Exposé für das Dissertationsvorhaben

„Cyberforensik“

Probleme bei Ermittlungen im Cyberspace im Kontext des österreichischen und europäischen Rechtsbereiches

Verfasser

Dipl.-Ing. Thomas Hrdinka

Angestrebter akademischer Grad

PhD in Interdisciplinary Legal Studies

Betreuer

ao. Univ.-Prof. Mag. DDr. Erich Schweighofer

Wien, am 18.11.2017

1. Einleitung

Ein technisches Teilgebiet welches der Aufklärung aber auch der Prävention von Straftaten dient, ist das junge Fachgebiet der Computerforensik. Handelte es sich zu Beginn vor etwa 20 Jahren noch um die Analyse von Festplatteninhalten, so entwickelte sich die Computerforensik[1] rasant weiter und unterteilt sich heute in zahlreiche weitere Teilgebiete wie zB der Netzwerkforensik, Cloudforensik, Carforensik, und der Cyberforensik. Der Cyberspace, abgeleitet von Kybernetik[2] und Raum, umfasst das Internet samt den vernetzten Computern und den damit geschaffenen Datenraum. Dieser unterteilt sich heute in ein allgemein sichtbares und nutzbares Internet, wo weder Anonymität noch Privatsphäre technisch geschützt sind, und in ein Peer-to-Peer Overlay Netzwerk, dem Darknet oder Deep Web, wo eben diese Anonymität technisch gewährleistet ist. Das Darknet wird daher in zunehmendem Maße für kriminelle und terroristische Zwecke genutzt.

2. Motivation

Ich bin seit meiner Befugnisverleihung zum Ziviltechniker für Informatik vor 17 Jahren, und noch vielmehr seit der Zertifizierung zum allgemein beeideten und zertifizierten Gerichtssachverständigen mit der Rechtsinformatik laufend konfrontiert. In zahlreichen Fällen, sowohl bei Privatgutachten, Aufträgen von Behörden oder Gerichten, waren nicht ausschließlich informationstechnische Fragestellungen zu behandeln, sondern auch materiellrechtliche. Diesbezüglich war und ist nach wie vor der Datenschutz (im Sinne von Privacy) ein zentrales Thema, der auch in weitere komplexe Gebiete wie zum Beispiel jene des e-Governments und des e-Healths ausstrahlt. Seit dem Inkrafttreten des Datenschutzgesetzes 2000, ist dieses Gesetz ständig neuen technisch-rechtlichen Herausforderungen, insbesondere jenen des Internets, unterworfen gewesen. Die Technologien entwickeln sich nach wie vor in einer rasanten Geschwindigkeit, und im globalen Ausmaß weiter, sodass Gesetzgeber oftmals den aktuellen Herausforderungen hinterher hinken. Dabei eröffnen sich immer häufiger rechtlich fragwürdige und sogar rechtsfreie Räume.

Mit der Europäischen Datenschutzgrundverordnung[3], die im Mai 2018 gültig wird, hat die Kommission eine Vereinheitlichung des Datenschutzrechts auf europäischer Ebene initiiert. Die Kommission versucht auch in anderen Bereichen den neuen Bedrohungen entgegen zu wirken, was sich einerseits in der Förderung von neuartigen Technologien wie der Cyberabwehr zeigt, aber auch mit der Schaffung entsprechender rechtlichen Rahmenbedingungen, die nötig sind, um diese neuen Technologien rechtlich gedeckt einsetzen zu können. Das zentrale Ziel ist den globalen Bedrohungen durch die organisierte Kriminalität und jener der Cyberterroristen effizient entgegenzuwirken[4].

3. Aktueller Forschungsstand

Der aktuelle Stand der Technik zur Bekämpfung der Bedrohungen in der Cyberwelt ist mittlerweile weit fortgeschritten. Hingegen eröffnet sich auf rechtlicher Ebene vielfach Neuland, was dazu führen kann, dass trotz technisch erfolgreicher Ermittlungen eine Strafverfolgung nicht möglich ist.

