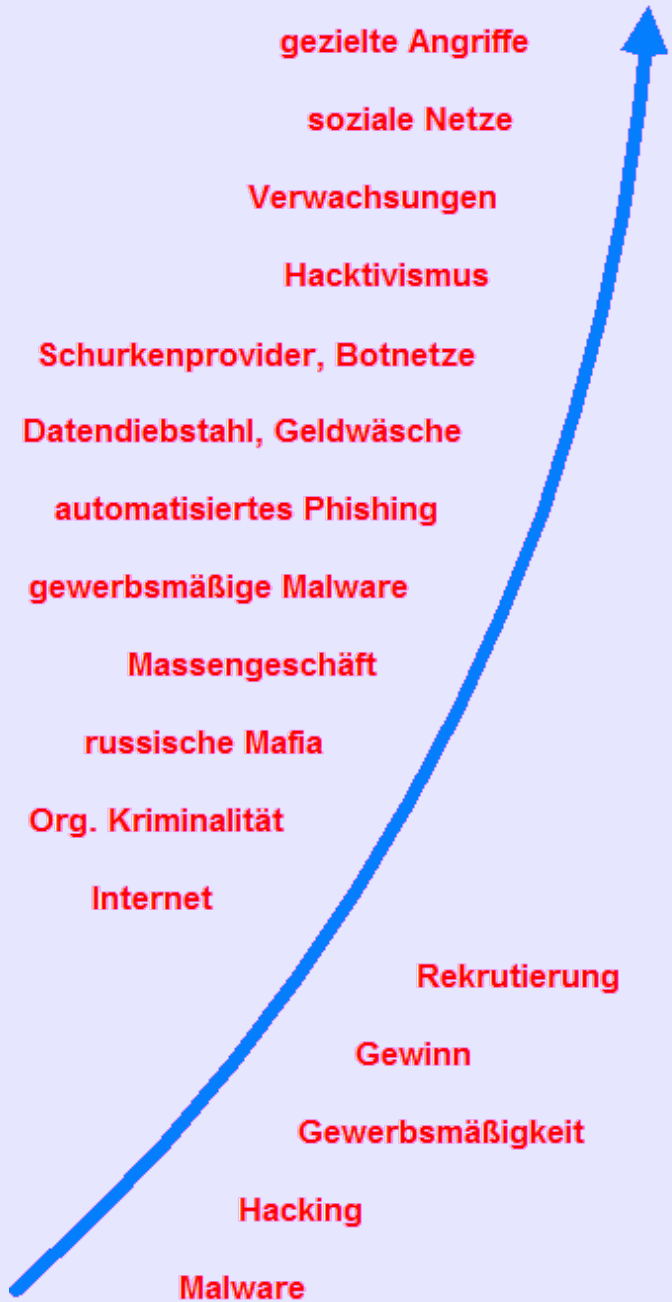
Dieter Kochheim

Cybercrime - Cyberwar

Vita

In der im Internet frei veröffentlichten Version wurde die Vita entfernt.

Zeitgeschichte der Cybercrime



gezielte Angriffe	2010: Aurora, Night Dragon, Stuxnet, WikiLeaks, Anonymous, Reaktionen
soziale Netze	2009: Twitter-Wurm, PirateBay
Verwachsungen	2008: DDoS (Litauen, Georgien), Online-Phishing, RBS WorldPay
Hacktivismus	2007: Pharming, Estland, Malware-Baukästen
Schurkenprovider, Botnetze	2006: RBN, Gozi-Botnet, DarkMarket
Datendiebstahl, Geldwäsche	2005: TJX-Hack, Finanzagenten
automatisiertes Phishing	2004: Homebanking-Trojaner, Sasser, TeamEvil, Phishing, Musik-Download
gewerbsmäßige Malware	2003: Hackerschulen, Trojaner-Verkauf
Massengeschäft	2002: Glückspiel, Sportwetten
russische Mafia	2001: CarderPlanet
Org. Kriminalität	2000: Skimming, Defacement
Internet	1998: Virus-Fabriken, Grabbing, Filesharing
Rekrutierung	1997: Green Army, Dialer
Gewinn	1996: Pornographie, Phishing
Gewerbsmäßigkeit	1990: Hackerfabriken
Hacking	1985: KGB-Hack
Malware	1982: Viren

