse und warum?

Um den mit dieser Überschrift formulierten Nebenfolgen auf den Ebenen von Systematik und der Inhalte näherzukommen, hilft es, die Grundsätze der Box 1 zu diskutieren. Dabei werden unterschiedliche Bedürfnisse der Datenverwendung in den Fokus genommen.
Die nachfolgende Tabelle 2 zeigt die Vulnerabilitäten aus der Entwicklung einer "Wenn/Dann-Abwägung".

Tabelle 2: Vulnerabilitäten der ersten Generation, 2019

Vulnerabilitäten (WENN)	Prozess "transformative Tiefe"	Zuschreibungen (DANN)
Präventive u. repressive Maßnahmen **Verständnis, fehlende Awareness, Grenzen der Sicherheitslösungen (fehlende Updates und Anpassungen an neuste Entwicklungen)**	*Resilient* *Suffizient* *Effizient*	handeln **Präventive fortlaufende und repressive Maßnahmen**
System-Kooperationen **Leichte Verfügbarkeit (KRITIS) heute nicht abgeschottet**	*Resilient* *Suffizient* *Effizient*	binden **System-Kooperationen**
Änderungsgeschwindigkeit **Marktteilnahme (Dienstleistung., Produkte)**	*Resilient* *Suffizient* *Effizient*	verstehen **Sicherheit zweitrangig**
Verlagerung als Entpersönlichung **Zensur, Nudging, überfürsorglich. Upload-Filter (wird gar nicht hochgeladen obwohl zugestimmt), automatisierte Entscheidungen**	*Resilient* *Suffizient* *Effizient*	entrechten **Widersprechen, ignorieren, bekommen das gar nicht mit! (Entpersönlichung), Schleichender paternalistischer Staat**
Ein (An-)griffe von außen – Cybersecurity **IT- Grundschutzkatalog vermitteln**	*Resilient* *Suffizient* *Effizient*	reagieren, schützen **abwehren**
Verlagerung von staatlichen Aufgaben auf Private **Datenverlagerung**	*Resilient* *Suffizient* *Effizient*	ausweichen **Verlagerung von staatlichen Aufgaben auf Private**
Tatnachweise neu justieren – Cybercrime **Spuren im Internet**	*Resilient* *Suffizient* *Effizient*	neue Vollzugs- und Erfassungslgik durch *forensische Analysen* **Tatnachweise neu justieren (geringeres Maß an Überzeugungskraft)**

Ein Ergebnis der bisherigen Arbeiten im VR 07 sind die folgenden Vulnerabilitäten

- **Komplexität** (komplexe IT-Anlagen u. Software, falsche Konfiguration)
- **Vertrautheit** (Verwendung von allgemein zugänglichem Code, dessen Lücken bereits bekannt sind)
- **Vernetzung** (je umfassender IT-Anlagen vernetzt sind, desto höher könnte das Risiko einer Verletzlichkeit sein, aber auch das Gegenteil ist denkbar)
- **Schlechtes Passwort-Management**
- **Fehler im Betriebssystem** (Gefahr der Infektion mit Viren, unerlaubter Zugang))
- **Software-Fehler**

- **Anwenderfehler** (die wohl größte Vulnerabilität dürfte der Anwender sein)[15]

Die Aussagen der Tabelle 2 machen es möglich, Erörterungen so darzustellen, dass Vulnerabilitäten als in den unterschiedlichen Projektstadien von DiDaT (kleine Schrift vor der 2. Stakeholder-Konferenz) erkannt werden. Die Ausführungen in normal großer Schrift kennzeichnen die Ausführungen zu den Vulnerabilitäten, die während der Arbeitsgruppenphase der 1. Stakeholder-Konferenz (SHK) entstanden. Der bisherige Bearbeitungsstand zeigt somit qualitative Unterschiede so auf, dass die Arbeitsergebnisse entsprechend der Inhalte in der transformativen Spalte (prozessuale Tiefe), erst nur als zu differenzierend erkannt werden und mit den Vulnerabilitäten der zweiten Generation in Tab. 3 so betrachtet werden können, dass die systematischen Abhängigkeiten in Form von Mechanismen erkannt und beschrieben werden können.