Zum Stand der Wissenschaften kann mit gutem Gewissen gesagt werden, dass trotz dieser sehr jungen Wissenschaft der Computerforensik auf technischer Ebene zwar einige wenige wissenschaftliche Arbeiten existieren, jedoch im rechtlichen Bereich keine bis marginal wenige Ergebnisse vorzufinden sind.

1 *Dewald Andreas*: Formalisierung digitaler Spuren und ihre Einbettung in die Forensische Informatik.
2 *Wiener Norbert*: Mensch und Menschmaschine. Kybernetik und Gesellschaft.
3 Verordnung (EU) 2016/679
4 *Reindl-Krauskopf Susanne*: Cyberstrafrecht im Wandel

Folgende beispielhafte Fälle sollen diesen Umstand verdeutlichen:

Angriffe gegen „kritische Infrastrukturen“ iSd StGB[5] werden immer häufiger subkonventionell mit Hilfe des Internets durchgeführt. Der Grund ist evident, denn konventionelle Angriffe wie zB jene mit Kampfbombern erfordern entsprechend hohe logistische Anforderungen, Kosten und Risiken. Spätestens seit der Zerstörung einer Urananreicherungsanlage im Iran mit Hilfe des Computerwurms „Stuxnet“, sollte jedem Betreiber krit Infrastrukturen und politisch Verantwortlichen klar sein, dass für den Cyberspace adäquate technische, rechtliche und organisatorische Maßnahmen getroffen werden müssen, um Angriffen rechtzeitig, also beispielsweise vor einem Blackout (ein großräumiger Stromausfall) begegnen zu können. Nicht nur die Stromnetze können Ziel einer Sabotage sein, gleichfalls sind auch Netze für Gas, Wasser und Abwasser bedroht. Der Grund ist, dass die Prozesssteuerungsanlagen für all diese Bereiche von den selben Herstellern stammen, und daher die Angriffsvektoren die gleichen sind. Die Europäische Kommission hat diesen Herausforderungen politisch Rechnung getragen und mit der ab 2016 geltenden eIDAS Richtlinie[6] und der von den Mitgliedsstaaten zeitgleich mit Inkrafttreten der EU-DSGVO 2018 umzusetzenden NIS Richtlinie[7] entsprechende rechtliche Rahmenbedingungen vorgegeben, wo auf sog „Wesentliche Infrastrukturen“ ein besonderes Augenmerk geschenkt werden soll.

Eine präventive Abwehr solcher Angriffe erfolgt vielfach mit neuartigen konspirativen Methoden, ohne entsprechend rechtlicher Deckung, abgesehen von Ausnahmen[8]. Im Rahmen des Treasuremap Projekts der NSA und GCHQ wird bspw versucht, eine weltweite Landkarte aller technischer, geographischer und personenbezogener Daten des Internets zu erstellen. Nachdem die rechtlichen Rahmenbedingungen für Spionage in den EU Mitgliedsländern unterschiedlichst geregelt sind, bieten solcherart konspirative Methoden im Cyberspace auch einen Freiraum für Wirtschaftsspionage[9]. Die EU einigte sich daher 2016 auf die Trade-Secret Richtlinie[10], die bis Juni 2018 umzusetzen ist. Mit diesem Schritt soll der Rechtsschutz der Geheimnisinhaber gestärkt werden.

Der technische Entwicklungsprozess ist bei weitem nicht abgeschlossen, sondern betrifft immer mehr die Privatsphäre der Nutzer. Sind heute zB Smartphones und Smart-TVs bereits alltäglich, die oftmals personenbezogene Daten ohne Zustimmung der Nutzer aus der EU exportieren, so werden zukünftig immer mehr Fahrzeuge vernetzt (Fahrzeugtelematik), die Wohnungen mit Informationstechnologien ausgestattet (Smart-Home) und letztendlich wird das zukünftige Internet of Things (IoT) eine Kontrolle des mit dieser Technologie überbordenden und oftmals verschlüsselten Datenverkehrs organisatorisch unmöglich machen. Ein Rechtsschutz betroffener Nutzer ist zwar mit dem geltenden Datenschutzgesetz, und zukünftig mit der EU-DSGVO gegeben, jedoch scheint es in solchen Fällen aus den vorher genannten Gründen praktisch nicht durchsetzbar zu sein.

