Cyber Crime –
Zunehmende Bedrohung der Informationsgesellschaft

Symposium
am 20. April 2012

Landesgruppe Österreich
der Internationalen Strafrechtsgesellschaft (AIDP)
und
Juristenverband

Für die Unterstützung
danken wir
dem Bundesministerium für Justiz und
dem Juristenverband

Medieninhaber:
Landesgruppe Österreich
der Internationalen Strafrechtsgesellschaft
(AIDP)
A-1016 Wien, Justizpalast

Redaktion:
Mag.ª Andrea Lehner
Mag. Michael Leitner

Druck:
Bundesministerium für Justiz
1070 Wien, Neustiftgasse 2

2012

Inhaltsverzeichnis

Vorwort

Prof. Dr. Otto F. Müller
Präsident der Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft AIDP

Die Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) hat gemeinsam mit dem Juristenverband am 20. 04. 2012 im Palais Trautson (Bundesministerium für Justiz) ein Symposium zum höchst aktuellen Thema „Cyber Crime – Zunehmende Bedrohung der Informationsgesellschaft“ durchgeführt.

Es diskutierten am Podium und mit den zahlreichen Symposiumsteilnehmern unter der bewährten Leitung von Herrn Generalprokurator Prof. Dr. Ernst Eugen Fabrizy die Herren Sektionschef Hermann Feiner (Bundesministerium für Inneres), Oberstaatsanwalt Mag. Peter Gildemeister (Oberstaatsanwaltschaft Wien), Leitender Staatsanwalt Dr. Christian Manquet (Bundesministerium für Justiz), Universitätsassistent Mag. Dr. Farsam Salimi (Universität Wien) und Rechtsanwalt Prof. Dr. Fritz Wennig (Präsident des Juristenverbandes).

Unter den zahlreichen Teilnehmern konnten wir auch die Frau Vizepräsidentin des Verfassungsgerichtshofes Dr. Brigitte Bierlein und die Herren Bundesminister für Justiz a. D. Dr. Nikolaus Michalek, Sektionschef im Bundesministerium für Inneres Mag. Dr. Mathias Vogl, Rechtsschutzbeauftragen Dr. Gottfried Strasser und Präsidenten der deutschen Landesgruppe der AIDP Hon.-Prof. Peter Wilkitzki begrüßen.

Mein besonderer Dank gilt allen am Podium und an der Diskussion Mitwirkenden sowie dem Bundesministerium für Justiz und dem Juristenverband für die hervorragende Zusammenarbeit bei der Vorbereitung und Durchführung dieser

Veranstaltung sowie für die Förderung des gesellschaftlichen Abschlusses.

Wien, im April 2012

Einleitende Worte

Prof. Dr. Otto F. Müller
Präsident der Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft AIDP

Sehr geehrte Damen und Herren!

Es ist für mich eine große Ehre und Freude, Sie im Namen der Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP) und des Juristenverbandes recht herzlich begrüßen und Ihnen für Ihre Teilnahme an unserer heutigen Veranstaltung danken zu dürfen.

Mit Ihrem Einverständnis darf ich folgende Gäste namentlich willkommen heißen:

Die Frau Vizepräsidentin des Verfassungsgerichtshofes Dr. Brigitte Bierlein, die Herren Bundesminister für Justiz a. D. Dr. Nikolaus Michalek, Sektionschef im Bundesministerium für Inneres Mag. Dr. Mathias Vogl, Rechtsschutzbeauftragten Dr. Gottfried Strasser und mit besonderer Freude den Herrn Präsidenten der deutschen Landesgruppe der AIDP Hon.-Prof. Peter Wilkitzki, mit dem wir seit vielen Jahren eng verbunden sind.

Mein besonderer Gruß und Dank geht auch an die Podiumsteilnehmer, alle hervorragenden Experten, die der Vorsitzende des Podiums, Herr Generalprokurator Prof. Dr. Ernst Eugen Fabrizy sodann noch einzeln vorstellen wird.

Die Frau Bundesministerin für Justiz Dr. Beatrix Karl ist dienstlich verhindert an unserer Veranstaltung teilzunehmen, sie übermittelt uns aber die besten Grüße und Wünsche für ein erfolgreiches Symposium.

Wir danken dem Bundesministerium für Justiz und dem Juristenverband für ihre Unterstützung bei der Vorbereitung und nunmehrigen Durchführung dieser Veranstaltung.

Wir hätten wohl kein aktuelleres Thema als Cyber Crime wählen können, das seit Monaten für Schlagzeilen in den Medien sorgt, insbesondere im Zusammenhang mit Hackerangriffen. Diese neuen Erscheinungsformen der global verbreiteten grenzüberschreitenden Computerkriminalität und Internetstraftaten stellen eine gefährliche Bedrohung der modernen Informationsgesellschaft im Bereiche der Informationstechnologie (IT) dar, so durch koordinierte Hackerangriffe sowohl gegen Einzelpersonen als auch auf wirtschaftliche Unternehmen, zuletzt etwa auch auf Einrichtungen der UNO, auf öffentliche Dienste und Infrastrukturen, wie besonders durch die Hackergruppe „Anonymous“ mit dem österreichischen Ableger „Anon Austria“. So gab es etwa auch Angriffe gegen die Homepage des Bundesministeriums für Justiz und auf die Webseiten einiger politischer Parteien. Dazu kommen Erpressungsversuche, Diebstahl von Kontodaten und Betrügereien mit erheblichem Schaden, aber auch in Bezug auf Wirtschafts- und Militärspionage sowie besondere Gefährdung durch Extremisten und Terroristen, wie beispielsweise der Fall „Estland“ (2007) zeigt.

Wie anfällig das Internetsystem für die geschilderten kriminellen Handlungen ist, beweist der jüngste Fall von Hacking eines 15-jährigen Schülers in NÖ, der die Computer von 259 Firmen knackte und damit einen groß angelegten Hackerangriff gegen die Wirtschaft führte.

Diese neue Art der Kriminalität bedeutet eine große Herausforderung für deren legistische Erfassung und wirksame Bekämpfung in der Praxis.

Es hebt sich sohin die Frage, ob es überhaupt hinreichend wirksame gesetzliche Bestimmungen und entsprechende technische Ausrüstung der Exekutive gibt.

Diesem Erfordernis hat etwa das Bundesministerium für Inneres durch die Einrichtung der Spezialeinheit Cyber-Crime-Competence-Center, C4, Rechnung getragen und damit den geschilderten Fall der Attacken des 15-jährigen Schülers rasch aufklären können.

Neben einschlägigen Veranstaltungen auf nationaler Ebene gibt es auch auf internationaler Ebene ernsthafte Bemühungen zur Bekämpfung der Computerkriminalität, wie etwa die „Conference on Cyberspace“ in London im November 2011, wo es um die Sicherheit des Netzes im militärischen Bereich ging, an der auch Vertreter der NATO und Österreichs teilnahmen.

Die EU-Innenkommissarin Cecilia Malmström hat am 28.03.2012 ein „Europäisches Zentrum zur Bekämpfung der Cyberkriminalität“ vorgestellt, das seine Tätigkeit im Jahre 2013 in Den Haag aufnehmen wird und zwar unter dem Dach von Europol mit dem Ziel der erforderlichen grenzüberschreitenden Zusammenarbeit der Mitgliedstaaten der EU.

Auch der nächste Internationale Strafrechtskongress der AIDP im Jahre 2014 in Rio de Janeiro wird sich mit dem Thema der Internetkriminalität befassen.

Für Österreich stellt sich die Frage, ob die geltenden strafrechtlichen Bestimmungen diesen neuen Erscheinungsformen der Kriminalität gerecht werden und welche Rolle hiebei das österreichische Strafrecht überhaupt spielt.

Vorweg sei gesagt, dass es mehrere strafgesetzliche Bestimmungen gibt, die nach internationalen Vorgaben geschaffen wurden.

So wurden entsprechend der Cyber-Crime-Konvention des Europarates ETS Nr. 185 durch das Strafrechtsänderungsgesetz (StRÄG) 2002 folgende neue Bestimmungen in das Strafgesetzbuch eingefügt, und zwar über den widerrechtlichen Zugriff auf ein Computersystem nach § 118a StGB (auch „Hacking“ betreffend), die Verletzung des Telekommunikationsgeheimnisses nach § 119 StGB und das missbräuchliche Abfangen von Daten nach § 119a StGB; in diesen Fällen wird jedoch der Täter, außer als Mitglied einer kriminellen Vereinigung beim Delikt nach § 118a Abs 3 StGB[1], nur mit Ermächtigung des Verletzten verfolgt (Ermächtigungsdelikte).

Weiters neu geschaffen wurde die Bestimmung betreffend die Störung der Funktionsfähigkeit eines Computersystems nach § 126b StGB und den Missbrauch von Computerprogrammen oder Zugangsdaten nach § 126c StGB.

Von Bedeutung ist in diesem Zusammenhang auch die Bestimmung über Datenbeschädigung nach § 126a StGB und betreffend den betrügerischen Datenverarbeitungsmissbrauch nach § 148a StGB, beides Delikte, die den Hauptanwendungsfall in der Praxis darstellen, gefolgt vom Delikt nach § 118a StGB.

Schließlich ist auch der Tatbestand des Schweren Betruges nach § 147 Abs 1 Z 1 StGB, wenn zur Täuschung falsche oder verfälschte Daten benützt werden, in Betracht zu ziehen.

Neu ist auch in Entsprechung der Umsetzung der erwähnten Cyber-Crime-Konvention des Europarates die Bestimmung des § 225a StGB über Datenfälschung zur Ahndung der Fälschung von Computerdaten.

Im § 74 Abs 1 Z 8 StGB werden als Computersystem sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen, definiert

[1] Siehe *Fabrizy,* StGB[10] § 118a Rz 5.

und zwar auch im Wesentlichen entsprechend der erwähnten Cyber-Crime-Konvention des Europarates.

Wie sieht es nun in Österreich in der Praxis aus?

Nach der Beantwortung einer parlamentarischen Anfrage durch das Bundesministerium für Justiz waren in dem Bereich der §§ 118a, 119, 119a, 126a, 126b, 126c und 148a StGB in Österreich im Jahre 2009 insgesamt 565 Fälle und im Jahre 2010 insgesamt 907 Fälle zu verzeichnen, wovon etwa jeweils die Hälfte das Delikt des betrügerischen Datenverarbeitungsmissbrauchs nach § 148a StGB und etwa ein Drittel jenes über Datenbeschädigung nach § 126a StGB betraf. Zu Urteilen kam es im Jahre 2009 in 174 Fällen und im Jahre 2010 in 162 Fällen. Beachtlich erscheint die hohe Zahl der Einstellungen und sonstigen Beendigungen der Verfahren. Die meisten Anklagen und Urteile erfolgten sohin wegen der Delikte nach §§ 148a, 126a und 118a StGB; alle anderen oben angeführten Bestimmungen spielen eine eher geringe Rolle.

An dieser Stelle darf ich dem Herrn Leitenden Staatsanwalt Dr. Robert Jirovsky vom Bundesministerium für Justiz für die Überlassung des Datenmaterials recht herzlich danken.

Durch dieses erwähnte Zahlenmaterial erscheint auch die Kritik an der Unanwendbarkeit dieser angeführten speziellen Normen, wie sie Dr. Christian Bergauer in seinem Vortrag in Ottenstein im Jahre 2007 über „Viren, Würmer, Trojanische Pferde – Computerstrafrecht auf dem Prüfstand“ äußerte, weitgehend entkräftet.

Dennoch kann nicht oft genug gefordert werden, dass sich alle Bemühungen zunächst auf die Gewährleistung der Sicherheit eines freien Netzes, die Schaffung wirksamer gesetzlicher Bestimmungen und die Ausforschung der Täter sowie deren strafgerichtliche Verfolgung richten, wenn alle Präventivmaßnahmen nicht ausreichen.

Ich möchte mit einem Wort der Frau Bundesministerin für Inneres Johanna Mikl-Leitner schließen, die am 14.4.2012 sagte, dass zur Cyber Security als Ziel der Abwehrtechnologien gelte, zu verhindern, dass bei einem Cyberangriff in Österreich die Lichter ausgehen.

Mit unserem Symposium wollen wir einen Beitrag zur Erreichung dieses Zieles leisten, dass es nämlich in Österreich immer hell bleiben möge.

Wir dürfen sohin eine interessante Veranstaltung erwarten und ich bitte Sie schon jetzt um rege Diskussionsbeteiligung.

Ich danke Ihnen für Ihre Aufmerksamkeit und erteile nun das Wort Herrn Prof. Dr. Ernst Eugen Fabrizy.

Cyber-Security – Ein Thema, das uns alle angeht

Sektionschef Hermann Feiner
Bundesministerium für Inneres

Sehr geehrte Damen und Herren!

Die Sicherheit im virtuellen Raum ist eine der zentralen gesellschaftspolitischen Herausforderungen der nächsten Jahre.

Die Cyberwelt ist eine globale und ständig wachsende neue Wirklichkeit. Und weil dieser Raum von Menschen global

genutzt wird, verschwimmen öffentliche und private Verantwortlichkeiten.

Aus der Nutzersicht sehen wir in Bezug auf die Sicherheit in dieser virtuellen Welt, dass wir Menschen ein Sozialisierungsdefizit im Umgang mit diesen neuen Medien aufweisen: Viele Nutzer verhalten sich im Internet so, wie sie sich in der realen Welt nie verhalten würden.

Dazu eingangs einige Zahlen als Problemaufriss:

Probleme & Auswirkungen

- 750 Milliarden Euro Schaden pro Jahr weltweit
- 150 Milliarden US-Dollar Umsatzvolumen - mehr als durch Drogenhandel
- 150.000 Cyber-Angriffe pro Tag
- Steigerung der Anzeigen um das 6-fache in den letzten 10 Jahren

Konsequenzen

- Zahlreiche Regierungen (USA, Deutschland, UK, Australien) arbeiten an **Cyber Security Strategien** bzw deren Umsetzung.
- Dem Thema Cyber Security wird in der „Strategie für die innere Sicherheit der EU“ ein zentraler Stellenwert beigemessen.
- Das gilt auch für die neue Österreichische Sicherheitsstrategie.
- Das Thema wird sicherheitspolitisch immer relevanter und auch von den Medien breit diskutiert.
- Verschiedene öffentliche und nicht öffentliche Akteure sind gefordert. Dem BM.I kommt eine zentrale Verantwortlichkeit zu.