Thematische Verdichtungen aus der "Wenn/Dann - Abwägungen" zu den jeweils in den Kästen der Tabelle 2 gegenüberliegenden Vulnerabilitätsräumen werden dabei so geführt, dass Antworten zu den folgenden Steuerungsfragen dazu befähigen, einen qualitativen Stakeholder-Diskurs zur Findung von Unseens entsprechend den Hauptbereichen fortzuführen. Die Stakeholder-Analyse, ist in Umfang und zuletzt verfassten Zuordnung insofern methodisch transparent, als eine Ausrichtung einer thematischen und systemrelevanten zur Diskussion geführt wird.

Unseens in Bezug auf digitale Daten

Cybercrime, insbesondere eine Gesetze verletzende Nutzung von digitalen Daten, beansprucht die Strafverfolgung in unterschiedlicher Qualität. Die Gründe hierfür, liegen in der zunehmenden Professionalität der Täter sowie auch einer örtlichen Flexibilität, mit der Cyberangriffe verübt werden.

Tatort und Taterfolgsort müssen nicht zwingend identisch sein und die Angriffe auf ausgewählte Ziele erfolgen zunehmend gut vorbereitet.[16] Die Errichtung von Schwerpunktstaatsanwaltschaften (etwa StA Cottbus) ist ein Beispiel für eine organisationsrechtliche Reaktion im Feld der Strafverfolgung von Cyberdelikten. Ist die Schwerpunktstaatsanwaltschaft im Vergleich zu herkömmlich organisierten Staatsanwaltschaften, so auch solche Cybercrime Delikte bearbeiten, bei der Strafverfolgung erfolgreicher? Oder spielen dabei noch andere Aspekte der staatsanwaltschaftlichen Arbeit und Sorgfältigkeit eine Rolle und wenn ja, welche? Ist eine Grenze zwischen der Bearbeitung von Cybercrime-Delikten in strafprozessualer Konkurrenz mit weiteren Delikten gezogen, oder wird diese bzw. kann diese bei „Hybrid-Delikten" interpretiert werden? Tatsächlich ist festzustellen, das derart gravierende organisationsrechtliche Vorhaben keinerlei empirischer Begleitung erfahren.

[15] https://www.upguard.com/blog/vulnerability

[16] Vgl. Bundesministerium des Innern, für Bau und Heimat, o. J.

3. Welche Stakeholder sind von Bedeutung?

Box 2: Vier Übergangsfragen zur Klärung von Vulnerabilitäten und deren Zuordnungen

1. Fragestellungen an Unternehmen als mögliche Stakeholder
   - Welche Missbräuche können Sie mit Ihren Mitteln identifizieren?
   - Handelt es sich bei den Auswertungsergebnissen um „Real-Time-Daten“ oder „Offline-Daten“?
   - Welche Maßnahmen kann das Unternehmen selbst und unmittelbar setzen? Sind diese Maßnahmen State-of-the-Art?
   - Verfügen Sie über ein Alarmierungssystem für das Unternehmen?
2. Verantwortlichkeiten
   - Grundsätzliche Frage:
     - Wer ist für den Schutz von was im Internet zuständig (Provider, Techniker, User)?
3. Wirtschaftsfaktor Sicherheit
   - Budgets für Cybersicherheit steigen (auch Auswirkungen als Folge der Datenschutzgrundverordnung)
   - Eigener Wirtschaftszweig
4. Paradigmenwechsel
   - Früher: Reaktionen auf Angriffe
   - Jetzt/Trend: Dynamische präventive Vorkehrungen im Rahmen von Cyber-Security. Angriff/Vorfall schnell erkennen und richtig darauf reagieren – Resilienz steigern
   - Man kann sich nicht vollständig vor Angriffen schützen – Reaktion (Zeit und Maßnahmen) sind wichtig!
     - Technische Vorkehrungen
     - Persönliche Sensibilisierung
   - Hack-back (moralisch und rechtlich vertretbar?)
   - Prävention statt Repression