Neuzeit bis 2000

1982	Malware	Viren und Varianten
1985	Hacking	KGB-Hack *(Kuckucksei)*
1990	Gewerbsmäßigkeit	Hackerfabriken in Bulgarien
1996	Gewinnstreben	Pornographie *(USA)* Phishing *(Osteuropa)*
1997	Rekrutierung	Green Army *(Hackerszene in China)* Dialer *(Einwahlhilfen, Mehrwertdienste)*
1998	Internet	Virusfabriken in Russland Grabbing *(Diebstahl von Internetadressen)* Filesharing *(direkter Datentausch)*
2000	Organisierte Kriminalität	Skimming Defacement *(Verunstaltung, Propaganda)*

Hackerschulen, Virusfabriken

Paget:

In Russland begann der Hacking-Boom 1998 infolge der Finanzkrise.
Eine Armee von jungen, gut ausgebildeten Programmierern hatte plötzlich keine Arbeit mehr und sie sahen sich einem Umfeld von Korruption, wirtschaftlichem Niedergang und beginnender Internetkriminalität ausgesetzt. Auch hier entstanden wie in Bulgarien „Virus-Fabriken“.

Carding

2001 russische Mafia CarderPlanet

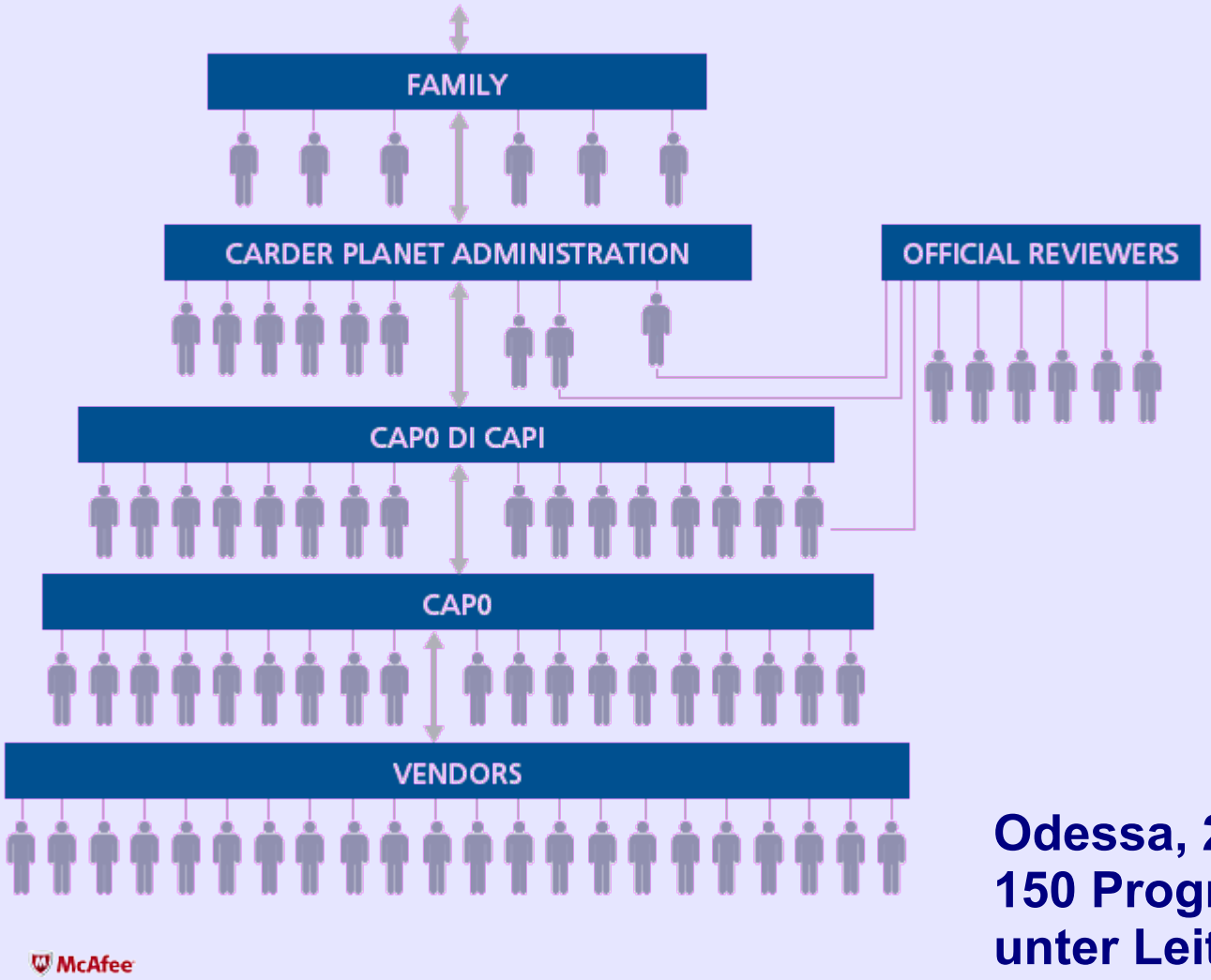
Paget:

