Basar-Kriminalität in der Cyberwelt

Herausforderungen für die Polizei in der Cybercrime

Agenda

- Einführung
- Phänomene der Cybercrime - Gegenwart und nahe Zukunft
- Modell der Cybercrime
- Thesen zu polizeilichen Herausforderungen in der Cyberwelt

Provokante These zum Umgang mit Cybercrime

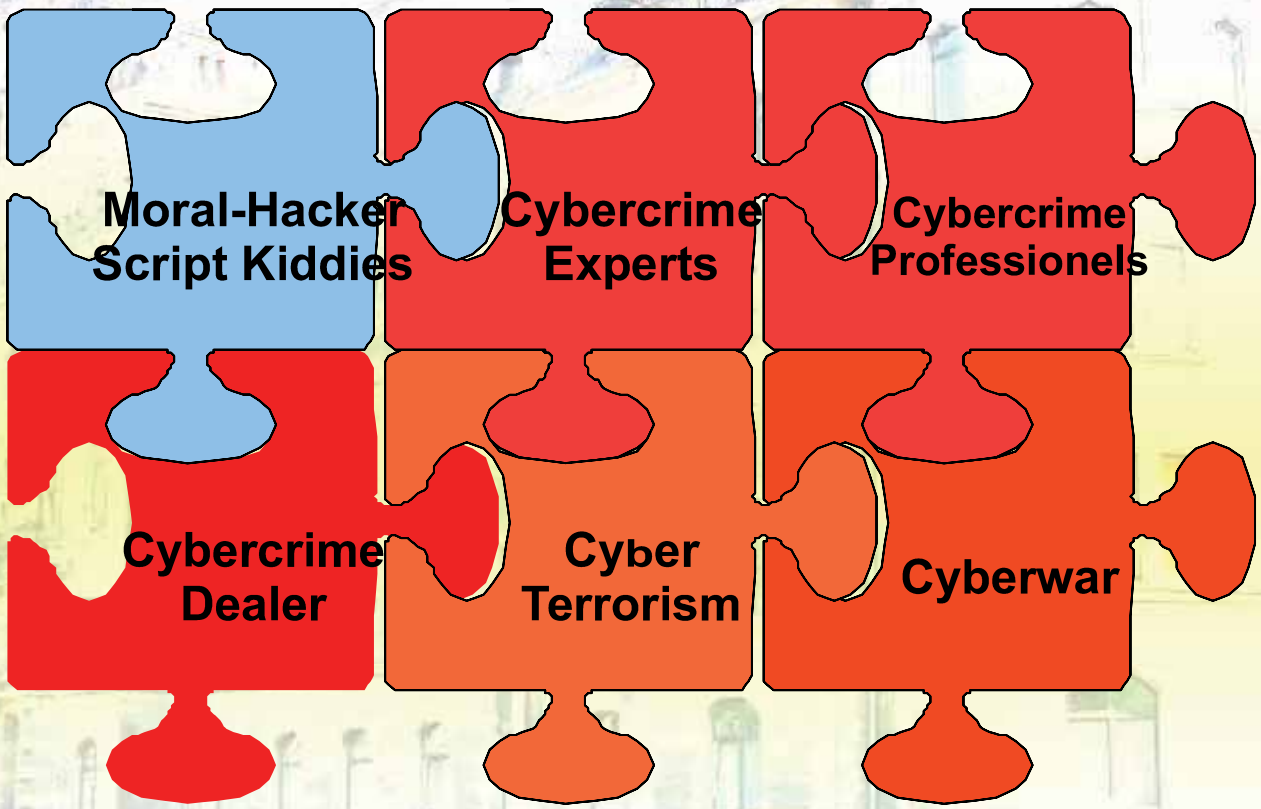
„Der millionenfachen Mitmachgemeinde des **„Web 2.0"** steht in Deutschland in weiten Teilen noch immer eine **„COP PGP"** – Gemeinde gegenüber, eine deutsche Polizeiorganisation, die sich im Wesentlichen an polizeilichen Strukturen **p**reußischer **G**rund**p**rägung orientiert."