Die Begründung der Stakeholder-Auswahl erfolgt mit der Zusammenfassung der ersten Beantwortungen der vier Zuordnungen in Box 2 als Herleitung, die prozessual transdisziplinär entstand. Dabei ist zu erkennen, dass thematisch räumliche (an welcher Stelle im Internet findet einer *Spurenanalyse* statt) und inhaltliche (paradigmatische Nutzung des digitalen Raumes durch z.B. geschäftliche, private oder andere Inhalte/Daten) Zuordnungen systematisch erkannt werden. Eine konkrete Arbeitsgrundlage als Basis zur weiteren Herangehensweise und Ergebnisermittlung, wird mit folgend dargestellten Verengungen der Fokusgruppe, bestehend aus Stakeholdern, so ermöglicht, dass *Unseens* optional im weiteren Verlauf sichtbar werden.

Im Laufe der Diskussion wurde auf der Grundlage der Stakeholderkonferenzen eine Analyse über möglich „Unseens“ erstellt, die im Laufe der Arbeiten im VR 07 zunehmen evaluiert und validiert wurden. Als Ergebnis ist eine Verschiebung der Vulnerabilitäten zu erkennen, mit der Folge, das anfangs zentrale Akteure nun eher nachgelagerte Bedeutung haben.

- Konzeptionelle Herangehensweise
- Brainstorming und Zugangsmöglichkeiten
- Erörterung der Teilnahmekriterien an einem zu identifizierenden Markt

Tabelle 3: Stakeholder-X-Tabelle VR07 Cybercrime/ Cyber Security, 2019

Mögliche Stakeholdergruppen u. Einzelvertreter der Gruppen	**Geschäftsfeldbeziehungen** Concerns / Competences / Threats / Sensitivities (Bedenken, Kompetenzen, Bedrohungen, Sensitivitäten)				
	Rechtsrahmen	Organisations-bezogene Fragen	Privatisierung staatlicher Aufgaben	Automatisierte Verfahren (KI)	Abwehrverhalten, digitale Resilienz
1. Staatsanwaltschaft Internetkriminalität	S	S	s	X	X
2. Mobilfunkunternehmen	M, G, s	M, G, s	M, G, s	M, G, s	M, G, s
3. Unternehmensberatung	X	A, M	A, M	A, M	X
4. Systemrelevante Anbieter (Banken)	A, M, KI, D, s	X	A, M, KI, D, s	X	A, M, KI, D, s
5. System- (Ausstatter u. Ausrüster)	M, G, s	X	X	X	X
6. Interpol / Zivilgesellschaft	S	S	s	X	X
7. Universitäten Cyber Security	A, K, S, KI	A, K, S, KI	X	A, K, S, KI	A, K, S, KI

Agenda: Awareness (A), KRITIS (K), Markt (M), automatisch (KI), Grundschutzkatalog (G), Datenverlagerung (D), Primäre Spuren im Internet zur Strafverfolgung (S), sekundäre Spuren im Internet zur Aufbewahrung (s)

Das derzeit vorhandene Recht erlaubt bei erster Analyse in vielen Fällen keinen hinreichenden Zugriff auf Datenkriminalität. Zur Einsicht der Themen Cybercrime und Cybersecurity wurde in den Unternehmen aber auch spezifisch bei der Staatsanwaltschaft – theoretisch - eine IST-Analyse durchgeführt. Die daraus resultierenden Ergebnisse und Perspektiven sind „faktisch“ das Cyberabwehrzentrum bei der Deutschen Bank, das Cyber Security Transparency Center von Huawei in Brüssel und die Sicherheitseinrichtungen von Vodafone.

Digitale Daten hinterlassen Spuren und solche Spuren sind Unseen, zu denen im Zuge der Td-Lab Forschung weitere Orientierungen entstehen. Heute erfolgt eine erste Beurteilung zu beachtbaren und weniger beachtbaren Spektren von Anwendungen im Internet. Diese Nutzungen führen zu systematischen Herausforderungen, dadurch, dass Daten im Netz selber erstellt als auch von außen an das Netz herangetragen werden und als ***digitale Spuren*** gefunden werden wollen. Der bisherige Bezug zur

Leitfrage wird mit Hilfe der Stakeholder-X-Tabelle und vor dem Hintergrund der Unseens weiter qualifiziert. Aus diesem Grunde ist eine methodische Fokussierung des Gegenstandsbereiches und des zukünftigen Bereiches, der aufgrund von systematischen Antwort, die auf Fragen von Unseens aufgeworfen werden, Gestalt (als Orientierungen) annimmt.