Im Mai 2001 trafen sich in Odessa 150 Cyber-Kriminelle und gründeten CarderPlanet. Sein sichtbarer Teil ist ein Forum (CardersPlanet), in dem Zahlungskartendaten von Hackern aus den USA und Großbritannien gehandelt wurden. Diese Daten wurden verkauft oder auf Kommission überlassen, um mit ihnen Internetgeschäfte abzuwickeln oder Zahlungskarten zu fälschen.

Carding = Kreditkartenbetrug

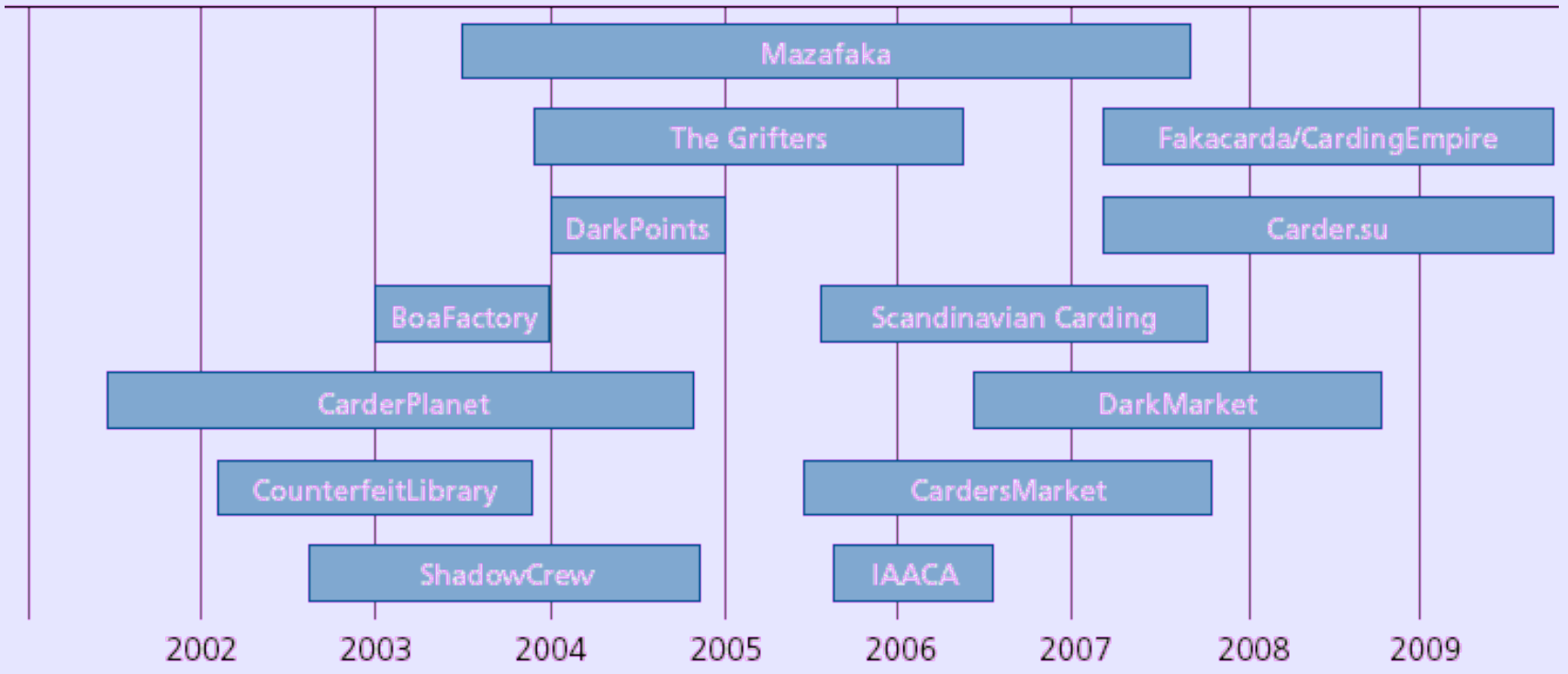
- **Bezahlen mit ausgespähten Kreditkartendaten**
- **Phishing (Onlinebanking)**
- **Skimming (Cashing)**
- **Identitätsdiebstahl im Allgemeinen**