Themenmatrix

EU-Strategie innere Sicherheit (ISS)

- Folgende **Cyber-relevante Hauptbedrohungen** werden genannt:
  - **Terrorismus** in jeglicher Form *(ua Radikalisierung und Verbreitung von Propaganda über das Internet)*
  - **Cyberkriminalität** *("stellt als globale, technologische, grenzüberschreitende und anonyme Bedrohung unserer Informationssysteme die Strafverfolgungsbehörden vor zahlreiche zusätzliche Herausforderungen")*
  - **Gewalt** an sich *(Anm: betrifft ua auch Cyber Mobbing, Cyber Stalking)*

Handlungsschwerpunkte zur Umsetzung der EU-Strategie innere Sicherheit

1. Schwächung internationaler krimineller Netzwerke
2. Maßnahmen gegen Terrorismus, Radikalisierung und die Rekrutierung von Terroristen
3. **Besserer Schutz der Bürger und Unternehmen im Cyber Space**

4. Erhöhung der Sicherheit durch Maßnahmen an den Außengrenzen

5. **Verbesserung der Widerstandsfähigkeit Europas gegenüber Krisen und Katastrophen** (inkludiert **Cyberangriffe** auf kritische Infrastruktur)

Besserer Schutz der Bürger und Unternehmen im Cyber Space – geplante EU-Maßnahmen

1. Aufbau von Kapazitäten bei der Strafverfolgung und in der Justiz

   - Schaffung **EU-Zentrum für Cyberkriminalität** bis 2013

   - Einheitliche **Standards** und Einrichtung von **Exzellenzzentren** in den EU-Staaten

2. Zusammenarbeit mit der Industrie

   - Europäische **öffentlich-private Partnerschaft für Robustheit** (EP3R)

   - Maßnahmen zur Verbesserung der Sicherheit kritischer Infrastruktur, der Robustheit des Netzes und der Informationsinfrastruktur

   - „**Contact Initiative against Cybercrime for Industry and Law Enforcement**“

3. Verbessertes Reaktionsvermögen gegen Cyberangriffe

   - Vernetzung der nationalen CERT bis 2012

   - Schaffung **Europäisches Informations- und Warnsystem bis 2013**

Entwurf Österreichische Sicherheitsstrategie 2011

Sicherheitspolitische Werte, Interessen und Ziele (Auszug)

- Umfassender Schutz der Bevölkerung

- Stärkung der demokratischen Gesellschaft gegenüber extremistischen und fundamentalistischen Strömungen und Einflussnahmen

- Stärkung der Widerstandsfähigkeit des öffentlichen und privaten Sektors gegen natürliche oder von Menschen verursachte Störungen und Katastrophen

- Bekämpfung des internationalen Terrorismus, der Organisierten Kriminalität und Korruption

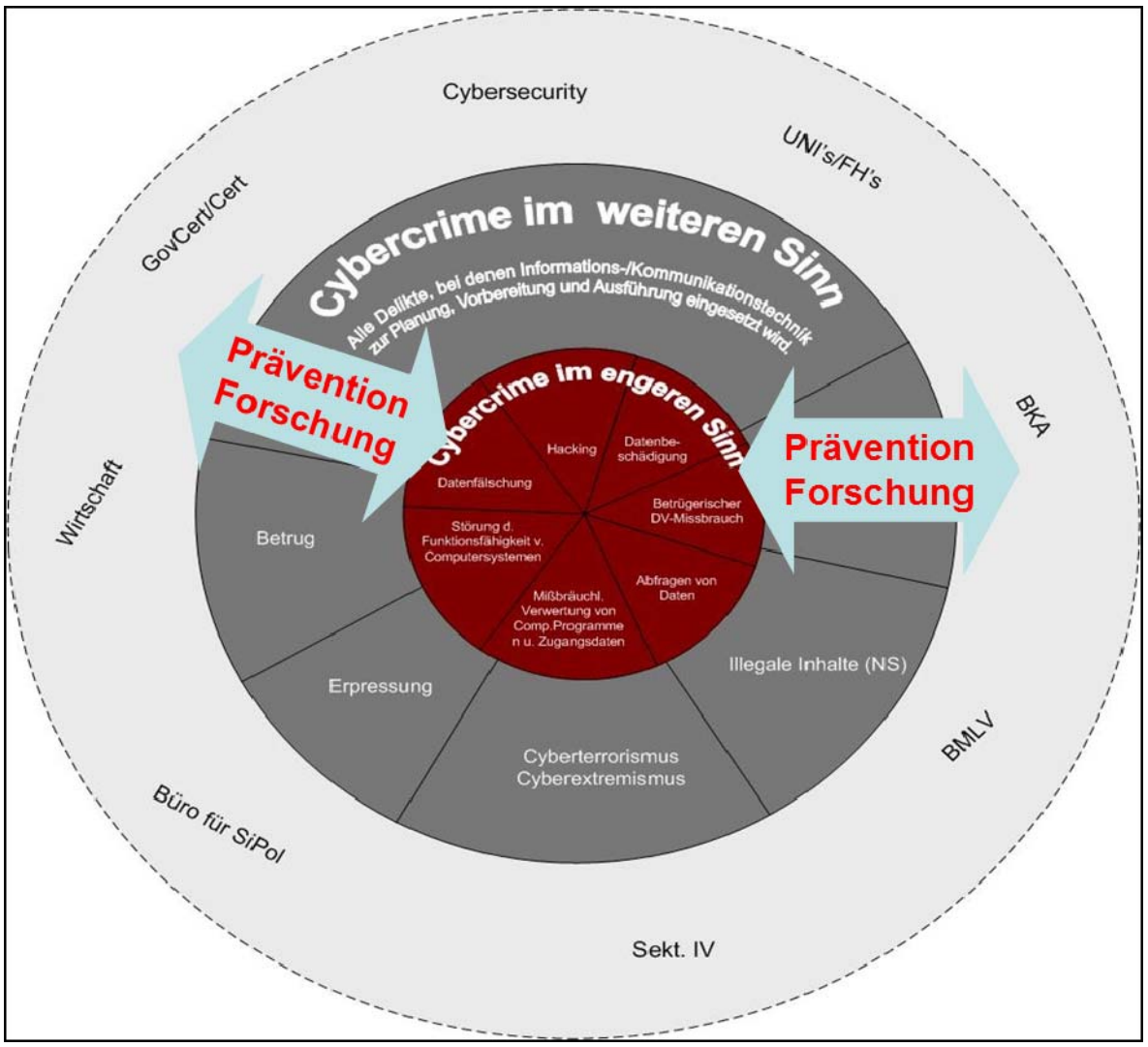
Sicherheitspolitik auf nationaler Ebene

Innere Sicherheit (Auszug):

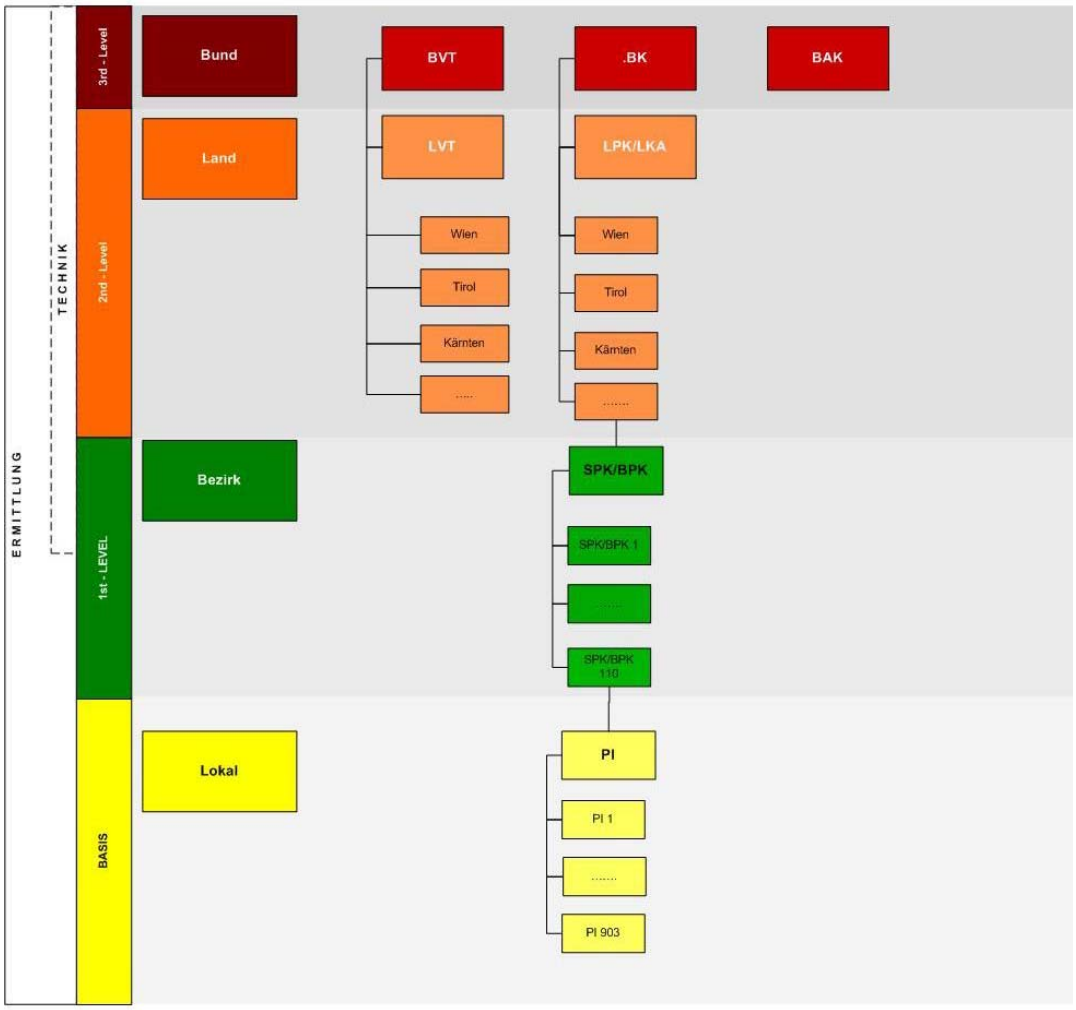
- „Kriminalität verändert sich laufend. Dies erfordert flexible Gegenstrategien. Neben den klassischen Herausforderungen der Massenkriminalität, der Gewalt gegen Leib und Leben und der Eigentumskriminalität, sind Phänomene wie die **Computer- und Netzwerkkriminalität,** Korruption und Wirtschaftskriminalität konsequent zu bekämpfen.“

- **„Cyberkriminalität, Cyber-Angriffe** oder der **Missbrauch des Internet für extremistische Zwecke** oder **Netzwerksicherheit** stellen besondere neue Herausforderungen für alle betroffenen Akteure dar und **erfordern ein breites Zusammenwirken im Rahmen eines Gesamtkonzepts.“**

Cybersecurity / Cybersafety / Cybercrime



CYBERCRIME – Organisationsstruktur (IST – STAND)



Derzeit befassen sich mit der Bekämpfung von Cybercrime rund 1000 Dienststellen österreichweit!

Alleine im Zentralstellenbereich sind derzeit mehr als 200 Personen in den verschiedensten OE mit dieser Thematik beschäftigt.

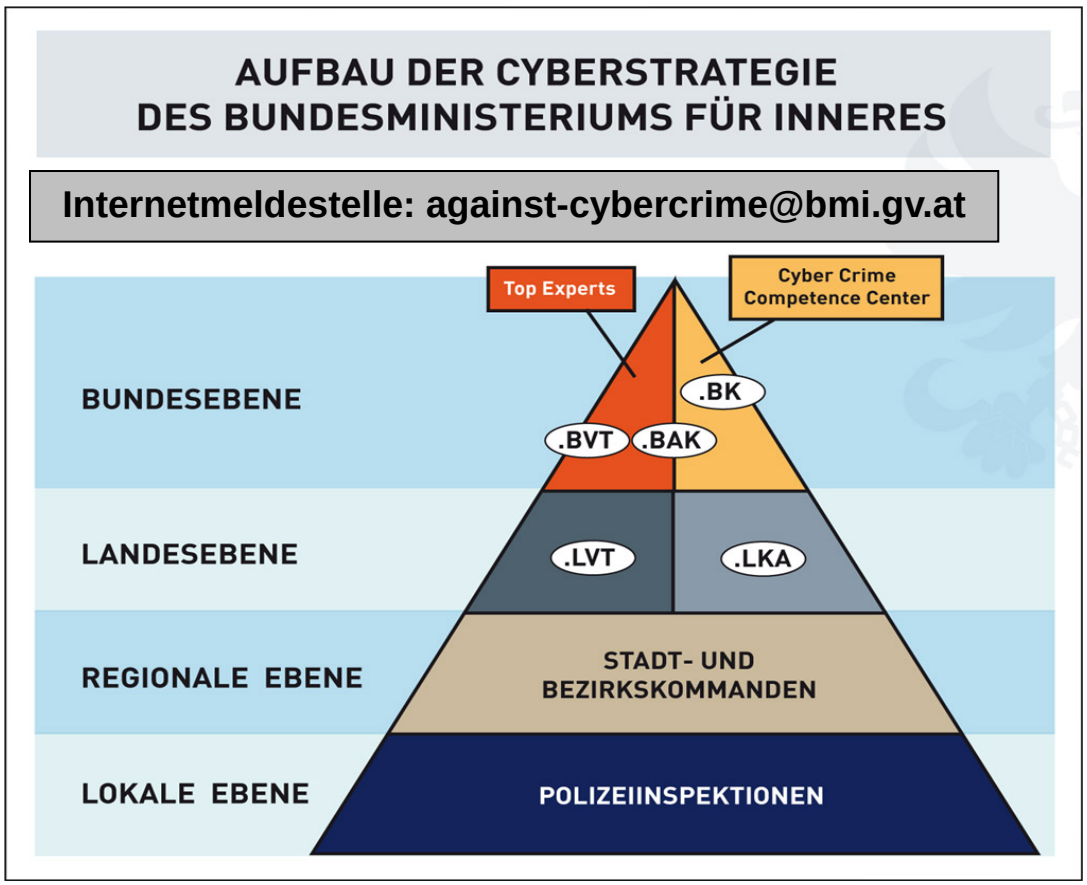
- 9 LPK/LKA
- 9 LVT
- 110 BPK/SPK
- 903 PI

Es gibt keine Gesamtstruktur (neg Auswirkungen):

- Doppelgleisigkeiten
- Know-How Defizite

- Ausbildungsdefizite
- zu viele Ansprechpartner
- mangelhafte Kompetenz vor Ort
- suboptimaler Ressourceneinsatz
- unklare Zuständigkeiten/Aufgabenverteilung

Strategie gegen Cybercrime



Ziele des „C4“- Projektes

- Etablierung im .BK (High Level Ermittlungs- und Supportebene – Sonderfall Black-Box-Staatsschutz)
- Klare Schnittstellendefinition zum Cyber-Security-Center (Sekt IV)

- Effiziente und effektive Aufbau- und Ablauforganisation (schnelle wirksame Intervention/Gefahrenbeendigung/ Ermittlung/Ausforschung)
- Know-How Konzentration
- Modernster technischer Level
- Kooperationsformen mit externen und internen Akteuren
- Rechtliche Ergänzungen und Anpassungen

Anlehnung an Best-Practice Modellen International

Belgien (10 Mio EW):
- Cyber Crime Unit
- 175 Beamte in der Zentralstelle + Regionale Büros

Frankreich (65 Mio EW):
- O.L.C.T.I.C. (Office Central de Lutte contre la Criminalitè lieè aux Techonolgies de l'Information et de le Communication)
- 80 Mitarbeiter in Zentralstellen + Regionale Büros

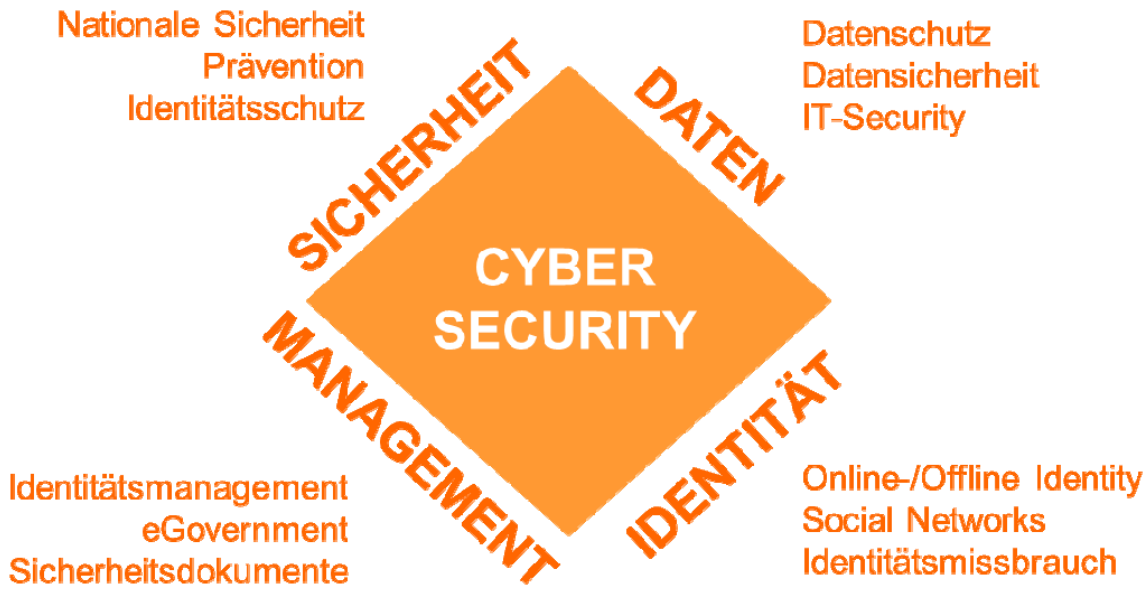
Deutschland (81 Mio EW):
- BKA KI 2 TESIT (Technisches Entwicklungs- und Servicezentrum, Innovative Technologien)
- 125 Mitarbeiter ohne Ermittlungsbereich