Können nationale Polizeiorganisationen mit den Mitteln der zwischenstaatlichen Zusammenarbeit den Herausforderungen einer global vernetzten Wissens- und Kreativgesellschaft mit uneingeschränkter "Kommunikationsmobilität" gerecht werden?

Phänomene der Cybercrime

- Der Cyberbasar als Handelsplattform - Marktplatz für "Profis" und "Berufseinsteiger"
- Cyberangriffe mit finanziellem Hintergrund (z.B.Malware für Identitätsdiebstahl, Bandbreite der Betrugsdelikte, Angriffe auf IT-Strukturen mit Erpressungshintergrund, Urheberrechtsverletzungen etc.)
- Cyberangriffe mit politischem Hintergrund (z.B. Malware für politisch motivierte Straftaten)

Modell der Cybercrime



Grundlage des Modells bei www.cyberfahnder.de

Herausforderungen im Zusammenhang mit Cybercrime

Private und Unternehmen

Cyber-Psychologie im Web 2.0

Bewältigungsfeld Technikwandel

Identitäts- und Reputationsmanagement

Sicherheitsbewusstsein in der Cyberwelt

Polizei und Justiz

Polizei und Cyberwelt

Wechselnde Spielarten bei Cyber-Delikten

Folgen des Technikwandels

Changemanagement in den Bereichen Prävention und Repression

Das Internet wird persönlich!

Das Identitätsmanagement (Authentifizierung und Autorisierung zwischen Bürgern sowie im Verhältnis Staat – Bürger) wird den Einzelnen in zunehmendem Maße erheblich fordern.
Es wird zunehmend schwerer werden, seine digitale Identität zu schützen. In Abhängigkeit davon muss der Einzelne auch seine analoge Identität schützen, denn er ist nicht mehr uneingeschränkter Herr seiner (digitalen) Daten. Der Aufwand für sein Reputationsmanagement wird zunehmen.

Für die Strafverfolgung bieten sich oftmals kaum Ermittlungsansätze!

Das Internet „entblößt“ – Informationen bleiben nicht länger in Streubesitz

Wikileaks ist zum Synonym für Menschen geworden, die eine Veröffentlichung von „geheimen“ Informationen als legitimes Mittel im Rahmen der gesellschaftlichen Auseinandersetzung sehen.

Staatliche Stellen müssen zunehmend damit rechnen, dass verfahrensinterne und damit vertrauliche oder geheime Informationen öffentlich werden. Eine Möglichkeit zum Selbstschutz haben viele Betroffene nicht, weil Ihnen der Schutz der Datenintegrität und der Datenintimität nicht oder nicht allein obliegt.

Der technische Fortschritt erfordert neue Formen der Arbeitsorganisation bei Justiz und Polizei

Der „Cyber-Ermittler" könnte der Prototyp des oft zitierten Wissensarbeiters in Justiz und Polizei werden. Er arbeitet von seinem jeweiligen Dienstort aus und ist arbeitstechnisch durch die Nutzung moderner Kommunikationsplattformen höchst flexibel. Er arbeitet zeitweilig an der Problemlösung unterschiedlichster Fälle innerhalb und außerhalb seines Zuständigkeitsbereichs mit. Damit gäbe es in Teilen eine Abweichung vom derzeitigen Personaleinsatzmanagment, das sich aktuell am lokalen Kriminalitätsanfall orientiert.

Auswirkungen in Bereichen Personal – Organisation- Technologien!