CarderPlanet



Odessa, 2001
150 Programmierer gründen unter Leitung von „Gottvater Dmitry Golubov“ das erste Carding-Board

Carding-Boards



McAfee

geschlossene Benutzergruppen
Gewinnbeteiligung des Veranstalters
Abschottung

Daten, Malware, Exploits, Diplome, Personalpapiere - alles

Neuzeit bis 2005

2002	Massengeschäft	Glückspiel, Sportwetten *vor allem im englischsprachigen Raum*
2003	gewerbsmäßige Malware	Hackerschulen in Moskau Trojaner-Verkauf *(Osteuropa)*
2004	automatisiertes Phishing	Homebanking-Trojaner Sasser TeamEvil *(Hacktisvismus gegen Israel)* Musik-Downloads
2005	Geldwäsche Datendiebstahl	Finanzagenten TJX-Hack *94 Millionen Kundendatensätze beim Finanzdienstleister TJX (USA) gestohlen* *Vertrieb in den Dark Markets*

Pornographie, Glückspiel

Paget:

Mehrere Mitglieder der Gambino-Familie gestanden 2005, von 1996 bis 2002 auf ihren kostenlosen Pornoseiten als Altersnachweis von den Besuchern ihre Kreditkartendaten verlangt zu haben.

Durch deren Missbrauch hätten sie mehr als 750 Millionen US-$ erbeutet.

Paget:

2007 gestand Nicholas "Nicky the Hat" Cimino, seit 2002 einen kriminellen Umsatz von monatlich rund 1 Million US-$ erzielt zu haben.

In Kanada verdiente die Mafia zwischen 2005 und 2006 binnen 18 Monaten 26 Mio. Dollar mit betwsc.com, einer illegalen Seite für Sportwetten. Der Server befand sich in Belize und später in der indianischen Reservation of Kahnawake, westlich von Montreal in Québec. Die wichtigste Person hinter der Betrug soll einen persönlichen Gewinn von 17 Mio. C-$ erzielt haben.

TJX-Hack

Paget:

TJX: Zwischen 2005 und 2007 wurden von 94 Mio. Kunden dieses Unternehmens aus Nordamerika und Großbritannien die Kreditkarten-Nummern gestohlen. Im August 2008 wurden elf Personen verhaftet, darunter drei US-Bürger, ein estnischer, zwei chinesische, ein weißrussischer Täter und drei Ukrainer. Nach Medienberichten waren sie Teil eines internationalen Hacker-Netzwerks, das in das Funknetzwerk (Wi-Fi) und in die Daten der leitenden Angestellten eingedrungen war.

Neuzeit bis 2006

2006 **Schurkenprovider** *(Rogue Provider)*

Russian Business Network *(St. Petersburg)*

Bullet-Proof-Dienste

- technische Verschleierung
- DNS-Protection
- Aliasnamen, Scheinfirmen
- keine Auskünfte an Dritte

- stabile Anbindung an das Internet
- technische Infrastruktur
- soziokulturelle Einbindung

Schurkenprovider

Balduan (2008):

Die Rogue Provider werben mit „bullet proof hosting“, also versprechen im Prinzip, dass sie Ermittlungen von Strafverfolgern nicht übermäßig unterstützen und dass sie auf Missbrauch-Beschwerden nicht reagieren.