BigData, die Vernetzung und Aggregierung großer, verteilter Datenbestände, ist nicht nur ein technischer Fachbegriff, sondern erfordert präzise rechtliche Rahmenbedingungen. Betreffend Ermittlungen bei Straftaten, Prävention vor terroristischen Angriffen und anderen Herausforderungen existieren in den Mitgliedsstaaten der Europäischen Union unterschiedlichste Rahmenbedingungen und Regelungen, solche Daten verarbeiten und verwerten zu dürfen. So ist es beispielsweise in Großbritannien zulässig, dass Scotland Yard eine vernetzte Videoüberwachung mit automatisierter Gesichtserkennung[11] und einer selbstlernenden Verhaltensvorhersage betreibt, während selbiges in Deutschland aufgrund der

5 BGBl. Nr. 60/1974 idgF, insb §§ 118a Abs 2, 126a Abs 2 Z 4, 126b Abs 4 Z 2
6 Verordnung (EU) Nr. 910/2014
7 Verordnung (EU) 2016/679
8 ETSI ES 201 671 V3.1.1: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
9 Bayerisches Landesamt für Verfassungsschutz, Baden-Würtemberg Landesamt für Verfassungsschutz: Wirtschaftsspionage in Baden-Würtemberg und Bayern, Daten-Fakten-Hintergründe
10 Richtlinie (EU) 2016/943
11 *Grund, Nico*: Biometrie - Algorithmen zur Personen-Authentifizierung und Datenschutzrechtliche Grundlagen

gegenwärtigen rechtlichen Rahmenbedingungen undenkbar ist. Es laufen dazu aber bereits Pilotprojekte, und es existieren auf diesem Gebiet zahlreiche Aktivitäten europäisch vernetzter Forschungsinstitute und Behörden, die an neuartigen Überwachungssystemen arbeiten.

4. Wissenschaftliche Problemstellung und Methode

Diese Dissertationsarbeit hat zum Ziel, die zuvor beschriebenen rechtlichen Rahmenbedingungen und Problemstellungen bei der Ermittlungstätigkeit auf europäischer Ebene und im Kontext konkreter technischen Bedrohungen[12] aufzuarbeiten, sowie punktuelle Vergleiche zur Rechtslage in Österreich zu ziehen. Weiters sollen gegenwärtige und zukünftige Herausforderungen und Bedrohungen analysiert werden, um daraus technische und vor allem rechtliche Maßnahmen dagegen schließen zu können.

Den Schwerpunkt dieser Arbeit bilden daher die rechtliche Aspekte des Einsatzes konspirativer und nicht konspirativer forensischer Methoden im Cyberspace. Folgende konkrete **rechtliche Problemstellung**, soll im Dissertationsvorhaben erforscht werden:

- Eigenermittlungen, Ermittlung durch Exekutive und Justiz und vernetzte Ermittlung auf europäischer Ebene:

  Die Eigenermittlung von Straftaten, im Speziellen der Internetkriminalität, unterliegt anderen rechtlichen Rahmenbedingungen als die Ermittlung durch die Exekutive und Justiz und sie bietet sowohl Vor- als auch Nachteile. Eine Eigenermittlung ist bei personenbezogenen Daten dann behindert, wenn aus Datenschutzgründen Betroffene oder der Betriebsrat keine Zustimmung zur Datenweitergabe erteilen. Trotzdem wird von dieser Ermittlungsmöglichkeit von insb Firmen Gebrauch gemacht, wenn Vorteile wie Zeitnähe und Schutz vor der Öffentlichkeit für diese ausschlaggebend sind. In anderen Fällen ist eine Strafverfolgung durch Behörden die bessere Wahl, und so ferne eine Anzeigepflicht besteht, auch obligatorisch. Seit 2013 ist eine spezielle EUROPOL Einheit, das European Cybercrime Centre (EC3) aktiv, um europaweit vernetzt die Cyberkriminalität[13] zu bekämpfen. Dabei ist die Abteilung „**Forensic Expertise**“ ein Teil dieser Organisation. Obwohl die EC3 in der kurzen Zeit ihres Bestehens bereits zahlreiche Erfolge aufweist, ist damit zu rechnen, dass Cybercrime und Cyberterror zukünftig vermehrt auftreten werden[14]. Auch die stetig steigenden Zahlen von Kriminalfällen im Cyberspace lassen einen Rückschluss darauf zu.