Ermittlungen müssen flexibel angepasst werden

- Aufgrund der Vielzahl der Kommunikationsmittel sind künftig in allen größeren Verfahren Kommunikationsanalysen erforderlich
- „Cyber Profiling" als Ermittlungsbegleitung standardisieren
- Entwicklung bzw. Nutzung neuer digitaler Internet Forensic tools
- länderübergreifender Kommunikationsplattformen für IT-Ermittlungsverfahren (Test zwischen NRW und BW)

Spezialisierte und modulare Ausbildungskonzepte

- Ermittlungskompetenzen in „digitalen Umfangsverfahren"
- Spezielle Erfahrung im Umgang mit Massendaten
  Weiterentwicklung von Überwachungstechniken vor dem Hintergrund von Mindestspeicherdaten, Kryptografie, Steganographie
- Umgang mit neuen digital forensic tools
- Kenntnis und Verständnis der Internet-Protokolle

Spezialisierte und modulare Ausbildungskonzepte II

- spezialsierte teamorientierte Expertisen (Windows, Linux, MacOs, Betriebssysteme für mobile Systeme wie Windows Mobile oder Windows Phone, iOS (iPhone und iPad), Android), Netzwerk- und Servertechnik (Programmierabläufe, Funktionsweisen von DDOS-Attacken und deren Verhinderung, Einsatz von Servertechniken (Betriebssystem, HTML Server, SQL-Injektion), Datenbanktechnik (Kenntnisse z.B: MySQL, PostgreSQL, Access, Oracle, MSQL-Server, Dbase, Arbeitsweise der SQL-Sprachen)
- Cloud Computing (Entwicklung im Vergleich zur bisherigen Servertechnik)
- Social Networking (W-Fragen: Instrument des Cyber Profilings i.S. digitaler Informationen zu Identität und Persönlichkeit von Personen)

Phänomenbezogene Prävention nur vernetzt und fachlich hinterlegt

Vernetzte Prävention muss im Bereich Cybercrime auch von den Spezialdienststellen umgesetzt werden.
In Hannover gibt es aktuell folgende Initiativen:

- Cyber licence – der Medienführerschein (www.cyberlicence.de)
- Aufsuchende Prävention in Unternehmen des Mittelstands in der Region Hannover (Korruption, IT-Sicherheit, Spionage)
- Vernetzung mit Unternehmen der IT-Sicherheit

Situatives staatliches Risc- und Business-Continiue-Management in Bezug auf Cyber-Angriffe

Welche Aufgaben haben Polizeibehörden neben anderen Behörden und Institutionen im Falle eines gezielten „Cyberangriffs" nach dem Vorbild „Stuxnet" auf ein Unternehmen wie z.B. Energieversorger, Verkehrsunternehmen (Luft, Land, Wasser), Wasserversorger, Chemieunternehmen, Telekommunikationsunternehmen, oder Unternehmen im Finanz- oder medizinischen Sektor) im Bereich der Gefahrenabwehr und der Strafverfolgung wahrzunehmen?

Schlussbemerkung

Das WEB 2.0 hat die Transitivität innerhalb der Subnetze des WWW (z.B. auch Netzwerke von Cyber-Kriminellen) deutlich erhöht. Dies hat den früheren Vorsprung der Sicherheitsbehörden (insbesondere IT-basierte Informationsverarbeitung und länderübergreifende Zusammenarbeit im Rahmen IKPO, Europol, EU, sonstige bi- oder multilaterale Kooperationen) zugunsten der Cyber-Kriminellen umgekehrt.

Die Sicherheitsbehörden werden im Bereich der Cyber-Kriminalität nur wieder Anschluss finden, wenn alle Beteiligten ebenfalls nach dem Prinzip gesteigerter Transitivität vorgehen (wissens- und bedarfsorientierte Zusammenarbeit auf allen Ebenen).

Die staatlichen Sicherheits- und Justizbehörden haben einen hohen Anpassungsdruck und müssen neben der Technologieweiterentwicklung insbesondere Teile ihrer Arbeitsorganisation und ihrer Mitarbeiterqualifikation im Bereich Cybercrime vorrangig überdenken.

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!