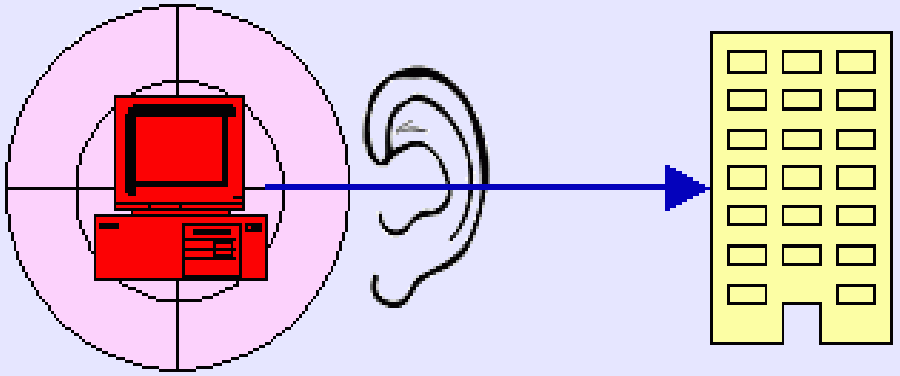
Das ... Geschäftsmodell des RNB war simpel und dreist: Je mehr eine Domain in den Fokus der Öffentlichkeit geriet, je mehr Beschwerden an die E-Mail-Adresse für Missbrauch geschickt wurden, desto mehr Geld verlangten die Russen von ihren Kunden.

***Paget:* … etwa 600 $ im Monat.**

Schurkenprovider:

- **vollwertiger Internetprovider Autonomes System - AS**
- **Bullet Proof Hosting „sichere“ Speicherplätze für Boards, Daten, „Drops“, Pharmen, Malware.**
- **DNS-Protection Verschleierung der Domaininhaber**
- **Beschwerderesistenz**
- **Scheinfirmen**
- **Geldverkehrsabwicklung**
- **gesellschaftliche Einbindung**

Identitätsdiebstahl



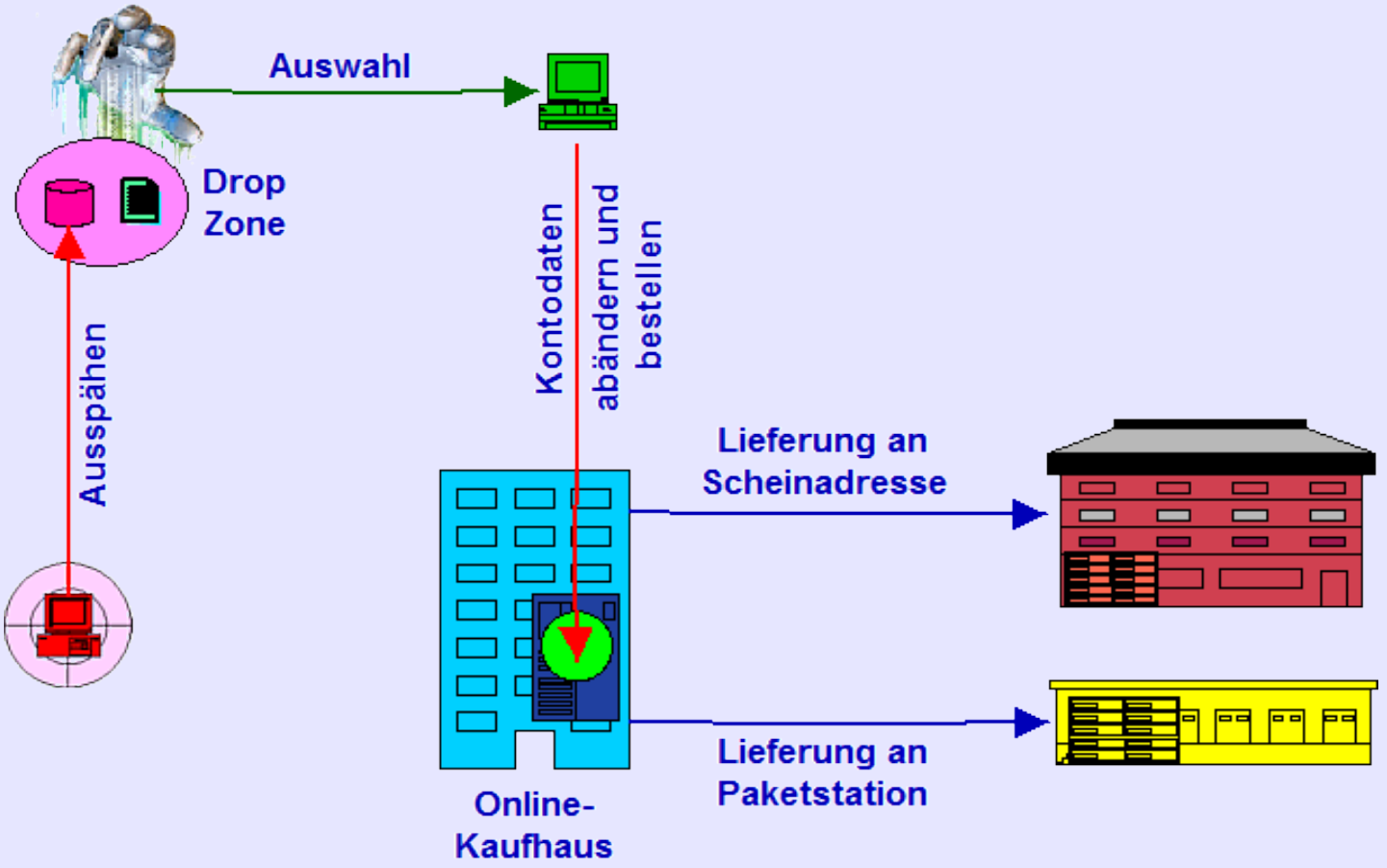
alle persönlichen Daten, die einen Wert auf dem Schwarzmarkt haben