Hessen (6 Mio EW, vergleichbar mit Österreich):
- Zentralstelle zur Bekämpfung der Internetkriminalität im LKA Hessen
- 57 Planstellen + 9 Techniker

Projektfortschritt/Zeitleiste

Juni - August	September	ab Oktober
•Rohkonzept •Analyse Ressourcenbedarf •Einrichtung Meldestelle	•Fertigstellung Detailkonzept •Definition v. Musterprozessen •Fertigstellung Personaleinsatzkonzept	•Beginn der konkreten Umsetzungsschritte

Themenmatrix

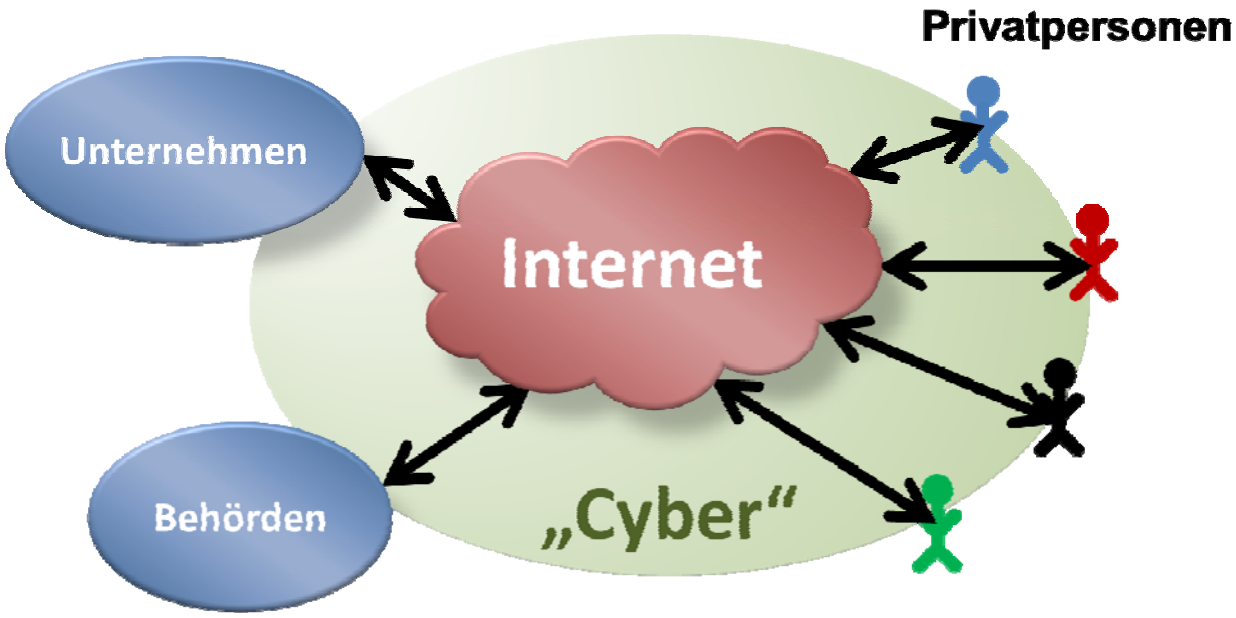


Cybersecurity

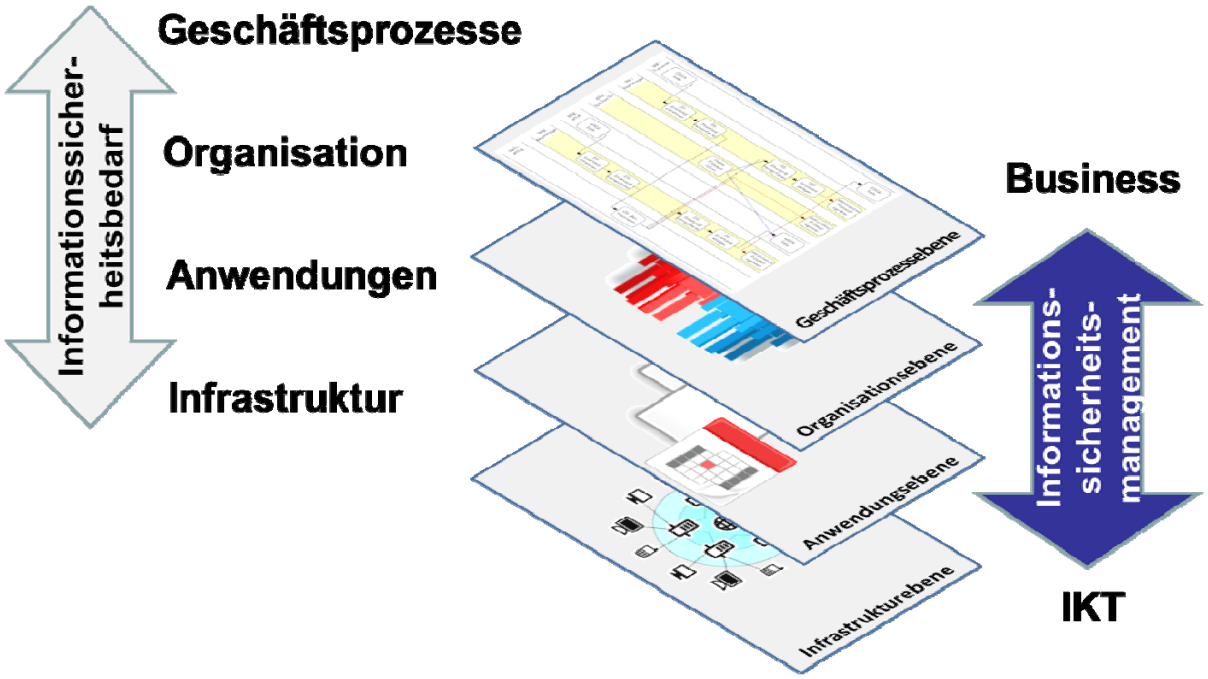
- Keine einheitliche, standardisierte Definition vorhanden
- Oft verwendeter Begriff für die Gewährleistung der sicheren aktiven und passiven Nutzung des Internets

- Sollte eigentlich mit dem Begriff Informationssicherheit (vgl ISO/IEC 27002) gleichgesetzt werden

Begriff „Cyber“



Informationssicherheit



Cybersecurity Einflussfaktoren

Technische

- Vernetzung der IT-Systeme
- Einsatz von System- bzw SW-Monokulturen
- Sicherheitslücken in Hardware und Software

Organisatorische

- Mangelndes Informationssicherheitsmanagement
- Fehlende Awareness
- Fehlendes Mitarbeiter Know-How

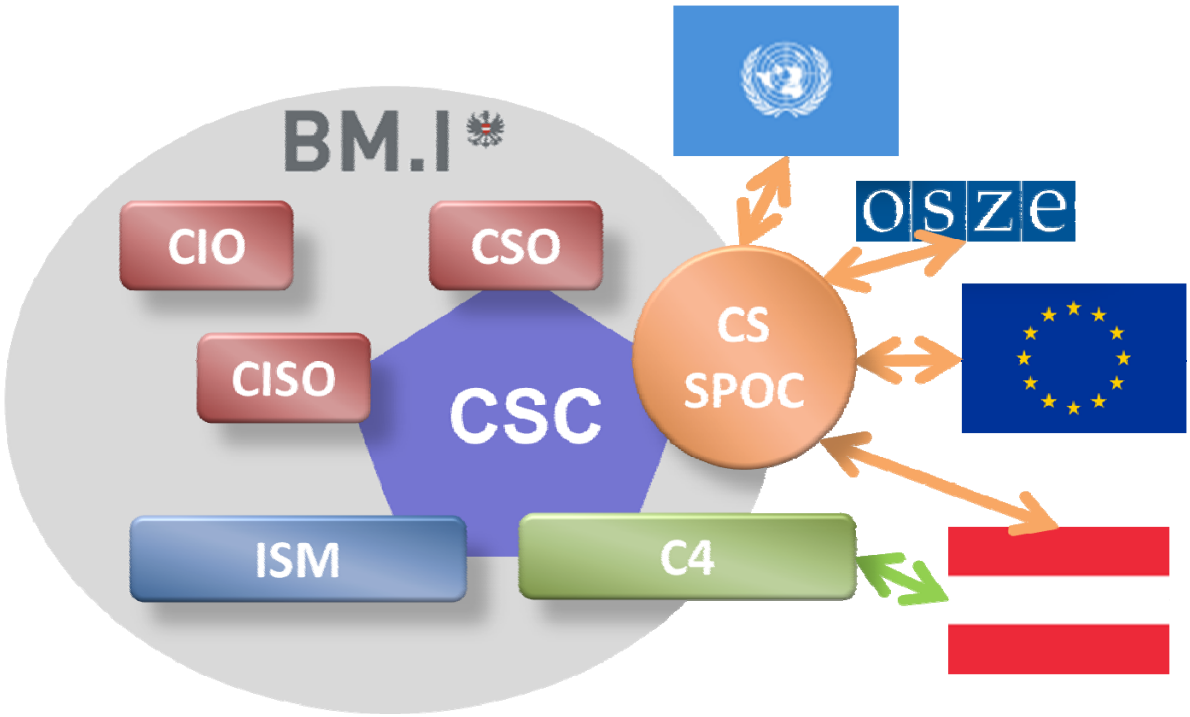
Ökonomische

- Kosteneffizienz als treibende Kraft
- Flexible und innovative Systeme und Anwendungen
- Sicherheitslücken in Hardware und Software
- Heterogene Supply Chain
- CIP und CIIP in privater Hand

Soziale

- Mensch als Bedrohung
- Subjektives Bedrohungs-/Sicherheitsgefühl
- Anonymität im Internet
- Mangelndes Unrechtbewusstsein

Cybersecurity im BM.I



Ziele und Strategien BM.I

- **Wahrnehmung eigener Verantwortlichkeiten** (Cybercrime, Terrorismus, BM.I-Netzwerksicherheit)
- **Ausbau von Know-how** und **Sensibilisierung von Behörden** und **Wirtschaft** (Bewusstseinsbildung, Vernetzung)
- **Proaktive Mitgestaltung** der gesamtstaatlichen **Strategie zu Cyber Security**
- **Proaktive Mitgestaltung** der **EU-Politik** zu Cyber Security

- Aufbau eines **Kompetenz-Clusters/ externen (internationalen) Expertennetzwerks**

BM.I: Cyber Security Aktivitäten

- Sicherheitskongress 2011 “Cyber Security - Cyber Crime” (31. 05. 2011)

- Einrichtung **Kompetenzcenter Cybercrime** (im .BK)

- **Forum Salzburg** 2011: Cyber Security gemeinsamer Schwerpunkt

- Einrichtung **Cybersecurity Center** (in der Sektion IV) KSÖ-Workshops: Erstellung **Cyber-Risikomatrix** (16. und 30. 08. 2011)

- Cyber Security Konferenz 20. 09. 2011: **Beitrag Strategieprozess**

- Enge **Zusammenarbeit mit relevanten Akteuren**

Cyber Crime – Herausforderungen in der Praxis

OStA Mag. Peter Gildemeister
Oberstaatsanwaltschaft Wien

1. Begriffsbestimmung

Was ist unter dem Begriff Cyber Crime in der Praxis zu verstehen? Was ist – im (scheinbaren) Gegensatz dazu – ein „klassisches Delikt“? Dies sind die ersten Fragen, die sich im Rahmen eines Symposiums zum Thema Cyber Crime aufdrängen.

Die Definition des Begriffs „klassisches Delikt“ scheint denkbar einfach. Unter diesen Begriff können zwanglos sämtliche strafbare Handlungen subsumiert werden, die ohne die Verwendung eines Computers oder technischer Methoden der Datenübertragung wie dem Internet begangen werden können. Dazu zählt zweifelsohne das Delikt des Betruges. Wird aber ein Betrug dann zu einem Cyber Crime, wenn die Geschäftsanbahnung und -abwicklung im E-Mail-Weg oder auf einer Online-Verkaufs-Plattform im Internet durchgeführt wird?

Die Definition des Begriffs Cyber Crime scheint dagegen wesentlich schwieriger. Handelt es sich hiebei um einen Überbegriff für sämtliche Delikte, bei denen Computer oder technische Methoden der Datenübertragung in irgendeiner Weise eine Rolle spielen? Wird ein Delikt bereits dadurch zum Cyber Crime, weil das Internet als bloßes Kommunikations- oder Publikationsmittel zum Einsatz kam? Liegt ein Cyber Crime dann vor, wenn ein Delikt ohne Verwendung eines Computers und / oder technischer Methoden der Datenübertragung an sich nicht verwirklichbar wäre? Oder handelt es sich bei einem Delikt erst dann um ein Cyber Crime, wenn es ohne Verwendung eines Computers und technischer

Methoden der Datenübertragung nicht begangen werden kann und darüber hinaus der Tatort ebenfalls in der elektronischen Welt (im „Cyber Space“) liegt?

Derartige dogmatische Begriffsbestimmungsversuche sind zwar möglicherweise im Rahmen eines Symposiums zum Thema Cyber Crime von Interesse, in der staatsanwaltschaftlichen Praxis sind sie jedoch ohne jegliche Bedeutung, solange sie nicht Fragen der behördeninternen Geschäftsverteilung berühren.

In der Praxis sind vielmehr jene Fragen relevant, die sich im Zusammenhang mit der Identifizierung des Täters sowie der Sicherung und Auswertung von Beweismitteln stellen, sobald ein Delikt unter Verwendung des Internets als Tatort und / oder technischer Methoden der Datenübertragung begangen wird, und zwar unabhängig davon, ob das Delikt dogmatisch als „klassisches Delikt“ oder als Cyber Crime einzuordnen wäre.

2. Erscheinungsformen in der Praxis

In der Praxis sind die Staatsanwaltschaften häufig mit strafbaren Handlungen konfrontiert, die dogmatisch grundsätzlich als „klassische Delikte“ einzuordnen wären, die jedoch durch die Umstände ihrer Begehung in die Nähe von Cyber Crime gerückt werden. Diese Delikte sind dadurch gekennzeichnet, dass für ihre Begehung an und für sich weder ein Computer noch das Internet oder technische Methoden der Datenübertragung benötigt werden. Der nahezu flächendeckende Anschluss der Bevölkerung an das Internet begünstigt jedoch die Täter bei der Begehung dieser Delikte durch:

- Vereinfachung der Kommunikationswege und Erhöhung der Geschwindigkeit der Kommunikation;

- erleichterter Zugang zu potentiellen Opfern durch größere Breitenwirkung;

- Nutzung des Internet als Publikationsort;

- Möglichkeiten zur Verschleierung der eigenen Identität.

Beispiele:

- Betrug (eBay und andere Verkaufsplattformen)

- Verbreitung von Kinderpornographie

- Verhetzung und Delikte nach dem Verbotsgesetz

- Straftaten mit terroristischem Hintergrund

- „Cyber Stalking“

Daneben ist die Praxis mit weiteren Delikten konfrontiert, die dogmatisch eher dem Bild eines „echten“ Cyber Crime entsprechen. Charakteristisch bei diesen Delikten ist, dass sie ohne Verwendung eines Computers und des Internets oder technischer Methoden der Datenübertragung als Tatmittel nicht begangen werden können. Der Begriff Computer ist in diesem Zusammenhang nicht eng auszulegen, sondern als Oberbegriff auch für andere Geräte zur Datenspeicherung und Datenverarbeitung zu verstehen, die in der Lage sind, eine Verbindung mit dem Internet herzustellen (zB Smartphones, Tablets, Spielkonsolen etc).