Box 3: Perspektiven-Wechsel

4. Paradigmenwechsel
- Früher: Reaktion auf Angriff
- Jetzt/Trend: Dynamische präventive Vorkehrungen im Rahmen von Cyber-Security. Angriff/Vorfall schnell erkennen und richtig darauf reagieren – Resilienz
- Man kann sich nicht vollständig vor Angriffen schützen – Reaktion (Zeit und Maßnahmen) sind wichtig!
    - Technische Vorkehrungen
    - Persönliche Sensibilisierung
- Hack-back (moralisch und rechtlich vertretbar?)
- Prävention statt Repression

Die mittels „empirischer Daten“ durchgeführte analytische Betrachtung der Stakeholderperspektiven – hin zu den Vulnerabilitäten als Teil eines transdisziplinären Prozesses zur Verwendung von digitalen Daten mit dem klaren Bezug zu Cybercrime – gibt zu erkennen, dass nicht alle bisherigen Zuordnungen, wie aus der Stakeholder X Tabelle ersichtlich, zutreffend sind.

4. Erwartete Ergebnisse und Folgeinitiativen als *Vertiefungsforschung*

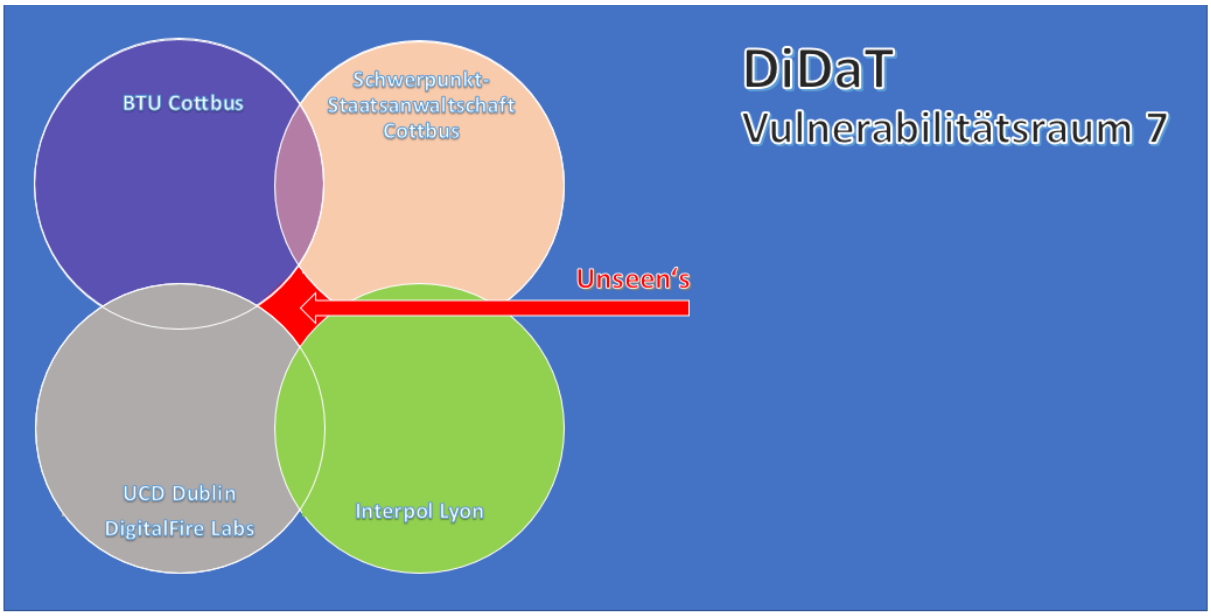
Eine Herausforderung ist, die unterschiedlichen wissenschaftlichen und praktischen Ansätze so zusammenzuführen. Eine Vertiefungsforschung als Schlussfolgerung dieses Feinplans, erfolgt mit den VR07-Teilnehmern BTU (Forensic Sciences and Engineering), Schwerpunktstaatsanwaltschaft (StA Cottbus), UCD Dublin – DigitalFire Labs und Interpol Lyon.Dabei werden bilaterale und multilaterale Schnittmengen herausgearbeitet. Durch diese Vorgehensweise sollen Unseen's komprimiert und so in den Fokus gestellt werden, dass diese eindeutiger zu identifizieren, als es bisher gelungen ist. In dieser Feinplanung sind Ergebnisse diejenigen Aussagen, die anhand der Bearbeitung zu den Wenn-Fragen als Suche nach Vulnerabilitäten durch die Dann-Antwort sich insofern ergeben haben, sodass eine Basis dieser Forschungsarbeit vorhanden ist. Der Feinplan stellt die erwünschte Arbeitsbasis zur empirischen Bearbeitung von Datennutzungen, Datenanalysen und Auswertungen bei der