- **Onlinebanking (Phishing)**
- **Handelskonten (Kaufhäuser, Amazon, eBay, PayPal)**
- **Sozialversicherung (USA)**
- **Personalpapiere**

Phishing

- **E-Mail-Formulare zur Eingabe der Kontodaten, PIN, TAN**
- **Spyware Trojaner mit Keylogger und Suchfunktionen DropZone**
- **Online-Phishing Man-in-the-Middle**

Beutesicherung



- Finanzagenten
- Warenagenten
- Fake-Bankkonten
- Bezahlsysteme

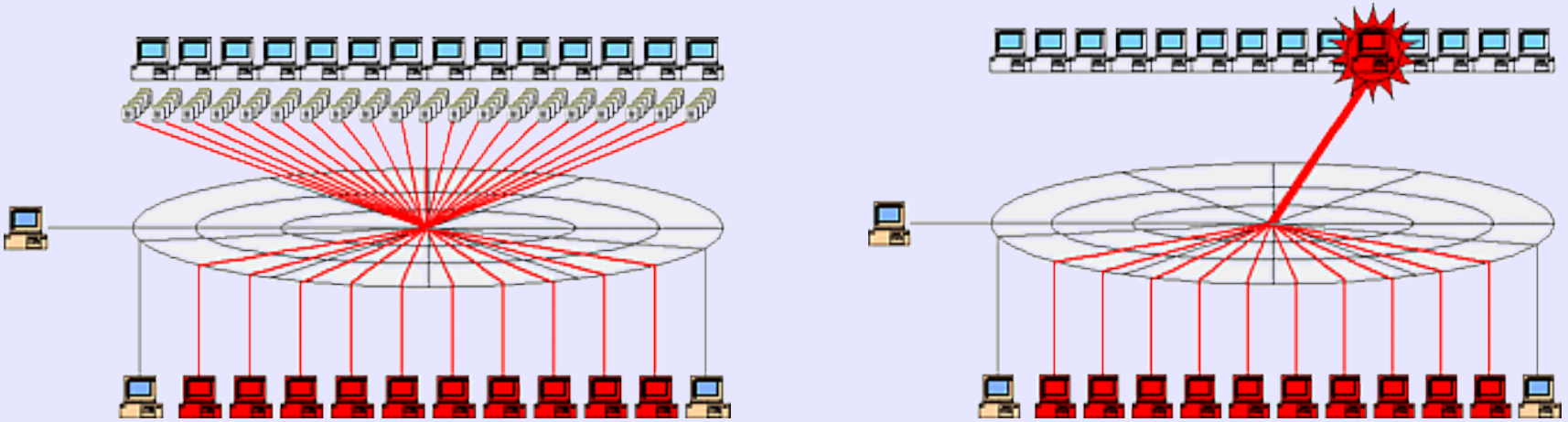
Neuzeit bis 2006

2006 Botnetze

Gozi-Botnet

Fernsteuerung einer Vielzahl von Zombies
- Malware, Exploits, Rootkits
- Fernwartung, Filesharing