Beispiele:

- Phishing (E-Mail-Phishing, Trojaner-Phishing);

- Angriffe auf Daten- und Computersysteme (Hacking, Denial-of-service, Kaperung fremder Internetseiten, ua)

3. Herausforderungen für die Strafverfolgungsbehörden

Die Aufklärung strafbarer Handlungen, die unter Verwendung des Internet und / oder technischer Methoden der Datenübertragung begangen werden, stellt die Strafverfolgungsbehörden vor zahlreiche Herausforderungen, und zwar unabhängig davon, ob es sich um „klassische Delikte“ oder „echte“ Cyber Crime handelt:

a.) Möglichkeiten zur Verschleierung der eigenen Identität durch den Täter

Es gibt zahlreiche (auch legale) Möglichkeiten, anonym bzw scheinbar anonym im Internet zu kommunizieren oder andere Tätigkeiten zu entfalten, Daten für den Abruf durch Dritte bereit zu halten und Inhalte zu publizieren.

Von zahlreichen Unternehmen werden kostenlos E-Mail-Dienste oder sonstige Kommunikationsdienste, Online-Speicherplätze für Daten und Speicherorte für Internetseiten angeboten, die eine ungeprüfte Registrierung des Benutzers mit Fantasiedaten zulassen. Im Rahmen eines Strafverfahrens ist es zwar möglich, auf die Registrierungsdaten zuzugreifen. Wenn diese jedoch ein Ergebnis wie „Max Mustermann, geboren und wohnhaft auf dem Planeten Erde“ ergeben, sind sie als weiterer Ermittlungsansatz wertlos.

Damit sich ein Täter für diese Dienste registrieren bzw diese in der Folge auch nutzen kann, muss er jedoch mit dem Anbieter der Dienste jeweils über das Internet eine Verbindung herstellen. Zu diesem Zweck wird dem internetfähigen Endgerät des Täters von einem Anbieter von Internet-Zugangsdiensten eine IP-Adresse zugewiesen, die wiederum vom Anbieter der Gratisdienste gespeichert werden kann. Auch bei anderen Tätigkeiten im Internet wie zB einem Hacking-Angriff kann der Täter beim Opfer Spuren in Form seiner IP-Adresse hinterlassen. Gelingt es im Zuge des Ermittlungsverfahrens, die IP-Adresse des Täters zu ermitteln, ist es im Wege des § 76a

StPO grundsätzlich möglich, über den Anbieter des Internet-Zugangsdienstes die wahre Identität des Täters auszuforschen. Je nachdem ob es sich um eine statische oder dynamische IP-Adresse handelt, sind § 76a Abs 1 StPO oder § 76a Abs 2 Z 1 StPO anzuwenden.

Der zuvor genannte, oftmals einzige Weg der Identifizierung des Täters über die IP-Adresse ist in der Praxis jedoch häufig mit Hürden versehen, die teilweise nahezu unüberwindlich sind:

- es gibt technische Möglichkeiten, die eigene IP-Adresse zu verschleiern, zu fälschen bzw gänzlich zu unterdrücken (zB Verwendung von Proxy-Servern oder eines TOR-Netzwerkes zur Anonymisierung von Verbindungsdaten). Anleitungen für derartige Maßnahmen sind leicht im Internet zu finden;

- nicht alle Anbieter von Internet-Zugangsdiensten sind verpflichtet, die IP-Adresse eines Benutzers aufzuzeichnen (kleine Anbieter, die nicht der Pflicht zur Vorratsdatenspeicherung unterliegen; kostenlose WLAN-Hotspots, Internet-Cafés, ua);

- es besteht die (nicht legale) Möglichkeit, ungesicherte private WLAN-Zugänge zu nutzen bzw gesicherte private WLAN-Zugänge zu hacken und dann zu nutzen. Private WLAN-Router protokollieren nämlich aufgrund ihrer Standardkonfiguration in der Regel nicht die Identifikationsnummern jener Endgeräte, die über sie eine Verbindung zum Internet herstellen;

- bei der Nutzung eines mobilen Internetzuganges wird nicht von allen Anbietern dem jeweiligen Endgerät eine eigene dynamische IP-Adresse zugewiesen, sondern es wird (legal) eine einzige dynamische IP-Adresse gleichzeitig bis zu mehreren tausend Endgeräten über (nicht protokollierte) Ports zugeordnet (NAT-PAT-Events – siehe auch die diesbezügliche Ausnahmebestimmung in § 76a Abs 2 Z 1 StPO);

- auch mit anonymen prepaid-SIM-Karten können über Mobiltelefone oder Datensticks Verbindungen in das Internet hergestellt werden; in diesem Fall geht eine Anfrage gemäß § 76a StPO grundsätzlich ins Leere.

b.) Grenzenloses Internet vs nationalstaatliche Grenzen

Während auf der einen Seite das Internet die Welt zum sprichwörtlichen „globalen Dorf“ gemacht hat, in dem es ohne Bedeutung ist, wo Daten oder Internetseiten gespeichert sind oder wo sich die Teilnehmer eines Kommunikationsvorganges bzw Angreifer auf ein Daten- oder Computersystem befinden, enden auf der anderen Seite die eigenen Ermittlungsmöglichkeiten der Strafverfolgungsbehörden grundsätzlich weiterhin an den nationalstaatlichen Grenzen. Außerhalb der nationalstaatlichen Grenzen können Ermittlungshandlungen nur im Rechtshilfeweg erwirkt werden. Rechtshilfeersuchen können jedoch bereits innerhalb der Europäischen Union zu einer erheblichen Erschwerung oder Verzögerung der Ermittlungstätigkeit führen, je nachdem welcher Staat um Mithilfe ersucht wird. Rechtshilfeersuchen in außereuropäische Länder sind darüber hinaus oftmals nicht wirklich erfolgversprechend. Darüber hinaus ist zu beachten, dass nicht in allen Ländern gleiche rechtliche Möglichkeiten zur Durchführung einzelner Ermittlungshandlungen bestehen.

Gerade in Phishing-Fällen, bei Propagandadelikten und in Fällen von Kinderpornographie hat es sich in der Praxis herausgestellt, dass die Angriffe im Wesentlichen vom Ausland ausgingen bzw die Inhalte auf ausländischen Servern gespeichert waren, was die Aufklärung der Straftaten wesentlich erschwert bzw in Phishing-Fällen fast ausschließlich verhindert hat.

c.) Ressourcen der Strafverfolgungsbehörden

Neben den zuvor genannten Schwierigkeiten sind Ermittlungsverfahren zur Aufklärung von Cyber Crime auch auf mehreren Ebenen ressourcenintensiv.

Sobald im Ermittlungsverfahren die Einbindung eines Anbieters erforderlich ist, entstehen Kosten, deren Höhe davon abhängt, welche Überwachungsmaßnahmen für welche Dauer durchzuführen sind.

Wenn schließlich die für das Ermittlungsverfahren notwendigen Daten sichergestellt sind, bedarf es deren Auswertung. Insbesondere in Fällen von Kinderpornographie fallen in der Regel sehr große Datenmengen an, deren Auswertung vor allem die Kriminalpolizei vor große Probleme stellt. Zum einen ist die Auswertung sehr zeitintensiv, zum anderen sind die personellen Kapazitäten begrenzt, weil für derartige Ermittlungshandlungen neben allgemeiner kriminalistischer Erfahrung in der Regel auch ein gewisses technisches Grundverständnis erforderlich ist. Der Staatsanwalt kann im Ermittlungsverfahren zwar auch externe Sachverständige beiziehen, deren Einsatz ist aber vor allem bei der Auswertung großer Datenmengen sehr teuer.

In der Praxis bedeutet aber nicht nur die schiere Menge der Daten sondern auch deren Struktur eine Herausforderung. So erfordert deren Auswertung häufig nicht nur eine geeignete Software, die überhaupt erst den Zugang zu den möglicherweise sogar verschlüsselten Daten ermöglicht, sondern auch entsprechend geschulte Ermittler zur Bedienung der Software.

Gerade die Geschwindigkeit des technischen Fortschritts und die Möglichkeiten zu dessen deliktischer Nutzung stellen die Strafverfolgungsbehörden immer wieder aufs Neue vor große Herausforderungen nach dem „Igel-Hase-Muster“.

Sobald die kriminalpolizeilichen Ermittlungen abgeschlossen sind und der Abschlussbericht vorliegt, liegt es am einzelnen Staatsanwalt, die rechtlich richtigen Schlüsse zu ziehen. Gerade in Fällen von Cyber Crime wäre es hilfreich, neben einer fundierten juristischen Ausbildung auch über ein technisches Grundverständnis zu verfügen, dessen Vermittlung jedoch nicht Gegenstand der herkömmlichen Ausbildung eines Staatsanwaltes ist.

d.) Rechtliche Aspekte

Sowohl die einschlägigen Bestimmungen des StGB als auch der StPO bilden grundsätzlich eine geeignete Reaktionsgrundlage auf unterschiedliche Ausformungen von Cyber Crime.

Hiebei fällt jedoch bei den Normen des materiellen Strafrechts auf, dass zum einen teilweise Ermächtigungsdelikte vorliegen und zum anderen die relevanten Tatbestände teilweise (Grund-)Strafdrohungen in einem Rahmen aufweisen, der einen Einsatz der Ermittlungsmethoden des § 134 Z 2 bis 4 StPO verhindert. Hiebei handelt es sich jedoch um rechtspolitische Entscheidungen, die von den Strafverfolgungsbehörden in der gegebenen Form in der Praxis umzusetzen sind.

Im formellen Strafrecht ist seit 01.04.2012 neben der Auskunft über Vorratsdaten vor allem die Auskunft über Stamm- und Zugangsdaten gemäß § 76a StPO von Bedeutung, die eine ältere Bestimmung des Telekommunikationsgesetzes ersetzt. Hiebei fällt bei der Anwendung des § 76a Abs 2 StPO in der Praxis eine erhebliche Erschwernis im Vergleich zur früheren Rechtslage auf:

Während seit 01.04.2012 die Staatsanwaltschaften eine ausformulierte und begründete Anordnung mit Angaben zu Tatverdacht, Zweckmäßigkeit und Verhältnismäßigkeit erlassen müssen, genügte davor – in Übereinstimmung mit der Rechtsprechung des Obersten Gerichtshofes – ein formloses

und nicht begründetes Ersuchen. Darüber hinaus unterliegen Anordnungen gemäß § 76a Abs 2 StPO immer einer Revision gemäß § 5 Abs 5 StAG, was insbesondere in dringenden Journalfällen am Wochenende zu Erschwernissen bzw Verzögerungen führen kann.

4. Fazit

Die durch den technischen Fortschritt entstehenden Möglichkeiten, diesen zu deliktischem Verhalten zu missbrauchen, stellen die Strafverfolgungsbehörden nicht nur vor rechtliche, sondern vor allem auch vor große ermittlungstechnische Herausforderungen. Insbesondere durch die zahlreichen Möglichkeiten, seine Identität als Täter nicht nur vor dem Opfer, sondern auch vor den Ermittlungsbehörden zu verschleiern, steht die Gesellschaft vor dem Phänomen, dass es Tätern mit ausreichendem technischen Wissen zumindest temporär gefahrloser möglich ist, Straftaten im Cyber Space denn in der „realen Welt“ zu begehen.

Zahnloses Cyberstrafrecht? – Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz

Univ.-Ass. Mag. Dr. Farsam Salimi
Universität Wien

A. Einleitung

Cyberkriminalität ist in aller Munde. In einer Mitteilung der Kommission über Cyberkriminalität ist von einem weltweiten Schaden von rund 388 Milliarden EUR im Jahr die Rede, womit die Cyberkriminalität einträglicher wäre als der gesamte weltweite Handel mit Marihuana, Kokain und Heroin zusammen.[2] Die Bedrohungen durch Cyberangriffe betreffen nicht nur das Vermögen oder die Funktionsfähigkeit von Computersystemen, sondern auch die Sicherheit und Geheimhaltung unserer Daten im Netz. Auf diesen Bereich will ich meine Ausführungen konzentrieren. In letzter Zeit wurde vermehrt darüber diskutiert, wie man Cyberattacken durch erhöhte Sicherheitsmaßnahmen im Netz präventiv begegnen kann (dabei spielen Fragen der Cyber-Security ebenso eine Rolle wie Fragen sicherheitspolizeilicher Ermittlungsbefugnisse). Ich will primär darauf eingehen, ob die Tatbestände des materiellen Strafrechts ausreichend Reaktionsmöglichkeiten des Staates auf von uns als strafwürdig angesehene Cyberattacken bilden. Ich nehme das Ergebnis gerne vorweg: Ich sehe im materiellen Strafrecht einige Lücken!

[2] Mitteilung der Kommission an den Rat und das Europäische Parlament, Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität; 28. 03. 2012 COM(2012) 140 final, mVa *Norton Cybercrime Report* 2011, http://de.norton.com/cybercrimereport/promo, Zugriff am 12. 04. 2012.

B. Zur Strafbarkeit der „Cyberattacke“ – Lücken in § 118a StGB

Das materielle Strafrecht schützt unsere Daten indirekt dadurch, dass es die widerrechtliche Zugangsverschaffung zu einem fremden Computersystem unter Strafe stellt. Damit werden freilich auch die dort gespeicherten Daten geschützt. Allgemein bekannt sind solche Verhaltensweisen als „Hacking“. Viele würden kaum daran zweifeln, dass „Hacking“ ein strafbares Verhalten ist. Nach geltendem Recht bleibt Hacking allerdings weitgehend sanktionslos.

So etwa auch folgendes Beispiel:

Ein Hacker verschafft sich nach Überwindung des Sicherheitssystems Zugang zu Ihrem PC, der dann in einem weiteren Schritt ohne Ihr Wissen – quasi ferngesteuert – für die Verbreitung von Links zu kinderpornographischem Material verwendet werden soll. (Bei Fernsteuerung mehrerer Systeme spricht man von einem „Botnetz“.)[3]

Das im März 2011 entdeckte und stillgelegte Botnetz „Rustock“ umfasste etwa 1 Million infizierte PCs, die in erster Linie zur Versendung von Spam-Mails genutzt wurden.[4] Die Verschaffung des Zugangs zu diesen PCs ist derzeit nicht nach § 118a strafbar. Das liegt nicht am objektiven Tatbestand. Dieser umschreibt das, was üblicherweise als „Hacking“ verstanden wird, nämlich die Zugangsverschaffung zu einem Computersystem, über das der Täter nicht allein verfügen darf, durch Überwindung einer spezifischen Sicherheitsvorkehrung. Die **Schwachstellen des § 118a** liegen im **subjektiven Tatbestand**. Dieser verlangt neben dem Tatbildvorsatz die Absicht, sich oder einem anderen Unberechtigten von im System abgespeicherten und nicht für ihn bestimmten Daten

[3] Der Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, 30. 09. 2010 KOM(2010) 517 endg sieht in Art 10 Abs 2 die Verpflichtung der Mitgliedstaaten die Benützung eines solchen Botnetzes für Hacking-Angriffe als erschwerenden Umstand zu behandeln vor.

[4] http://www.heise.de/security/meldung/Rustock-Botnetz-ausser-Gefecht-1210310.html abgerufen am 12. 04. 2012.

Kenntnis zu verschaffen und dadurch, dass er diese Daten selbst benutzt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Vorausgesetzt sind somit **Spionageabsicht**, **Benutzungs- oder Verbreitungsabsicht und Bereicherungs- oder Schädigungsabsicht**. Bereits an der Spionageabsicht kann es mangeln: So etwa im Eingangsbeispiel, in dem der Täter das fremde Computersystem nur als Tatwerkzeug verwenden will, sich für die darin gespeicherten Daten aber gar nicht interessiert. Die Absichtsformen müssen darüber hinaus kumulativ vorliegen. Auch daran wird es in vielen Fällen scheitern: Will sich der Täter etwa nur Kenntnis von den Daten verschaffen (reine Spionageabsicht), scheidet § 118a aus. Zudem muss für § 118a die Absicht bestehen, die Vorteilsgewinnung bzw Schädigung gerade *durch die Datenbenützung* zu erreichen („dadurch, dass“).