Schwerpunkt-Staatsanwaltschaft in Cottbus dar. Auf dieser Basis kann die Arbeitsgruppe des VR 07 Cybercrime/-security die nötigen Ergebnisse als Beiträge zum Weißbuch erarbeiten und darüber hinaus in Vertiefungsforschungsprojekten und in der Anwendung der Td-Labs fortführen.

Vertiefungsforschung *Cyber Security*

Die Analyse des ***DarkNet*** ist notwendige Folge, da in diesem Bereich die meisten ***kriminellen Aktivitäten als Dienste angeboten*** werden (Angriff als ein Service). Das DarkNet und das DeepWeb werden/sind gerade vor dem Hintergrund solcher ***Dienste*** ein besonderer Marktplatz für illegale Geschäfte.[17] Analysen dazu können helfen, das Ausmaß und die Vielfalt von Cybercrime zu untersuchen und besser zu verstehen. Das wiederum hilft, gezielte Maßnahmen zu erarbeiten, um solche Aktivitäten zukünftig durch Präventionsmaßnahmen und -strategien zu unterbinden (Cyber Security).

Abbildung 2: Vertiefungsforschung „digitale Spuren“



Vertiefungsforschung *Cybercrime*

Die Kooperation zwischen der BTU (Studiengang Forensic Sciences and Engineering), der Hochschule UCD in Dublin/Ireland (Prof. Gladyshev) und Interpol in Lyon (Cybercrime) entfaltet vor dem Hintergrund des Projektes DiDaT eine *neue Perspektive*, die dazu einlädt, Vertiefungsforschung im VR07 wie folgt zu beginnen.

Der Wissensbedarf zum Thema “Digitale Forensik” ist in den Bereichen des Spurenbeweises sehr hoch. Bisherige Erkenntnisse aus diesem Bereich sind solche, die in Gerichtsverfahren den Verfahrensverlauf erfolgreich begleitet und zu einem entsprechend zuverlässigen Abschluss gebracht haben (Daten). Forensische Gutachten im digitalen Bereich und darüber

[17] Vgl. Bundeskriminalamt, 2018, S. 25

hinaus in Bereichen der transdisziplinären Verständnisart ermöglichen es, einen dynamisch zu gestaltenden Lernprozess neuartig zu begründen. Das Tool für die Ausbildung von Staatsanwälten, Richtern und Ermittlern existiert bereits und erste Schulungen wurden im Rahmen der Arbeiten bei Interpol durchgeführt Es gilt eine erste *Vertiefungsforschung* im Hinblick auf Anwendbarkeit und Adaptierbarkeit, zusammen mit den vier Partnern (BTU, Schwerpunktstaatsanwaltschaft Cottbus, UCD und Interpol) unter dem Dach von DiDaT aktuell bis zum 15.12.2019 zu erreichen.

Literatur

Banks, J. (2010): Regulating hate speech online, International Review of Law, Computers & Technology, 24:3, 233-239,

Bundesamt für Sicherheit in der Informationstechnik (o. J.): Cyber-Sicherheit. <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html>, [Zugriff 2019-10-23]

Bundesamt für Sicherheit und Informationstechnik (o. J.): IT Grundschutz, Die Phasen des Sicherheitsprozesses. <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchu-lung/OnlinekursITGrundschutz2018/Lektion_2_Sicherheitsmanagement/Lektion_2_02/Lektion_2_02_node.html>, [Zugriff 2019-10-23]

Bundeskriminalamt (2017): Cybercrime, Bundeslagebild 2017, S. 25.