- Spam, Malwareverbreitung
- verteilte Angriffe *(DDoS)*
- Auspähen
- Kontrolle *(CC-Server, Webserver)*



Projektmanagement

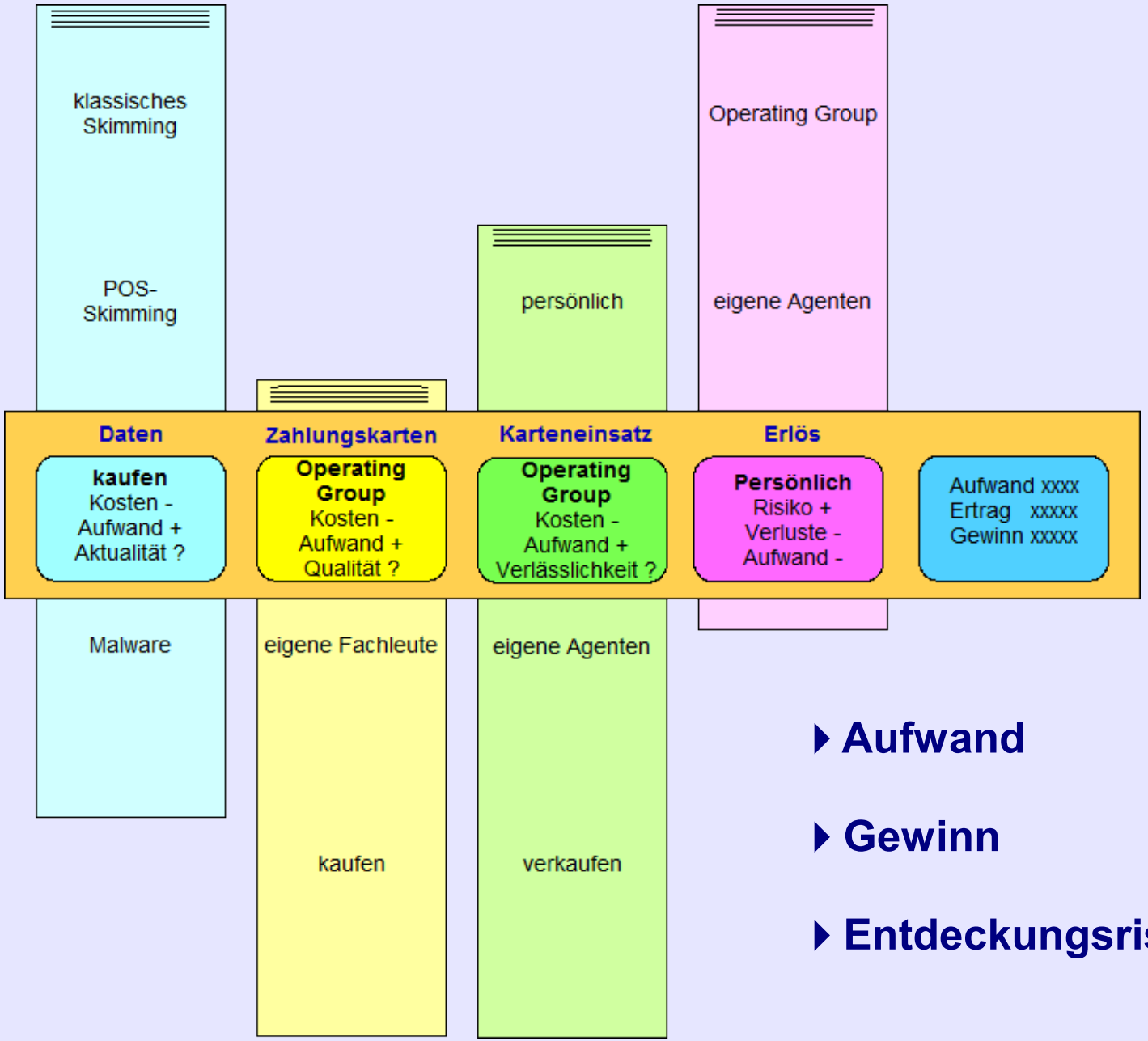
2006 **kriminelles Projektmanagement**

Koordinatoren

Balduan

Die zentrale Figur jedoch ist ... ein „Independent Business Man“ – eine Person, die Kontakte zur Unterwelt pflegt und zwischen Bot-Herdern, Hackern, Malware-Schreibern und Spammern koordiniert. ... mithilfe der Botnetz-Infrastruktur kann der Koordinator Unternehmen mit verteilten Massenangriffen auf ihre Webseiten drohen und so Schutzgeld erpressen, Spam-Wellen mit Werbung für überteuerte Produkte oder Aktien lostreten oder tausendfach persönliche Informationen wie Bankzugangsdaten ergaunern.