Hier stellt sich die Frage, was unter „Benützen“ der Daten zu verstehen ist. Die Formulierung orientiert sich nach den EBRV an § 51 DSG[5] – eine Bestimmung, die mE denkbar ungeeignet ist, als Vorbild für andere Straftatbestände herzuhalten, zumal auch dort der Begriffsinhalt des Benützens nicht geklärt ist (dazu näher unter C.).

Jedenfalls kein „Benützen“ ist das **Löschen** der Daten. Verschafft sich somit jemand mit der Absicht Zugang zu einem System, um diese Daten auszuspähen (Spionageabsicht) und diese dann zu beschädigen, zu löschen oder unbrauchbar zu machen, ist dies de lege lata nicht gem § 118a strafbar. Das Problem wird zwar dadurch entschärft, dass in solchen Fällen eine Strafbarkeit wegen Datenbeschädigung, allenfalls in Versuchsform, in Frage kommt. Dennoch: Der Unwert des Eindringens in ein System wird durch eine Strafbarkeit nach § 126a nicht erfasst. Einen sachlichen Grund, die

[5] EBRV StRÄG 2002, 1166 BlgNR 21. GP 24.

Löschungsabsicht anders zu behandeln als die Benutzungsabsicht, sehe ich nicht.

Doch wie steht § 118a in seiner derzeitigen Form zu den internationalen und europäischen Vorgaben?

§ 118a wurde durch das StRÄG 2002[6] in Umsetzung des **Art 2 der Convention on Cybercrime** des Europarates vom 23. 09. 2001[7] (CyCC) („illegal access“) eingeführt.[8] Dieser sieht die Möglichkeiten vor, die Strafbarkeit auf subjektiver Ebene auf solche Fälle einzuschränken, in denen „intent of obtaining computer data or other dishonest intent“ vorliegt. Die Formulierung könnte zwar auch als Beschreibung einer Alternative verstanden werden[9], im *explanatory report* ist jedoch klargestellt, dass die Vertragsstaaten die subjektiven Schranken auch kumulativ vorsehen können.[10] Das in § 118a vorgesehene dreifache Absichtserfordernis ist daher wohl mit dieser Vorgabe vereinbar.

Aus **Art 2 des Rahmenbeschlusses des Rates über Angriffe auf Informationssysteme**[11] kann für die Frage des subjektiven Tatbestands wenig gewonnen werden: Die Mitgliedstaaten sind verpflichtet, vorsätzliche Hacking-Angriffe zumindest dann unter Strafe zu stellen, wenn kein „leichter Fall vorliegt“. Art 3 des zurzeit in Verhandlung befindlichen RL-Entwurfes der Kommission ist gleichlautend.[12] Nach dem Verständnis des österreichischen Gesetzgebers sind alle Verhaltensweisen, die nicht alle in § 118a vorgesehenen subjektiven Voraussetzungen

---

6 BGBl I 2002/134.

7 Council of Europe, European Treaty Series No 185.

8 Vgl auch *Reindl,* E-Commerce und Strafrecht 147.

9 *Beer,* Die Convention on Cybercrime und österreichisches Strafrecht 125 nimmt Konventionswidrigkeit an.

10 Convention on Cybercrime, ETS No 185, Explanatory Report, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, abgerufen am 12. 04. 2012; so auch *Schuh,* Computerstrafrecht im Rechtsvergleich 77.

11 RB 2005/222/JI des Rates vom 24. 02. 2005, ABl L 69/67.

12 Vgl Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, 30. 09. 2010 KOM(2010) 517 endg.

erfüllen, als leichte Fälle einzustufen.[13] Das kann man durchaus so sehen.

Insgesamt lässt sich festhalten: Der Tatbestand des § 118a ist mit den internationalen Vorgaben vereinbar.

Österreich hat sich hinsichtlich der Strafbarkeit des Hackings aber für die Minimallösung entschieden. Im ME zum StRÄG war kein solcher erweiterter Vorsatz vorgesehen.[14] Erst nach Anregungen im Begutachtungsverfahren bekam der subjektive Tatbestand seine jetzige Form.[15] Die Materialien halten fest, dass die Strafbarkeitsschwelle des § 118a „auf den ersten Blick relativ hoch" erscheine. „Vor dem Hintergrund der Möglichkeiten, die die Umsetzung der Cyber-Crime-Konvention allem Anschein nach bietet und der derzeit noch ungleich höheren Schwelle für strafgerichtlichen Datenschutz" erscheine aber die Vorgangsweise „vertretbar".[16] Doch sind diese Hürden in Zeiten der von allen Seiten betonten verstärkten Bekämpfung von Cybercrime noch sachgerecht? Zwischen dem gänzlichen Verzicht auf einen erweiterten Vorsatz im ME und der schließlich beschlossenen Dreifachabsicht liegt ein weiter Spielraum. ME ist das Unrecht des vorsätzlichen Eindringens in ein gesichertes System bereits für sich strafwürdig. Im Detail sprechen mE folgende Punkte dafür, die im Laufe der Gesetzwerdung eingefügten subjektiven Schranken zumindest zT wieder herabzusetzen:[17]

a) Hacking als „Elektronischer Hausfriedensbruch"

Hacking wird oft als elektronischer Hausfriedensbruch bezeichnet.[18] In Zeiten der zunehmenden Digitalisierung des Privat- und Geschäftslebens kann man durchaus eine solche Parallele zwischen realer und digitaler Welt ziehen. Das

---

13 EBRV StRÄG 2008, 285 BlgNR 23. GP 7.
14 308/ME zum StRÄG 2002, 21. GP.
15 EBRV StRÄG 2002, 1166 BlgNR 21. GP 24.
16 EBRV StRÄG 2002, 1166 BlgNR 21. GP 25.
17 Kritisch aus rechtsvergleichender Sicht auch *Schuh* Computerstrafrecht im Rechtsvergleich 83.
18 *Ernst*, Hacker und Computerviren im Strafrecht, NJW 2003, 3236; *Dietrich*, Die Rechtsschutzbegrenzung auf besonders gesicherte Daten des § 202a StGB; NStZ 2011, 249.

Eindringen in eine Wohnstätte mit Gewalt gem § 109 Abs 1 ist strafbar, ohne dass es für das Grunddelikt auf einen weiteren Vorsatz ankäme. Das entspräche beim virtuellen Hausfriedensbruch der unbefugten Zugangsverschaffung unter Überwindung einer Sicherheitsvorkehrung.

b) Der Vergleich mit verwandten Straftatbeständen des österreichischen Strafrechts

Vergleicht man § 118a mit anderen, schon vor dem StRÄG 2002 enthaltenen verwandten Delikten, ergibt sich folgendes Bild: Die Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses nach § 123 StGB verlangt lediglich den Vorsatz, das Geheimnis zu verwerten, Dritten zu überlassen oder der Öffentlichkeit preiszugeben. Absicht ist gar nicht gefordert. In den Gesetzesmaterialien zu § 118a werden die im darin vorgesehenen hohen subjektiven Anforderungen damit begründet, dass § 118a im Gegensatz zu § 51 DSG[19] und § 123 StGB keine spezielle Datenkategorie, spezielle Geheimnisse oder den Inhalt von Nachrichten schütze, sondern allgemein Daten.[20] Dies ist zwar zutreffend, übersieht aber, dass in § 118a im Ausgleich für diese Weite der vor Zugriff geschützten Daten eine hohe Anforderung bei der Tathandlung, nämlich die Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem vorgesehen ist. § 123 verlangt demgegenüber keine spezielle, mit krimineller Energie verbundene Handlungsweise; es muss kein spezifisches Sicherheitssystem überwunden und auf ein fremdes System zugegriffen werden. Der besonderen Schutzwürdigkeit des Zielobjekts bei § 123 ist die speziell vorgesehene Tatmodalität des § 118a gegenübergestellt. Insofern gleichen sich die objektiven Voraussetzungen mE wertungsmäßig aus, sodass ein Vergleich der subjektiven Voraussetzungen durchaus zulässig erscheint.

---

19 Zu beachten ist, dass durch die DSG-Novelle 2010 die subjektiven Voraussetzungen des § 51 DSG herabgesetzt wurden und seitdem § 51 DSG anders als § 118a nicht mehr als Ermächtigungsdelikt ausgestaltet ist; kritisch zur Konstruktion des § 118a als Ermächtigungsdelikt: *Beer,* Die Convention on Cybercrime 125 f.

20 EBRV StRÄG 2002, 1166 BlgNR 21. GP 24.

Dasselbe Bild ergibt sich bei einem Vergleich mit § 118, der Verletzung des Briefgeheimnisses und mit § 119, der Verletzung des Telekommunikationsgeheimnisses. Bei wertungsmäßig vergleichbaren objektiven Tatbestandsvoraussetzungen stellen diese durchwegs geringere Anforderungen an den Vorsatz.

c) Rechtsvergleichende Aspekte

Der Befund einer zu rigiden subjektiven Tatseite wird auch durch einen Blick auf die vergleichbare Bestimmung des deutschen Strafrechts bestärkt: Hacking wird dort durch **§ 202a dStGB** erfasst.[21] Danach macht sich strafbar, „wer unbefugt sich oder einem Dritten Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft". Während der objektive Tatbestand weitgehend mit jenem des § 118a vergleichbar ist, verlangt der subjektive Tatbestand nichts weiter als den bedingten Tatbildvorsatz.[22]

d) Beweisschwierigkeiten

Es liegt auf der Hand, dass eine neben dem Tatbildvorsatz erforderliche, dreifache Innentendenz des Täters auf der Intensitätsstufe der Absichtlichkeit im Strafverfahren sehr oft nicht nachweisbar sein wird. Schon allein dieser Umstand führt zur praktischen Nicht-Anwendbarkeit des Tatbestands.[23]

---

21 Vgl *Bosch* in *Satzger/Schmitt/Widmayer* § 202a Rz 1; *Hilgendorf/Frank/Valerius* Computer- und Internetstrafrecht 647 ff; *Schuh* Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz 49 ff; *Herzog* Straftaten im Internet, Computerkriminalität und die Cybercrime Convention, *Polít. crim.*, Vol 4, Nº 8 (12/2009), Doc 1, pp 475-484 (1-10), http://www.politicacriminal.cl/Vol_04/n_08/Vol4N8D1.pdf, abgerufen am 12. 04. 2012.

22 *Schünemann,* LK[12] § 202a Rz 7; *Bosch* in *Satzger/Schmitt/Widmayer* § 202a Rz 8; *Krutisch,* Strafbarkeit des unberechtigten Zugangs zu Computerdaten und -systemen 128.

23 Ebenso *Schuh,* Computerstrafrecht im Rechtsvergleich 83; *Krutisch* Strafbarkeit des unberechtigten Zugangs zu Computerdaten und -systemen 218.

e) Der kriminalpolitische Aspekt

In Zeiten der verstärkten Gefahr von Cyberattacken sollte zur stärkeren Präventionswirkung die mit krimineller Energie erfolgte Zugangsverschaffung zu einem gesicherten Computersystem zu strafrechtlicher Sanktion führen, ohne dass dafür fast unüberwindbare subjektive Hürden aufgebaut werden. Eine Bestimmung, die weitgehend unanwendbar bleibt, kann keine ausreichende abschreckende Wirkung entfalten.
Eine Herabsetzung der subjektiven Schranken des § 118a wäre daher mE sachgerecht, wobei sich folgende Vorgangsweisen anbieten:

1) Es wäre denkbar, – wie noch im ME zum StrÄG 2002 oder im deutschen Strafrecht – auf den erweiterten Vorsatz gänzlich zu verzichten.

2) Alternativ dazu könnte das Gesetz die Zugangsverschaffung mit **reiner Spionageabsicht** ausreichen lassen. Es wären damit nur jene Hacker von der Strafbarkeit ausgenommen, die lediglich Schwachstellen in Systemen aufzeigen oder die ihre technischen Fähigkeiten austesten wollen.

3) Als dritte Alternative wäre es denkbar, den erweiterten Vorsatz des § 118a auf die **Absicht** zur **Kenntniserlangung und auf Benützung, Zugänglichmachen oder Veröffentlichen** der Daten einzuschränken. Dies entspräche – abgesehen vom Absichtserfordernis – § 123, wonach der Vorsatz ausreicht, die Daten zu „verwerten, einem anderen zur Verwertung zu übergeben oder der Öffentlichkeit preiszugeben“.

4) Weiters wäre zu überlegen, alternativ zur Benützungsabsicht auch die **Löschungsabsicht** ausreichen zu lassen. Dies könnte etwa durch Ergänzung des Wortes „Benützen“ durch die Tathandlungen des § 126a erfolgen.

5) Generell könnte für den erweiterten Vorsatz – unabhängig von seiner konkreten Reichweite – **bedingter Vorsatz** ausreichen. Dies würde mE in der Praxis zu erheblichen Beweiserleichterungen führen.

C. Zur Strafbarkeit der Datenverwendung – Lücken und Unklarheiten in § 51 DSG

Den zweiten Teil meiner Ausführungen möchte ich der Verwendung von – etwa durch einen soeben beschriebenen Hacking-Angriff – illegal erlangten Daten widmen. Dazu ein Beispiel:

Eine anonyme Hackergruppierung stellt personenbezogene Daten von Polizeibeamten – Name, Adresse usw – ins Internet. Die Daten wurden ihr von einem ehrenamtlichen Mitarbeiter eines polizeinahen Vereins zugespielt.[24]

Gleich vorweg: ME ist sowohl die Weitergabe durch den Vereinsmitarbeiter als auch die Veröffentlichung der Daten derzeit strafrechtlich nicht zu fassen. In Frage kommt für beide Verhaltensweisen § 51 DSG: **§ 51 DSG** pönalisiert das Benützen, Zugänglichmachen oder Veröffentlichen von personenbezogenen Daten, an denen ein Geheimhaltungsinteresse besteht und die dem Täter ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat.

Auf objektiver Ebene verlangt § 51 DSG somit zunächst einen **speziellen Täterkreis**: Nur derjenige, dem die Daten ausschließlich aufgrund seiner berufsmäßigen Stellung anvertraut wurden oder zugänglich geworden sind oder derjenige, der sich die Daten widerrechtlich verschafft hat, kann sich gem § 51 DSG strafbar machen.

---

[24] Ein Sachverhalt, der sich Medienberichten zufolge im Fall der Hackergruppe „Anonymous“ in Grundzügen so abgespielt hat: http://diepresse.com/home/techscience/internet/sicherheit/695982/Anonymous-veroeffentlicht-Daten-von-25000-Polizisten, abgerufen am 12. 04. 2012.

Das Anvertrauen von personenbezogenen Daten ist im Internet-Zeitalter alltägliche Praxis: User stellen regelmäßig ihre Personendaten Internetunternehmen – seien es Online-Kaufhäuser oder soziale Netzwerke – zur Verfügung. Damit sind aber die Daten nicht automatisch vor missbräuchlicher Verwendung geschützt. Das in § 51 DSG vorgesehene Erfordernis, dass die Daten ausschließlich aufgrund *berufsmäßiger* Beschäftigung[25] anvertraut oder zugänglich geworden sein müssen, ist mE zu eng: Unter „Beruf" sind nach allgemeinem Sprachgebrauch solche Tätigkeiten zu verstehen, die der Bestreitung des Lebensunterhalts dienen. Aushilfstätigkeiten, die unentgeltlich und gelegentlich erfolgen sowie reine Ausbildungsverhältnisse fallen wohl nicht darunter. Dasselbe gilt für rein ehrenamtliche Tätigkeiten.[26] Eine extensive Interpretation des Begriffs „beruflich", die auch solche Beschäftigungen umfassen würde, scheitert mE an der Wortlautschranke.