In **technischer Hinsicht** soll folgender Bereich beleuchtet werden:

- Lösungsansätze für die IT-Forensik gegen Cybercrime, Cyberterror, Kryptographie, Cracken und Antiforensik

  Es werden laufend neue, und daher schwer bekämpfbare Angriffe und Bedrohungen mit Hilfe des Cyberspaces geplant, die nach dem derzeitigen Rechtsstand als rechtswidrig, tw aber auch als legal einzustufen wären. Ein Ende dieser Entwicklung ist nicht absehbar, vielmehr wird mit der Einführung des Internet of Things (IoT) die Möglichkeit geschaffen, eine unkontrollierbare Menge von Geräten im Internet mit Sicherheitslücken für kriminelle Zwecke zu nutzen[15]. Sicherheitstechnische Maßnahmen, Sicherheitskonzepte und Kryptographie schützen die IT-Systeme und bilden gem der EU-DSGVO den „Stand der Technik“ für den Schutz von personenbezogenen Daten. Auch werden kryptographische Verfahren bei elektronischen Signaturen, im e-Government, e-Health und auch in der Kommunikation wie dem elektronischen Rechtsverkehr uvm eingesetzt. Ein Brechen dieser, in manchen Rechtsmaterien sogar gesetzlich verordneter Verfahren, kann dazu

12 Bundesministerium für Inneres: Cybercrime-Report 2015
13 Europäischer Rat: White Paper on transnational organised crime
14 World Economic Forum: The Global Risks Report 2017
15 Symantec: 2016 Internet Security Threat Report, Symantec Corporation

führen, dass eine Manipulation von verschlüsselten Daten dazu führt, dass der originale Datenverkehr nicht mehr von Fälschungen zu unterscheiden wäre. Neuartige, zukünftige Computersysteme wie Quantencomputer, die in verschiedenster Technologie dz als Prototypen existieren, oder bereits kommerziell verfügbare „Adiabatische Quantencomputer“ könnten aufgrund massiver Parallelisierung der Berechnungen nur einen Bruchteil der Zeit benötigen, um gegenwärtig als sicher geltende Verfahren und Schlüssellängen in kurzer Zeit zu brechen.

Abgeleitet aus den vorab beschriebenen Problemstellungen sollen im Dissertationsvorhaben folgende **technisch-rechtliche Fragen** beantwortet werden:

1. Mögliche Lösungsansätze für eine effiziente Ermittlungsarbeit im Cyberstrafrecht?

   Aufgrund der vorliegenden Vor- und Nachteile zw Eigenermittlung und Ermittlung durch die Exekutive und Justiz, so ferne keine Anzeigepflicht besteht, sollen Möglichkeiten erforscht werden, die eine verbesserte bzw beschleunigte polizeiliche Ermittlungsarbeit gewährleisten. Auch sollen Maßnahmen die Eigenermittlungen gerichtlich verwertbar machen (insb in Bezug auf Nachvollziehbarkeit und Glaubwürdigkeit) definiert werden, und auch datenschutzrechtliche Hinderungsgründe aufgezeigt, samt Lösungsmöglichkeiten dazu erforscht werden.