Bundeskriminalamt (o. J.): Internetkriminalität/Cybercrime. <https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html>, [Zugriff 2019-10-23]

Bundesministerium des Innern, für Bau und Heimat (o. J.): Cyberkriminalität. <https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyber-kriminalitaet-node.html> [Zugriff 2019-10-23]

Carraro, L., Castelli, L. (2011): Ideology is related to basic cognitive processes involved in attitude formation. Journal of Experimental Social Psychology, Vol. 47, Issue 5, S. 1013-1016.

Décary-Hétu, D., u. Dupont, B. (2012) The social network of hackers, Global Crime, 13:3, 160-175,

Del Monte, A., Papagni, E. (2001): Public expenditure, corruption, and economic growth: the case of Italy. European Journal of Political Economy, vol. 17, issue 1, 1-16.

Ebert, H., Maurer, T. (2017): Cyber Security. In: Patrick James (ed.): Oxford Bibliographies in International Relations. Oxford University Press, New York.

Eckert, C. (2017): Cybersicherheit beyond 2020. Informatik-Spektrum 40 (2017), Nr. 2, S. 141-146.

Falk, M. (2017): Cyber Security. Der blinde Fleck auf der CEO-Agenda. Entscheidern fehlt das «Big Picture» in der Diskussion um Cyber-Risiken. www.klardenker.kpmg.de (abgerufen am 02.05.2019).

Freiling, F., Grimm, R., Großpiesch, K.-E., Keller, H.B., Mottok, J., Münch, I., Rannenberg, K., Saglietti, F. (2014): Technische Sicherheit und Informationssicherheit. Unterschiede und Gemeinsamkeiten. Informatik-Spektrum 37, Nr. 1, S. 14-24.

Godbole, S. (2016): From Information Security to Cyber Security. www.isaca.org (abgerufen am 02.05.2019)

Goeken, M., Fröhlich, M. (2018): Sicherheit im Cyberraum – Stand der Dinge, Herausforderungen, Lösungsansätze. IT-Governance 27, S. 3-9.

Golem Media GmbH (o. J.): Darknet. <https://www.golem.de/specials/darknet/>, [Zugriff 2019-10-23]

Lentner, G. M. (2019). *Comparative Legal Analysis on Digital Data as subject of the European/German, US-American and Hongkong Law*.

Mertens, P., Barbian, D., Baier, S. (2017): Digitalisierung und Industrie 4.0 – eine Relativierung. Springer Wiesbaden.

Miebach, K. (2016), § 261, Rn. 58 f., in: Knauer, C., Kudlich, H., Schneider, H. (Hrsg.), Münchener Kommentar zur StPO, Beck, München.

Polizei (o. J.): Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen. <https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html> [Zugriff 2019-10-23]

Pospisil, B., Gusenbauer, M., Huber, E., Hellwig, O. (2017): Cyber-Sicherheitsstrategien – Umsetzung von Zielen durch Kooperation. Datenschutz und Datensicherheit – DuD, Ausgabe 10.

Scholz , R. W., u. Kley, M. (2019): Stocks and Flows-based Stakeholder Analysis of Digital Data – Basic concepts, tools for analysis, data, and the role of digital data infrastructure providers. Kreuzlingen: STTM.

Siepermann, M. (2017): Stichwort «IT Security». In: Gabler Wirtschaftslexikon online. www. wirtschaftslexikon.gabler.de (abgerufen am 02.05.2019)

Von Solms, R., van Niekerk, J. (2013): From information security to cyber security. Computers u. Security, Vol. 38, 10/2013, S. 97-102.

Wikimedia Foundation Inc. (2019): Tor (Netzwerk). <https://de.wikipedia.org/wiki/Tor_(Netzwerk)> [Zugriff 2019-10-23]

Whitman, M., Mattord, H. (2012): Principles of Information Security. 4th ed., Boston.