Es ist durchaus möglich, dass innerhalb eines Unternehmens Personen Zugriff auf die Daten bekommen, deren Tätigkeit somit nicht als „beruflich" einzuordnen ist. Auch im beschriebenen Eingangsbeispiel besteht dieses Problem: Der ehrenamtliche Vereinsmitarbeiter hat wohl nicht ausschließlich aufgrund „berufsmäßiger" Beschäftigung Zugang zu den Polizeidaten erlangt. Daher scheidet für die Weitergabe der Daten § 51 DSG aus!

Der Tatbestand der Verletzung von Berufsgeheimnissen gem § 121 StGB etwa berücksichtigt dieses Problem zum Teil und dehnt in Abs 4 den Anwendungsbereich des Tatbestands auch auf Hilfskräfte und Personen in Ausbildungsverhältnissen aus.[27]

---

25 Zur ähnlichen Formulierung in § 121 StGB: *Lewisch* in WK² § 121 Rz 3.

26 Dazu ausführlich *Salimi* in WK² § 51 DSG Rz 16 ff.

27 Dazu *Lewisch* in WK² § 121 Rz 14 f, *Thiele,* SbgK § 121 Rz 40 ff. Die Materialien erwähnen in Bezug auf § 121 Abs 4 StGB typische Anwendungsfälle wie Angehörige von Ärzten, die in der Praxis mitarbeiten oder praktizierende Medizinstudenten (EBRV 1971, 259 f).

Die Einschränkung auf berufsmäßigen Zugang in § 51 DSG ist sowohl aus Sicht des Datenschutzes als auch aus Sicht des strafrechtlichen Unwerts **nicht sachgerecht**. Der Missbrauch von Daten, der dem Täter durch eine spezielle ehrenamtliche Tätigkeit ermöglicht wurde, erscheint nicht weniger strafwürdig. Ebenso fehlt in § 51 DSG eine § 121 Abs 4 StGB entsprechende Erweiterung des Täterkreises auf unentgeltlich tätige Aushilfen und Personen in reinen Ausbildungsverhältnissen. Eine **Erweiterung auf jede spezielle Tätigkeit**, die den Zugang zu den Daten ermöglicht, sei diese beruflich, gelegentlich, ehrenamtlich oder zu Ausbildungszwecken, wäre mE vorzuziehen, weil sie dem Schutzzweck des § 51 DSG entspräche.

Doch wie sieht es mit der Strafbarkeit des **Veröffentlichens der Daten** im Internet aus? Der Hackergruppe wurden die Daten nicht anvertraut. Daher kommt nur die zweite, von § 51 DSG erfasste Art des Zugangs zu den Daten in Frage: die **widerrechtliche Verschaffung.** Hierunter fallen alle rechtswidrigen Verhaltensweisen der Datenbeschaffung, va ist an Hacking-Attacken iSd § 118a oder auch an das Phänomen des „Phishings“ zu denken. Verschaffen setzt aber jedenfalls – ich verweise etwa auf das Begriffsverständnis bei § 241e StGB[28] – **aktives Tun** des Täters voraus. Werden einer Person zunächst durch Dritte widerrechtlich verschaffte personenbezogene Daten ohne ihr Zutun zugespielt und veröffentlicht diese die Daten, ist der Veröffentlichungsakt nicht unter § 51 DSG subsumierbar. Würde das Gesetz auf Daten abstellen, „die sich der Täter widerrechtlich verschafft **oder ihm widerrechtlich übermittelt“** wurden, wären alle Daten erfasst, die der Täter nicht „haben dürfte“. Damit wäre auch die Veröffentlichung der Daten im Eingangsbeispiel strafbar.[29]

---

[28] Vgl *Kienapfel/Schmoller,* StudB BT III² § 241e Rz 10; *Schroll* in WK² § 241e Rz 8.

[29] Die Strafbarkeit der Weitergabe der Daten durch den Vereinsmitarbeiter gem § 51 DSG würde womöglich wiederum daran scheitern, dass dieser den Zugang zu diesen Daten nicht aus *beruflichen* Gründen (ehrenamtliche Tätigkeit!) erlangt hat.

Zu dieser Enge des erfassten Täterkreises kommen Unklarheiten bei den Tathandlungen des § 51 DSG, was im Besonderen den **Begriffsinhalt des „Benützens“** betrifft.

Benützen ist nach der Begriffswelt des DSG in § 4 Z 9 DSG ein Unterfall des Verarbeitens, das Verarbeiten wiederum eine Form des Verwendens. Nach der Literatur zu § 4 Z 9 DSG fällt unter Benützen „insb auch das Gebrauchen und Verarbeiten der Daten für die vorgegebenen Zwecke“.[30] Daraus erhellt, dass das Benützen nach der Terminologie des DSG keine spezielle Form des Umgangs mit Daten darstellt, sondern jede Art der Datenverwendung, verbunden mit einem speziellen Zweck bzw durch einen bestimmten Personenkreis (Auftraggeber oder Dienstleister). Es ist aber kaum denkbar, dass durch eine im Verarbeitungszweck gelegene Benützung eine strafrechtlich relevante Verletzung von Geheimhaltungsinteressen eintreten würde, womit für diese Tathandlung kaum ein Anwendungsbereich bliebe. Daher lässt sich aus der Terminologie des DSG keine für eine Strafbestimmung brauchbare Definition des Benützens ableiten.

Ich bin aber auch aus **systematischen Gründen** der Ansicht, dass die datenschutzrechtlichen Begrifflichkeiten insoweit auf den gerichtlichen Straftatbestand des § 51 DSG nicht anwendbar sind. Dafür spricht etwa, dass das DSG die Handlung des „Zugänglichmachens“ an keiner anderen Stelle kennt.[31]

Unter Benützen ist daher mE – ganz dem allgemeinen Sprachgebrauch entsprechend – jeder Einsatz der Daten zu verstehen. Ein Benützen kann darin liegen, dass mit Hilfe der Daten ein Vermögensdelikt begangen wird oder diese im Geschäftsverkehr eingesetzt werden.

---

30 *Dohr/Pollirer/Weiß/Knyrim,* DSG 2000 § 4 Anm 10 und *Jahnel*, Handbuch Datenschutzrecht 159; *Drobesch/Grosinger,* DSG § 4 Z 9 Anm 1 definieren das Benützen als konventionelle wie auch durch automationsunterstützten Zugriff erfolgte Verwendung der Daten „für den Zweck, der mit der Datenverarbeitung verfolgt wird“.

31 Ausführlich *Salimi* in WK² § 51 DSG Rz 39 ff; vgl auch *Bergauer* in *Jahnel* (Hrsg), Jahrbuch Datenschutzrecht 2010, 78.

Daten werden mE auch dann benützt, wenn mit dem Datensatz aus technischer Sicht nichts weiter passiert, der Täter aber sein Wissen darüber einsetzt, dh die Information verwertet.[32] Auf den ersten Blick wirkt die strafrechtliche Erfassung der Verwendung einer Information als sehr weitgehend. Aus Sicht des Grundrechtsschutzes erscheint mir diese weite Auslegung des Benützungsbegriffes jedoch fast zwingend: Verschafft sich ein Täter auf illegalem Weg personenbezogene Daten einer Person und verwendet dieses Wissen in krimineller Absicht gegen das Opfer, ist das wohl einer der schwerwiegendsten Eingriffe in das Recht auf Datenschutz und das damit verbundene Geheimhaltungsinteresse, auch wenn – rein technisch gesehen – mit den Daten selbst nichts weiter geschieht. Es genügt in sehr vielen Fällen der Einsatz des Wissens über den Dateninhalt, um das Opfer zu schädigen. Diese Verhaltensweisen nicht als Benützen anzusehen, würde den Anwendungsbereich der Tathandlung des Benützens zu sehr einschränken.[33]

ME setzt Benützen iSd § 51 DSG aber jedenfalls eine Außenwirkung voraus. Das bloß interne Speichern, Löschen oder Vervielfältigen der Daten ohne nach außen hin gerichteten Akt kann nicht zur Verletzung von Geheimhaltungsinteressen führen, sodass diese Handlungen nach § 51 DSG nicht tatbildlich sind.

Strafbar nach § 51 DSG ist das Benützen, Zugänglichmachen oder Veröffentlichen der Daten. Das bloße **Ausspionieren der Daten** zum Zweck der Verwendung, etwa durch Herauslocken durch eine „Phishing“-Attacke, somit das bloße Ermitteln der Daten ist jedoch nicht bereits als „Benützen“ anzusehen. Die widerrechtliche Verschaffung der Daten ist eine Voraussetzung für die Begehung des § 51 DSG und kann nicht schon die Vollendung des Tatbestands bewirken.[34] Damit ist aber eins klargestellt: Es gibt in Österreich – abseits vom Schutz von

---

32 So auch *Jahnel,* Handbuch Datenschutzrecht 3/72; *Berka*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, Gutachten zum 18. ÖJT 40.

33 *Salimi in* WK² § 51 DSG Rz 47.

34 So auch *Reindl,* SIAK-Journal 2007, 10; *Salimi* in WK² § 51 DSG Rz 48.

Geschäfts- und Betriebsgeheimnissen und des Urheberrechts – keine Strafbarkeit des „Datendiebstahls“ als solches, sondern nur eine Strafbarkeit der illegalen Datenverwendung, und auch das nicht umfassend. Im **deutschen Bundesdatenschutzgesetz (BDSG)** hingegen erfasst § 44 iVm § 43 Abs 2 BDSG auch das Erheben von Daten als Tathandlung.[35] Es wäre daher zu überlegen, ob nicht bereits das illegale Ermitteln personenbezogener Daten unter Umständen unter Strafe gestellt werden sollte.

§ 51 DSG hat in den letzten Jahren **keine praktische Bedeutung** erlangt, was sich in der gerichtlichen Kriminalstatistik widerspiegelt.[36] Daran hat auch – soweit bisher überblickbar – der Wegfall des Ermächtigungserfordernisses durch die DSG-Novelle 2010 nichts geändert. Ich bin der Meinung, dass – freilich neben möglichen anderen Faktoren – auch die Unschärfe des Tatbestands ihren Beitrag zur zurückhaltenden Anwendung leistet. Doch warum sollte § 51 DSG „reanimiert“ werden? Ich halte die **zurückhaltende Sanktionierung** der Verletzung des Grundrechts auf Datenschutz generell für ein Problem. Dies trägt mit dazu bei, dass das Datenschutzrecht von vielen Normadressaten als komplizierte, viele Rechtsbereiche übergreifende Rechtsmaterie begriffen wird, deren Verletzung aber letztlich zu keiner scharfen staatlichen Sanktion führt: Auch die Verwaltungsstrafbestimmungen des § 52 DSG sind weitgehend zahnlos: Zum einen kann die DSK als Expertengremium selbst keine Verwaltungsstrafen verhängen, sondern hat diese bei der zuständigen Verwaltungsbehörde, idR die BH, anzuregen (vgl § 52 Abs 5 DSG).[37] Aussagen über die Häufigkeit der von den Bezirksverwaltungsbehörden verhängten Strafen sind naturgemäß schwierig; auffallend ist aber, dass sich keine diesbezügliche veröffentlichte Berufungsentscheidung eines UVS findet.[38] Zudem ist die Höhe der in § 52 DSG angedrohten

---

35 Die deutsche Strafbestimmung sieht alternativ zur Geldstrafe eine Freiheitsstrafe bis zu 2 Jahren vor, während in § 51 DSG nur eine Freiheitsstrafe bis zu einem Jahr vorgesehen ist.

36 Es finden sich seit dem Jahr 2000 nur drei Verurteilungen in der gerichtlichen Kriminalstatistik.

37 *Jahnel,* Handbuch Datenschutzrecht Rz 9/90.

38 Ebenso *Jahnel,* Handbuch Datenschutzrecht Rz 9/90.

Verwaltungsstrafen mE nicht geeignet, eine ausreichende Abschreckungswirkung zu entfalten. Die zunehmende Sensibilisierung der Bevölkerung für Fragen des Datenschutzrechts sollte sich auch in einer wirksamen Sanktionierung von Verstößen widerspiegeln. Umso mehr kommt der gerichtlichen Strafbestimmung des § 51 DSG mit einer Strafdrohung von bis zu einem Jahr Freiheitsstrafe Bedeutung zu. Eine Präzisierung des § 51 DSG, verbunden mit einer erhöhten Sensibilität und einer verstärkten Anwendung würde mE insgesamt zur Stärkung des Datenschutzes in Österreich beitragen.

D. Schlussbemerkungen

Die von mir in den Eingangsbeispielen genannten Fälle sind mE durchaus strafwürdig, werden aber derzeit nicht oder jedenfalls nicht durch das gerichtliche Strafrecht sanktioniert. Im Kampf gegen Bedrohungen durch Cyberkriminalität sind mE die Lücken im materiellen Strafrecht zu schließen. Durch Herabsetzung der subjektiven Schwellen für das Hacking und durch Präzisierung und eventuell Ausweitung des Anwendungsbereichs des § 51 DSG wären wichtige Schritte im Kampf gegen neue Bedrohungen durch Cybercrime gesetzt. Die im Titel meines Vortrags aufgeworfene Frage lässt sich somit bejahen: Das materielle Computerstrafrecht ist – wenn auch nur partiell – zahnlos, seine Zahnlosigkeit ließe sich aber relativ leicht beheben**.**

CYBERCRIME

Prof. Dr. Fritz Wennig
Präsident des Juristenverbandes

Der folgende Artikel soll sich weniger mit den technischen Details zum Thema Cybercrime – welche natürlich zweifelsfrei ebenfalls für die Erfassung dieses Themas im Ganzen nicht unwichtig sind – befassen, als vielmehr mit jenen Gegebenheiten, mit welchen sich der Rechtsanwalt konfrontiert sieht. Das bedeutet insbesondere seine Tätigkeit als Vertreter des Geschädigten, seine Tätigkeit als Verteidiger des Täters und allenfalls seine Tätigkeit im Rahmen rechtsgutächtlicher Beurteilung.

Wer in den letzten Wochen Radio gehört oder Zeitung gelesen hat, wird mit dem Computerwurm „Conficker“ vermutlich bereits vertraut sein. Mit der Bemühung, auf technische Details nicht mehr als zum Verständnis unbedingt notwendig einzugehen, kann „Conficker“ stark vereinfacht wie folgt dargestellt werden:
Es handelt sich um einen hochintelligenten, relativ neuen, vermutlich von IT-Profis aus der Ukraine entwickelten Computerwurm, dessen Eindringen in ein Computersystem dem durchschnittlichen Nutzer gar nicht auffällt. Aufgabe von „Conficker“ ist es, die Kontrolle über alle infizierten Computer zu übernehmen und zu einem mächtigen Netzwerk, einem so genannten Botnetz, zu verbinden. Ein Bot (abgeleitet vom slawischen Wort *robot*, sowie englisch *Roboter*) ist ein Computerprogramm, das weitgehend selbstständig sich wiederholende Aufgaben abarbeitet, ohne dabei auf eine Interaktion eines menschlichen Benutzers angewiesen zu sein. Kommunizieren solche Bots untereinander, so spricht man von einem Botnet. Ein solches kann vom Schöpfer des Computerwurms gesteuert werden und somit andere Computer gezielt attackieren. Der Zweck von „Conficker“ ist noch rätselhaft, denn eine allseits befürchtete große Cyberspace-

Attacke ist bis dato ausgeblieben. Bekannt wurde bisher nur der Fall einer europäischen Bande, die einen Teil des Botnetzes nutzte, um 72 Millionen US-Dollar von amerikanischen Konten zu stehlen. IT-Experten schätzen aber die Dunkelziffer solcher verbrecherischer Angriffe weit höher. Danach soll „Conficker“ für eine ganze Reihe verbrecherischer Taten wie Sabotage oder Spionage genutzt werden, die den Opfern großteils gar nicht auffallen.