2. Maßnahmen in der EU zur Förderung einer effizienten Ermittlungsarbeit im Cyberspace?

   Effiziente Maßnahmen zur Bekämpfung der Cyberkriminalität werden auf europäischer Ebene durch EUROPOL verfolgt, jedoch unterliegen die Ermittlungen nach wie vor nationalem Recht. Nachdem die Geschwindigkeit des strafrechtlichen Handelns auch durch eine Verbesserung der technischen Möglichkeiten stetig steigt, ist die polizeiliche Ermittlungsarbeit dadurch immer mehr gefordert, und muss durch neue supranationale Möglichkeiten unterstützt werden. Präventive Maßnahmen zum Schutz vor Cyberattacken sind zwar mit der NIS-RL, und dem Grunde nach auch mit der DSGVO eingeführt worden, es ist aber zu befürchten, dass sich diese Gesetzesmaterien für eine effiziente Cyberabwehr und Cyberforensik als unzureichend erweisen werden, und eine weitere Nachbesserung daher geboten sein wird. Aus diesem Grund sollen Maßnahmen für eine EU-weite präventive Cyberabwehr erforscht werden.

3. Welche Folgen technischer und rechtlicher Natur in Bezug auf die Ermittlungen ergeben sich, wenn Cracken und Antiforensik erfolgreich sind?

   In Bezug auf die Ermittlungsarbeit sind erfolgreiche Angriffsversuche oder Abwehrmaßnahmen sehr hinderlich, und müssten erst durch mühsame, zeitintensive Gegenmaßnahmen begegnet werden, falls das überhaupt technisch möglich ist. Einerseits werden Algorithmen und Schlüssellängen penibel genau vorgegeben[16], andererseits wird lediglich der „Stand der Technik“ gefordert, ohne auf technische Details näher einzugehen. Auch gibt es die Möglichkeit, dass geforderte Verordnungen für nähere Anforderungen an qualifizierte Zertifikate[17] noch nicht erlassen worden sind. Gelänge ein Brechen der Schlüssel, so wäre eine Fälschung vom Original nicht mehr unterscheidbar (Beispielsweise ein Kassabon), und jegliche Spurensuche wäre somit per se konterkarierbar. Dieser Umstand erfordert in den gesetzlichen Bestimmungen über die Definition von Algorithmen und Schlüssellängen hinaus weitere, der Forensik dienliche Bestimmungen, wie beispielsweise eine Forderung zur fälschungssicheren Protokollierung, wobei Entwicklungen wie jene der Blockchain zweckdienlich sein könnten.

16 BGBl. II Nr. 410/2015
17 BGBl. I Nr. 50/2016

5. Vorläufiges Inhaltsverzeichnis

1. Cyberforensik und Spurensuche
    1. IT-Forensik; Einführung und Teilgebiete
    2. Stand der Technik und Wissenschaften in der Cyberforensik
    3. Physische und Digitale Spuren
    4. Cyber-Bedrohungen, Ziele und Schutz
        1. Das Darknet
        2. Das Internet of Things
        3. Kritische/Wesentliche Infrastrukturen
    5. Antiforensik
        1. Kryptographie
        2. Methoden und Schutz
2. Ermittlung/Strafverfolgung
    1. Cyberstrafrecht: Straftatbestände im Zusammenhang mit Computern und dem Internet
    2. Ermittlungsverfahren im Bereich Computerkriminalität
    3. Innovative Methoden und Tools zur Ermittlung im Cyberspace
    4. Grenzen und Probleme bei der Ermittlung
        1. Zuständigkeiten und Effizienz
        2. Datenschutz
        3. Weitere Rechtsmaterien
    5. Ermittlung auf europäischer Ebene
    6. Dokumentation und Austausch von Ermittlungsergebnissen
3. Ergebnisse und Maßnahmen
    1. Rechtsfolgen der Antiforensik
    2. Effizienz in der Ermittlung
    3. Technische und rechtliche Maßnahmen zur Ermittlung im Cyberspace
4. Schlussfolgerungen

6. Zeitplan

Vorbehaltlich der Genehmigung dieses Dissertationsvorhabens, wird folgender Zeitplan angestrebt:

2018	Bis Jänner	Literaturrecherchen, Recherchen, Fine-Tuning Kapitelstruktur
2018	Bis Juni	Kapitel 1
	Bis Dezember	Kapitel 2
2019	Bis Juni	Kapitel 3
	Bis Dezember	Kapitel 4, Pflichtlehrveranstaltungen, Auflagen
2020		Defensio

7. Ausgewählte Literatur

Folgende ausgewählte Literatur, Standards und Gesetze geben einen vorläufigen Stand der Literaturrecherche an:

[1] *Locard Edmund*: L'enquete criminelle et les methodes scientifique. Ernest Flammarion, Paris, 1920

[2] *Wiener Norbert*: *Mensch und Menschmaschine. Kybernetik und Gesellschaft*. Alfred Metzner Verlag, Frankfurt am Main 1952.

[3] *Inman, Keith ; Rudin, Norah*: Principles and Practice of Criminalistics: The Profession of Forensic Science. CRC Press, 2000

[4] Bayerisches Landesamt für Verfassungsschutz, Baden-Würtemberg Landesamt für Verfassungsschutz: Wirtschaftsspionage in Baden-Würtemberg und Bayern, Daten-Fakten-Hintergründe, München/Stuttgart, 2006

[5] ETSI ES 201 671 V3.1.1: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic, ETSI Standard, Sophia Antipolis, 2007

[6] *Grund, Nico*: Biometrie - Algorithmen zur Personen-Authentifizierung und Datenschutzrechtliche Grundlagen. Diplomarbeit, Marburg, 2007

[7] *Garfinkel, Simson L.*: Digital Forensics Research: The Next 10 Years. In: Proceedings of the Digital Forensics Research Conferencs (DFRWS), 2010

[8] *Saferstein, Richard*: Criminalistics: An Introduction to Forensic Science. 10th. Pearson, 2010

[9] *Geschöneck, Alexander*: Computer Forensik – Computerstraftaten erkennen, ermitteln, aufklären. Dpunkt Verlag, Heidelberg, 2010 – 4. Auflage

[10] BSI: Leitfaden „IT-Forensik". Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2010

[11] *Casey, Eoghan*: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011. – 3. Auflage

[12] *Dewald Andreas*: Formalisierung digitaler Spuren und ihre Einbettung in die Forensische Informatik. Dissertation, Erlangen, 2012

[13] ISO: Standard 27037 on "Guidelines for identification, collection, acquisition and preservation of digital evidence", Genf, 2012

[14] ENISA: Identification and handling of electronic evidence - Handbook, Document for teachers. European Union Agency for Network and Information Security (ENISA), 2013

[15] Europäischer Rat – CyberCrime@IPA: Electronic evidence guide - A basic guide for police officers, prosecutors and judges (Restricted/not for publication), Council of Europe, Strasbourg, 2013

[16] Europäischer Rat: White Paper on transnational organised crime, Council of Europe, Strasbourg, 2014

[17] CERT-EU: Incident Response - Data Acquisition Guidelines for Investigation Purposes. Security White Paper, Brüssel, 2012-04

[18] Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

[19] *Reindl-Krauskopf Susanne*: Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112

[20] Bundesministerium für Inneres: Cybercrime-Report 2015

[21] OLAF: Leitlinien zu digitalforensischen Maßnahmen für die Bediensteten des OLAF, Europäisches Amt für Betrugsbekämpfung, Brüssel, 2016

[22] Symantec: 2016 Internet Security Threat Report, Symantec Corporation, Mountain View, 2016

[23] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie)

[24] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

[25] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung

[26] BGBl. Nr. 60/1974 idgF: Strafgesetzbuch

[27] BGBl. I Nr. 50/2016: Signatur- und Vertrauensdienstegesetz

[28] BGBl. II Nr. 410/2015: Registrierkassensicherheitsverordnung

[29] COM(2017) 10 final: Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)

[30] World Economic Forum: The Global Risks Report 2017, 12th Edition, World Economic Forum, Geneva, 2017