In einem strafrechtlichen Zusammenhang stellt sich bei diesem Computerwurm eine mE sehr interessante Frage. Angenommen „Conficker“ wird auf einen PC eingeschleust, ohne dass bis jetzt irgendein Schaden eingetreten wäre, es besteht allerdings die jederzeitige Möglichkeit, dass ein Schaden hervorgerufen wird. Handelt es sich beim „bloßen“ Einschleusen – ohne Eintreten eines technischen Schadens – des Virus schon per se um die Erfüllung eines gesetzlichen Straftatbestandes oder lediglich um eine Vortat, deren Strafbarkeit in einem nächsten Schritt zu klären wäre? § 118a des Strafgesetzbuches normiert den „widerrechtlichen Zugriff auf ein Computersystem“ als einen Straftatbestand. Ohne diesen sehr langen und relativ komplizierten Paragraphen in seine Einzelteile zerstückeln zu wollen, kann gesagt werden, dass der objektive Tatbestand dann erfüllt wird, wenn sich jemand Zugang zu einem Computersystem, über das er nicht (alleine) verfügen darf, verschafft. Dies unter Verletzung spezifischer Sicherheitsvorkehrungen. Es kann hier also problemlos unterstellt werden, dass der Tatbestand des § 118a StGB erfüllt ist. Der subjektive Tatbestand erfordert allerdings neben gewöhnlichem dolus eventualis auf den objektiven Tatbestand zusätzlich noch Absichtlichkeit bezüglich Spionage, Verwendung von Daten sowie Gewinn- bzw Schädigungsabsicht. Man wird also zum Ergebnis kommen müssen, dass dieser Straftatbestand nicht erfüllt ist, womit sich die Beantwortung der Frage auf die Ebene der Vortat verschieben wird.

Aus zivil- und gerade aus schadenersatzrechtlicher Sicht drängt sich bei derselben Fallkonstellation die Frage auf, ob durch das „bloße“ Einschleusen bereits ein (ersatzfähiger) Schaden entstanden ist und bejahendenfalls, worin dieser liegt. Als ein theoretisches Beispiel soll davon ausgegangen werden, dass der Geschädigte zwei Notebooks besitzt, die er beide zu veräußern beabsichtigt. In den Medien hört und liest er vom „Conficker“-Wurm und ist daran interessiert, zu wissen, ob eines oder gar beide seiner beiden Notebooks von diesem Wurm betroffen sind. Er wendet sich an ausgewiesene Computerexperten, wie beispielsweise die technische Hochschule, welche sodann feststellen müssen, dass eines der beiden Notebooks vom Virus befallen ist. Ein Schaden am Notebook ist durch den Virus zwar noch nicht eingetreten, die Computerexperten sind aber auch nicht in der Lage, ihn zu beseitigen. Als redlicher Verkäufer möchte der Geschädigte nun keinesfalls einen wesentlichen Mangel – nämlich den Befall durch den „Conficker-„Wurm verschweigen, weshalb er den Käufer wahrheitsgemäß aufklärt. Der Käufer wird naturgemäß einen wesentlich geringeren Kaufpreis für das infizierte Notebook bezahlen als für das mangelfreie Exemplar, eventuell vom Kauf des mangelhaften Notebooks gar zurücktreten. Genau hierin liegt mE der Vermögensschaden, weshalb die gestellte Frage jedenfalls zu bejahen ist.

Aus Sicht des Vertreters des Geschädigten ergeben sich interessante Fragen des Weiteren auch ganz allgemein – nicht nur mit dem „Conficker“-Wurm – in Zusammenhang mit einem Angriff auf einen Computer oder dessen Daten, ohne dass zumindest hinsichtlich gewisser Örtlichkeiten bis jetzt ein Missbrauch begangen wurde. Um diese sehr theoretisch formulierte Frage etwas zu veranschaulichen, sei folgender Sachverhalt unterstellt: Die Firma X verfügt in Österreich über 60 Filialen. Für einen Dritten, insbesondere für Konkurrenzunternehmen, kann es durchaus interessant sein, zu wissen, welche Umsätze erzielt werden, wie hoch die Miet- und Personalkosten sind, welcher Aufschlag auf den Wareneinkauf vorgenommen wird, etc. Deshalb dringt nun ein

„Hacker“ in das Computersystem einer der 60 Filialen ein und verschafft sich die begehrten Informationen hinsichtlich dieser „gehackten“ Filiale. Die Firma sieht sich nun bei den restlichen 59 Filialen gezwungen, Schutz- und Rettungsmaßnahmen zu ergreifen. Es wird ein Computertechniker damit beauftragt, die Zugangscodes zu ändern, ein sonst nicht übliches, spezielles Antiviren-System zu installieren, etc. In weiterer Folge kann der Täter gefasst werden. Es erhebt sich nunmehr die Frage, ob dieser Täter für die Schutzmaßnahmen an den weiteren 59 Standorten, an denen er zwar keine Tat begangen hatte, wo aber der dringende Verdacht nahe gelegen war, dass er auch in diese Computernetzwerke eindringen wird, zum Schadenersatz herangezogen werden kann.

Diesbezüglich ist vor allem von folgender Rechtslage auszugehen:

Es lässt sich dem österreichischen Zivilrecht eine direkte Bestimmung, auf welche sich ein derartiger Schadenersatz stützen ließe, nicht entnehmen. Die Haftung für vorbeugende Maßnahmen ist dem österreichischen Recht allerdings nicht fremd. So bestimmt beispielsweise § 11 Abs 3 Atomhaftungsgesetz: *„Die Ersatzpflicht umfasst weiters die Kosten angemessener vorbeugender Maßnahmen zur Abwehr einer […] unmittelbar drohenden Gefahr (Rettungskosten).“* Anspruch auf Ersatz dieser Kosten hat diejenige Person, die den Aufwand tatsächlich getragen hat. Diese Ersatzpflicht umfasst auch den Verdienstentgang von Personen, die durch vorbeugende Maßnahmen in ihrer Erwerbstätigkeit gehindert worden sind. Auf das Computerrecht übertragen könnte das bedeuten, dass sowohl die vorbeugenden Maßnahmen wie das Einsetzen eines anderen Passwortes, etc ersatzfähig sind, als auch der Schaden derjenigen Personen, die durch das „Hacken“ des Systems mit dem Computer über eine gewisse Zeit nicht arbeiten konnten. Ob eine solche Bestimmung auch für das Computerrecht noch sinnvollerweise geschaffen wird, ob die – zugegebenermaßen weither geholten Bestimmungen aus dem Atomhaftungsgesetz – analog anzuwenden sind oder

ob es sich dabei eben um getrennte Rechtskreise handelt, wird die Zukunft weisen.

Da die meisten Straftatbestände im Zusammenhang mit Computerkriminalität als Ermächtigungsdelikte formuliert sind, ist als Vertreter des Geschädigten weiters stets darauf zu achten, dass die Ermächtigung an die Strafverfolgungsbehörden fristgerecht und ordnungsgemäß erteilt wird.

Im Rahmen der Vertretung kann es sodann auch notwendig sein, sich die Frage nach der Möglichkeit der Ergreifung einstweiliger Maßnahmen zu stellen, sei es in die Richtung, dass durch einstweilige Verfügung verboten werden soll, gehackte Daten zu verwenden oder auf einen anderen Datenträger zu speichern, etc. Im Strafprozess, dem sich der Geschädigte bekanntlich als Privatbeteiligter anschließen kann, richten sich die Sicherstellung und Beschlagnahme von Gegenständen nach den §§ 109 ff StPO. Hierbei kommt das Recht der Antragstellung allerdings ausschließlich dem Staatsanwalt zu. Hier wird der Vertreter gut beraten sein, auf derartige einstweilige Maßnahmen hinzuwirken, da ein Rechtsanspruch nicht besteht. Im Zivilprozess richten sich einstweilige Verfügungen nach der ZPO, welche wiederum einen Verweis auf die Exekutionsordnung enthält.

Von Bedeutung für den Vertreter des Geschädigten könnte des Weiteren auch die Vorgehensweise, wenn der Betroffene nicht unmittelbar, sondern bloß mittelbar geschädigt ist, sein. Der Ersatz von Drittschäden wird von der ständigen Rechtsprechung und Lehre in Analogie zu den §§ 1358 ABGB sowie 67 VersVG bei deliktischer Schädigung immer dann bejaht, wenn der Schaden aus besonderen Umständen auf einen Dritten bloß verlagert wird und es sich zudem nicht um einen bloßen Vermögensschaden handelt. Wird ein Dritter also beispielsweise durch das Abziehen von Daten in einem absolut geschützten Rechtsgut (zB geistiges Eigentum) verletzt, so stellt sich die Frage nach der Ersatzfähigkeit eines

Drittschadens gar nicht, da er in diesem Fall selbst unmittelbar geschädigt ist.

Wurden nun einige Aspekte beleuchtet, auf die als Vertreter des Geschädigten Bedacht zu nehmen ist, so sollen nun einige derjenigen Fakten und Fragestellungen dargestellt werden, mit denen sich der Verteidiger des Täters auseinanderzusetzen hat.

Vorweg empfiehlt es sich immer, auf die Verjährungsfristen der einzelnen in Frage stehenden Delikte Bedacht zu nehmen. Bei allen mit Computerkriminalität in Zusammenhang stehenden Tatbeständen des StGB (namentlich: § 118a Widerrechtlicher Zugriff auf ein Computersystem, § 119 Verletzung des Telekommunikationsgeheimnisses, § 119a Missbräuchliches Abfangen von Daten, § 126a Datenbeschädigung, § 126b Störung der Funktionsfähigkeit eines Computersystems, § 126c Missbrauch von Computerprogrammen oder Zugangsdaten) bewegen sich die Strafdrohungen – wenn man von den etwaigen Wertqualifikationen, auf welche natürlich immer gesondert Bedacht zu nehmen ist, absieht – zwischen Geldstrafen und Freiheitsstrafen bis zu 6 Monaten. Die Verjährungsfrist beträgt folglich zumeist 1 Jahr.

Hat die Tat einen Auslandsbezug, was vor allem bei Cybercrime-Delikten durch die weltweite Vernetzung von Computern nicht unwahrscheinlich ist, sollte die Überlegung angestellt werden, ob man bei genauerer Betrachtung nicht vielleicht zur Anwendbarkeit eines günstigeren Rechts gelangt. Gemäß § 65 Abs 2 StGB ist die Strafe so zu bestimmen, dass der Täter in der Gesamtauswirkung nicht ungünstiger gestellt wird, als nach dem Gesetz des Tatorts. Hierbei handelt es sich also um eine bloße Strafzumessungsvorschrift, welche nicht die Anwendbarkeit eines ausländischen, eventuell günstigeren Rechts regelt, sondern lediglich normiert, dass die Strafe so zu bestimmen ist, dass der Täter nicht schlechter gestellt wird, als wenn er von einem Gericht des Tatortes verurteilt worden wäre. Die Strafe ist demzufolge nach Art und Höhe nicht strenger

auszumessen, als nach dem ausländischen Recht des Tatortes.

Weiters ist man als Vertreter gut beraten, sich mit einer möglichen Reuefähigkeit der zur Last gelegten Straftaten zu beschäftigen. § 167 StGB nennt als – für die Computerkriminalität relevante – Bestimmungen die Datenbeschädigung (§ 126a StGB), sowie die Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) explizit als reuefähige Delikte. Nicht genannt werden der widerrechtliche Zugriff auf ein Computersystem (§ 118a StGB), die Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB), das missbräuchliche Abfangen von Daten (§ 119a StGB) sowie der Missbrauch von Computerprogrammen und Zugangsdaten (§ 126c StGB). Bei den §§ 118a, 119 sowie 119a handelt es sich um Ermächtigungsdelikte. § 126c enthält in seinem Abs 2 selbst eine zur Straffreiheit führende Bestimmung: *„ […] ist nicht zu bestrafen, wer freiwillig verhindert, dass […].* Weiters *[…] ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie* (die Gefahr) *zu beseitigen.“* Es handelt sich hierbei um eine Mischung zwischen tätiger Reue und ernsthaftem Rücktritt vom Versuch. Im Ergebnis sind somit all diese Delikte – mit Ausnahme der Ermächtigungsdelikte – reuefähig. Bei der tätigen Reue ist zu beachten, dass bei einer Faktenmehrheit das Privileg nur dann zum Tragen kommt, wenn der gesamte Schaden gutgemacht wird (OGH 12 Os 10/09a), sie niemals zukünftige Straftaten zum Gegenstand haben kann (OGH 14 Os 159/03) und in der gegenüber dem Geschädigten mündlich oder schriftlich abgegebenen Erklärung sowohl die Schadenshöhe ziffernmäßig als auch die Leistungsfrist kalendermäßig bestimmt sein muss (OGH 11 Os 56/99; OGH 13 Os 142/02).

Wie bei den meisten Straftatbeständen ergeben sich auch bei den Cybercrime-Delikten komplizierte teilweise nur sehr schwer zu beantwortende Konkurrenzfragen. Hier seien bloß exemplarisch einige Beispiele dargestellt: Wer etwa bei einem

widerrechtlichen Zugriff auf ein Computersystem (§ 118a) auch Daten beschädigt (§ 126a), verantwortet wegen der unterschiedlichen Schutzgüter der Normen, beide Straftaten in echter Konkurrenz. Auch mit der Verletzung des Telekommunikationsgeheimnisses (§ 119) ist eine diesbezügliche Konkurrenz denkbar, wenn der Täter etwa in einen Mailserver eindringt und mittels eines bösartigen Programms Kopien aller über diesen Server laufenden E-Mails und Nachrichten erhält. Das missbräuchliche Abfangen von Daten (§ 119a) ist beispielsweise ausdrücklich subsidiär zur Verletzung des Telekommunikationsgeheimnisses (§ 119). Immer wenn also nicht bloß Daten, sondern auch Nachrichten ausspioniert werden, tritt § 119 zurück.

Nicht nur für den Vertreter des Geschädigten oder Verteidiger des Täters, sondern generell für den interessierten Juristen mag folgendes verwunderlich sein: Wenn man im Internet unter Datendiebstahl stöbert, findet man sehr schnell eine Internetseite der „Arge-Daten“ mit der Überschrift „Datendiebstahl wird in Österreich nicht bestraft“. Es muss sich die Frage gestellt werden, ob dies auch in dieser Form richtig ist. Schnell wird man dieser Aussage insofern einen gewissen Wahrheitsgehalt beimessen müssen, als dass dem österreichischen Strafgesetzbuch ein Delikt mit dem Namen „Datendiebstahl“ fremd ist. Möchte man das Stehlen bzw Abziehen fremder Daten unter den Diebstahlsbegriff des § 127 subsumieren, wird man schnell scheitern, da Daten als nicht körperliche Sachen eben keine diebstahlsfähigen Sachen sind. Im Zuge der Umsetzung der Cybercrime-Richtline der Europäischen Union wurde eine Reihe neuer Strafbestimmungen in das StGB, wie zum Beispiel der bereits mehrfach genannte § 118a, eingefügt. Wie oben bereits ausgeführt, hat diese Bestimmung eine sehr weite subjektive Tatseite, welche naturgemäß mit Beweisschwierigkeiten seitens der Gerichte verbunden ist. Interessant ist hier der Vergleich mit Deutschland, in dessen Strafgesetzbuch die §§ 202a, 202b das Ausspähen bzw das Abfangen von Daten unter Strafe stellen. Vor allem das Ausspähen von Daten (§ 202a) ist im Volksmund

und Lehre als so genannter „Datendiebstahlsparagraph“ bekannt. Der schon wesentlich einfacher formulierte objektive Tatbestand fordert zudem bloßen Eventualvorsatz, also – anders als die österreichische Bestimmung – weder Bereicherungs- noch Schädigungsabsicht. Es mag daher richtig sein, dass eine Bestrafung wegen Datendiebstahls in anderen Ländern der Europäischen Union – wie eben gerade der Vergleich mit Deutschland zeigt – leichter zu erreichen ist und sich die Anwendbarkeit der österreichischen „Cybercrimebestimmungen“ auf Grund ihrer recht komplizierten Formulierungen und hohen Anforderungen auf der subjektiven Tatseite als schwieriger erweist; eine generelle Straffreiheit in Österreich ist damit aber noch keinesfalls bewirkt.

STATUTEN

der Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft

§ 1

Name, Sitz und Tätigkeitsbereich

Der Verein führt den Namen "Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft" und hat seinen Sitz in Wien. Seine Tätigkeit erstreckt sich auf das ganze Bundesgebiet.

§ 2

Zweck

(1) Die Landesgruppe Österreich (im nachstehenden Landesgruppe genannt) der Internationalen Strafrechtsgesellschaft - Association Internationale de Droit Pénal (A.I.D.P.) - mit dem Sitz in Paris ist eine gemeinnützige, nicht auf Gewinn zielende Einrichtung und hat die Aufgabe, als Mitglied der Internationalen Strafrechtsgesellschaft (im nachstehenden Gesellschaft genannt) im Rahmen und im Sinne der Statuten der Gesellschaft an deren Arbeiten und Veranstaltungen mitzuwirken und zur Verwirklichung ihrer Ziele beizutragen. Diese Ziele sind ein Gedankenaustausch und eine engere Zusammenarbeit zwischen Einzelpersonen und Institutionen in den einzelnen Ländern, die sich mit Studien oder mit der Anwendung des Strafrechts oder mit der Erforschung der Kriminalität und ihrer Ursachen befassen. Auf diese Weise soll das Strafrecht mit seinen wissenschaftlichen Grundlagen möglichst in Einklang gebracht sowie die theoretische und praktische Entwicklung des internationalen Strafrechts gefördert werden.

(2) Die Aufgaben der Landesgruppe sollen, gegebenenfalls in Zusammenarbeit mit anderen Landesgruppen, insbesondere durch die Ausarbeitung von österreichischen Landesreferaten zu den von der Gesellschaft veranstalteten Internationalen Strafrechtskongressen sowie durch die Bestellung von Berichterstattern zu diesen Kongressen und von Mitarbeitern an den Untersuchungen, Studien und Veröffentlichungen der Gesellschaft verwirklicht werden. Darüber hinaus kann die Landesgruppe eigene wissenschaftliche und gesellschaftliche Zusammenkünfte veranstalten und Dokumentationen dieser Veranstaltungen sowie Abhandlungen ihrer Mitarbeiter veröffentlichen.

§ 3

Aufbringung der Mittel

Die Geldmittel, die zur Erreichung des Vereinszwecks erforderlich sind, werden durch Mitgliedsbeiträge, Subventionen, Spenden, Vermächtnisse und sonstige Einnahmen aufgebracht.

§ 4

Mitglieder

(1) Mitglieder können alle physischen und juristischen Personen werden, die die in § 2 festgelegten Ziele und Absichten des Vereines zu fördern und zu unterstützen bereit sind. Die Aufnahme erfolgt auf Grund eines Aufnahmeansuchens, über das der Vorstand mit Stimmenmehrheit beschließt. Die Gründe einer Ablehnung werden nicht bekanntgegeben.

(2) Alle Mitglieder haben die gleichen Rechte und Pflichten. Sie haben Sitz und Stimme in der Generalversammlung sowie das aktive und passive Wahlrecht. Sie erhalten kostenlos die Publikationen der Gesellschaft und der Landesgruppe.

(3) Die Mitglieder sind zur Entrichtung des jeweils festgesetzten Mitgliedsbeitrages zu den festgesetzten Zeitpunkten an die Landesgruppe verpflichtet. Weiters sind sie verpflichtet, die Tätigkeit und Ziele der Gesellschaft sowie der Landesgruppe zu fördern und die Statuten der Landesgruppe ebenso einzuhalten, wie die Beschlüsse ihrer Organe.

(4) Zum Zwecke der Führung einer zentralen Mitgliederevidenz ist der Vorstand ermächtigt, der Internationalen Strafrechtsgesellschaft die hiefür erforderlichen Daten der Mitglieder der Landesgruppe zu übermitteln.

§ 5

Beendigung der Mitgliedschaft

(1) Die Mitgliedschaft endet:

(a) durch Tod oder durch den Untergang der Rechtspersönlichkeit juristischer Personen;

(b) durch Austritt.
Mitglieder, welche trotz Mahnung mit ihrem Beitrag mehr als ein Jahr im Rückstand bleiben, können vom Vorstand als ausgetreten betrachtet werden. Mitglieder der Landesgruppe können jederzeit ohne Angaben von Gründen austreten. Der Mitgliedsbeitrag ist bis zum Ende des Kalenderjahres, in dem der Austritt erklärt worden ist, zu entrichten.

(c) Durch Ausschluss.
Mitglieder, die dem Zweck oder dem Ansehen der Landesgruppe zuwiderhandeln oder deren Satzungen und Beschlüsse verletzen, können durch Beschluss des Vorstandes ausgeschlossen werden. Der Vorstand hat das ausgeschlossene Mitglied mit eingeschriebenem Brief von seiner Entscheidung zu verständigen. Dem Betroffenen steht es frei, binnen vier Wochen ab Zustellung schriftlich Einspruch dagegen zu erheben und die Einberufung eines Schiedsgerichtes zu verlangen. Über den Termin der

Einberufung des Schiedsgerichtes entscheidet der Vorstand.

(2) Die Beendigung der Mitgliedschaft berechtigt in keinem Fall zur Rückforderung der an die Gesellschaft erbrachten Leistungen.

§ 6

Organe der Gesellschaft

(1) Die Gesellschaft hat folgende Organe:
1. Generalversammlung
2. Vorstand
3. Rechnungsprüfer
4. Schiedsgericht.

(2) Alle Funktionen werden ehrenamtlich ausgeübt.

§ 7

Generalversammlung

(1) Die ordentliche Generalversammlung der Landesgruppe hat vor jeder ordentlichen Generalversammlung der Gesellschaft stattzufinden. Mitglieder der Gesellschaft, die juristische Personen sind, werden durch je eine bevollmächtigte Person vertreten, stimmberechtigte Mitglieder können sich durch bevollmächtigte Personen in der Generalversammlung vertreten lassen.

(2) Die Mitglieder sind ein Monat vor Abhaltung der Generalversammlung schriftlich unter Angabe von Zeit, Ort- und Tagesordnung durch den Vorstand einzuladen.

(3) Anträge von Mitgliedern zur Tagesordnung müssen spätestens 14 Tage vor der Generalversammlung schriftlich im Sekretariat der Gesellschaft eingebracht sein. Beschlüsse

können nur über Anträge gefasst werden, die auf die Tagesordnung gesetzt worden sind. Dringlichkeitsanträge während der Versammlung sind unzulässig. Die Generalversammlung ist beschlussfähig, wenn mindestens ein Drittel der stimmberechtigten Mitglieder anwesend ist. Ist die Generalversammlung zur festgesetzten Stunde nicht beschlussfähig, findet eine halbe Stunde später am gleichen Ort mit derselben Tagesordnung eine neue Generalversammlung statt, die ohne Rücksicht auf die Zahl der anwesenden Mitglieder beschlussfähig ist.

(4) Beschlüsse werden, soweit die Statuten nichts anderes vorsehen, mit einfacher Stimmenmehrheit gefasst. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Für Beschlüsse über Statutenänderungen ist eine Dreiviertelmehrheit der abgegebenen Stimmen erforderlich.

(5) Der Generalversammlung obliegt:
(a) die Wahl des Präsidenten und des Vizepräsidenten;
(b) die Wahl der Mitglieder des Vorstandes;
(c) die Bestätigung kooptierter Vorstandsmitglieder;
(d) die Wahl von zwei Rechnungsprüfern und zwei stellvertretenden Rechnungsprüfern;
(e) die Beschlussfassung über den Tätigkeitsbericht und die Entlastung des Vorstandes;
(f) die Festsetzung der Mitgliedsbeiträge;
(g) die Beschlussfassung über Statutenänderungen;
(h) Beschlussfassung über Anträge von Mitgliedern;
(i) Beschlussfassung über die Auflösung des Vereines.

§ 8

Außerordentliche Generalversammlung

Eine außerordentliche Generalversammlung ist einzuberufen:
(a) über Beschluss des Vorstandes;
(b) über schriftlichen, unter Angabe der Gründe gestellten Antrag von mindestens einem Zehntel der

stimmberechtigten Mitglieder. Eine Unterschriftenliste ist anzuschließen. Die außerordentliche Generalversammlung ist spätestens acht Wochen vom Zeitpunkt des Beschlusses beziehungsweise des Einlangens des schriftlichen Antrages vom Vorstand einzuberufen.

§ 9

Vorstand

(1) Der Vorstand wird auf die Dauer von fünf Jahren gewählt und besteht aus:
1. dem Präsidenten,
2. dem Vizepräsidenten,
3. dem Generalsekretär,
4. dem Finanzreferenten und
5. bis zu zehn weiteren Vorstandsmitgliedern.

Neben den in den Z. 1 bis 5 erwähnten Vorstandsmitgliedern darf der Vorstand bei besonderem Bedarf für bestimmte Zeit, die jedoch in keinem Fall die Funktionsperiode des Vorstandes überschreiten darf, bis zu drei wählbare Mitglieder kooptieren, wobei die Gesamtzahl der Vorstandsmitglieder 17 nicht übersteigen darf. Kooptierte Vorstandsmitglieder sind den gewählten Vorstandsmitgliedern gleichgestellt; sie sind in ihren Funktionen von der nächsten Generalversammlung zu bestätigen.

(2) Die Beschlussfähigkeit des Vorstandes ist bei Anwesenheit des Präsidenten oder des Vizepräsidenten sowie des Generalsekretärs und eines weiteren Mitgliedes des Vorstandes gegeben. Bei Entscheidungen über finanzielle Angelegenheiten hat der Finanzreferent mitzuwirken. Vorstandsbeschlüsse werden mit einfacher Stimmenmehrheit gefasst.

(3) Der Vorstand bestellt aus seiner Mitte den Generalsekretär und den Finanzreferenten.

(4) Dem Vorstand obliegt die Leitung der Landesgruppe, die Verwaltung des Vereinsvermögens sowie die Besorgung aller nicht ausdrücklich der Generalversammlung vorbehaltenen Angelegenheiten. Insbesondere gehört zu den Aufgaben des Vorstandes:

(a) der Vorschlag der Tagesordnung der Generalversammlung und deren Einberufung;
(b) die Beschlussfassung über den Haushaltsvoranschlag und den Rechnungsabschluss;
(c) die Beschlussfassung über die Geschäftsordnung der Gesellschaft;
(d) die Beschlussfassung über das Arbeitsprogramm;
(e) die Aufnahme und der Ausschluss von Mitgliedern;
(f) die Kooptierung von Vorstandsmitgliedern;
(g) die Vergebung von Forschungsaufträgen.

(5) Der Generalsekretär hat nach Maßgabe der Geschäftsordnung die laufenden Angelegenheiten der Gesellschaft zu erledigen und die Arbeitsvorhaben im Rahmen des vom Vorstand beschlossenen Jahresarbeitsplanes vorzubereiten, den Fortgang vergebener Arbeitsvorhaben zu überwachen, fertiggestellte wissenschaftliche Arbeiten zu prüfen und gegebenenfalls deren Drucklegung zu veranlassen. Der Generalsekretär kann zur Erfüllung der ihm übertragenen Aufgaben auch andere Vereinsmitglieder heranziehen.

§ 10

Vertretung der Gesellschaft

(1) Der Präsident, in seiner Vertretung der Vizepräsident, beruft die Sitzungen ein, führt den Vorsitz in den Vorstandssitzungen und in der Generalversammlung. Der Präsident oder der Vizepräsident oder der Generalsekretär vertreten die Gesellschaft nach außen.

(2) Der Vizepräsident oder der Generalsekretär dürfen nach Abs 1 nur tätig werden, wenn der Präsident verhindert ist. Die

Wirksamkeit von Vertretungshandlungen wird dadurch nicht berührt.

(3) Die von der Gesellschaft ausgehenden Schriftstücke werden vom Präsidenten gemeinsam mit dem Generalsekretär gezeichnet. Im Rahmen des § 9 Abs 5 ist der Generalsekretär allein zeichnungsberechtigt.

§ 11

Finanzreferent

Der Finanzreferent hat den Vorstand bei der Ausarbeitung des Haushaltsvoranschlages zu beraten. Er legt den Voranschlag dem Vorstand vor und berichtet dem Vorstand und der Generalversammlung über die Finanzgebarung. Der Finanzreferent kann zur Erfüllung der ihm übertragenen Aufgaben auch andere Vereinsmitglieder heranziehen.

§ 12

Rechnungsprüfer

Die Rechnungsprüfer werden für die Dauer von drei Jahren aus den Vereinsmitgliedern gewählt; sie dürfen nicht Mitglieder des Vorstandes sein. Ihnen obliegt die regelmäßige Geschäftskontrolle und die Überprüfung des Rechnungsabschlusses. Sie haben das Ergebnis ihrer Überprüfung an den Vorstand und in der Generalversammlung zu berichten.

§ 13

Schiedsgericht

(1) Streitigkeiten aus dem Vereinsverhältnis sowohl zwischen dem Vorstand und einzelnen Mitgliedern als auch zwischen Mitgliedern untereinander werden durch ein Schiedsgericht

entschieden, in das jeder der Streitteile zwei Vereinsmitglieder als Schiedsrichter entsendet. Die Schiedsrichter wählen mit einfacher Stimmenmehrheit ein Vereinsmitglied zum Obmann. Bei gleicher Stimmenzahl entscheidet das Los.

(2) Das Schiedsgericht entscheidet nach Anhörung der Streitteile bei Anwesenheit aller seiner Mitglieder. Die Entscheidungen werden mit einfacher Stimmenmehrheit gefasst. Bei Stimmengleichheit gibt die Stimme des Obmannes den Ausschlag.

§ 14

Arbeitsausschüsse

Für einzelne Arbeitsvorhaben können vom Vorstand Arbeitsausschüsse eingesetzt werden, deren Angehörige nicht Mitglieder der Gesellschaft sein müssen.

§ 15

Beschlüsse der Kollegialorgane

Für gültige Beschlüsse sämtlicher Kollegialorgane der Gesellschaft ist, sofern die Statuten nichts anderes bestimmen, die Anwesenheit von mindestens der Hälfte der Mitglieder dieses Organes erforderlich. Die Beschlüsse werden mit einfacher Stimmenmehrheit gefasst. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag.

§ 16

Auflösung der Landesgruppe

Die Auflösung der Landesgruppe kann nur in einer ausschließlich zu diesem Zweck einberufenen Generalversammlung mit Vierfünftelmehrheit aller anwesenden stimmberechtigten Mitglieder beschlossen werden. Die gleiche

Generalversammlung beschließt im Falle der freiwilligen Auslösung über die Verwertung des Vereinsvermögens, das gleichen oder ähnlichen Zwecken, wie sie die Gesellschaft verfolgt hat, jedenfalls gemeinnützig wissenschaftlichen Zwecken zufallen soll.

Aktuelle Liste der Mitglieder des Vorstandes der Landesgruppe Österreich der Internationalen Strafrechtsgesellschaft (AIDP)

(seit 27. November 2009)

Präsident:	Prof. Dr. Otto F. MÜLLER
Vizepräsident:	Prof. Dr. Ernst Eugen FABRIZY
Generalsekretär:	Mag. Michael LEITNER
Finanzreferent:	Dr. Erich WEISZ
weitere Mitglieder:	Dr. Gerhard BENN-IBLER Dr. Brigitte BIERLEIN em. Univ.-Prof. Dr. Manfred BURGSTALLER Dr. Jo DEDEYNE-AMANN Dr. Helmut EPP Dr. Irene GARTNER Mag. Gerhard JAROSCH Dr. Nikolaus MICHALEK Prof. Dr. Roland MIKLAU Dr. Gottfried STRASSER
kooptierte Mitglieder:	o. Univ.-Prof. Dr. Frank HÖPFEL Prof. Dr. Friedrich WENNIG