Kalkulation



- **Aufwand**
- **Gewinn**
- **Entdeckungsrisiko**

Operation Groups

2006 **kriminelles Projektmanagement**

Operation Groups

Balduan

Die Zwischenhändler bezeichnet Balduan als Operation Groups. Sie haben ihre Kontakte und Leute, auf die sie bei jedem Auftrag zurück greifen können. Sie und besonders ihre leitenden Unternehmer erleichtern das Geschäft für alle Beteiligten. Die Spezialisten müssen sich nicht um ihre Vermarktung kümmern und die Auftraggeber nicht darum, den richtigen Spezialisten oder Zulieferer zu finden.

Die Cybercrime organisiert sich dadurch arbeitsteilig und marktmäßig - um Straftaten zu ermöglichen und durchzuführen.

Organisierte Internetverbrecher

McAfee
Zweite große europäische Studie über das Organisierte Verbrechen und das Internet (2006)

Die Täter der Internetkriminalität reichen heute von Anfängern mit nur eingeschränkten Programmiererkenntnissen, die ihre Angriffe nur mit vorgefertigten Skripts durchführen können, bis hin zu gut ausgebildeten professionell arbeitenden Kriminellen, die über die aktuellen Ressourcen verfügen.

Wie in den meisten Gemeinschaften erfolgreicher Krimineller sitzen tief im Inneren einige streng abgeschirmte Köpfe, die sich auf die Mehrung ihrer Gewinne mit beliebigen Mitteln konzentrieren. Sie umgeben sich mit den menschlichen und technischen Ressourcen, die dies ermöglichen.

McAfee
Zweite große europäische Studie über das Organisierte Verbrechen und das Internet (2006)

- Innovatoren; Gefahr: gering.
- ruhmgierige Amateure und Nachahmer, Gefahr: Mittel.
- Insider; Gefahr: hoch.
- Organisierte Internetverbrecher; Gefahr: hoch.

Neuzeit bis 2009

2007	Hacktivismus	verteilter Angriff gegen Estland Pharming Malware-Baukästen
2008	Verwachsungen	verteilte Angriffe gegen Litauen und Georgien Online-Phishing RBS WorldPay
2009	soziale Netze	Twitter-Wurm PirateBay

RBS World Pay

Heise:

Ende 2008 wurde ein Angriff auf den Finanzdienstleister RBS World Pay bekannt, der für Unternehmen die Auszahlung von Lohngeldern vornimmt. Dabei hatten die Eindringlinge laut RBS die Daten von 100 Karten ausspioniert.

Die Kriminellen haben das Geld am 8. November 2008 von 130 Geldautomaten in 49 Städten weltweit, darunter Atlanta, Chicago, New York, Montreal, Moskau und Hongkong im 30-Minuten-Takt abgehoben. Das besondere an dem Coup: Normalerweise ist die Summe der Auszahlungen am Automaten pro Tag begrenzt. Vermutlich hatten die Hacker bei dem Einbruch in das Netz von RBS aber nicht nur die Daten gestohlen, sondern auch die Limits manipuliert.

Quelle:
Kriminelle stehlen 9 Millionen Dollar in weltweitem Coup, Heise online 06.02.2009

Neuzeit bis jetzt

2010 **gezielte Angriffe**

Eskalation

Industriespionage
- **Aurora *(Ausspähen, Google)***
- **Night Dragon *(Petrochemie, VPN-Tunnel)***

Sabotage mit Malware
- **Stuxnet**
  (iranische Atomanlagen, industrielle Steuerungen)

alternative Wirtschaft
- **WikiLeaks, Whistleblowing**
  (Afghanistan, Irak, Depeschen; DoS)

Hacktivismus
- **Anonymous *(DoS gegen Amazon, professionelles Hacking)***

Internet-Wirtschaft
- **gewerbliche Exploithändler**
- **IT-Söldner *(HBGary Federal)***

Aurora

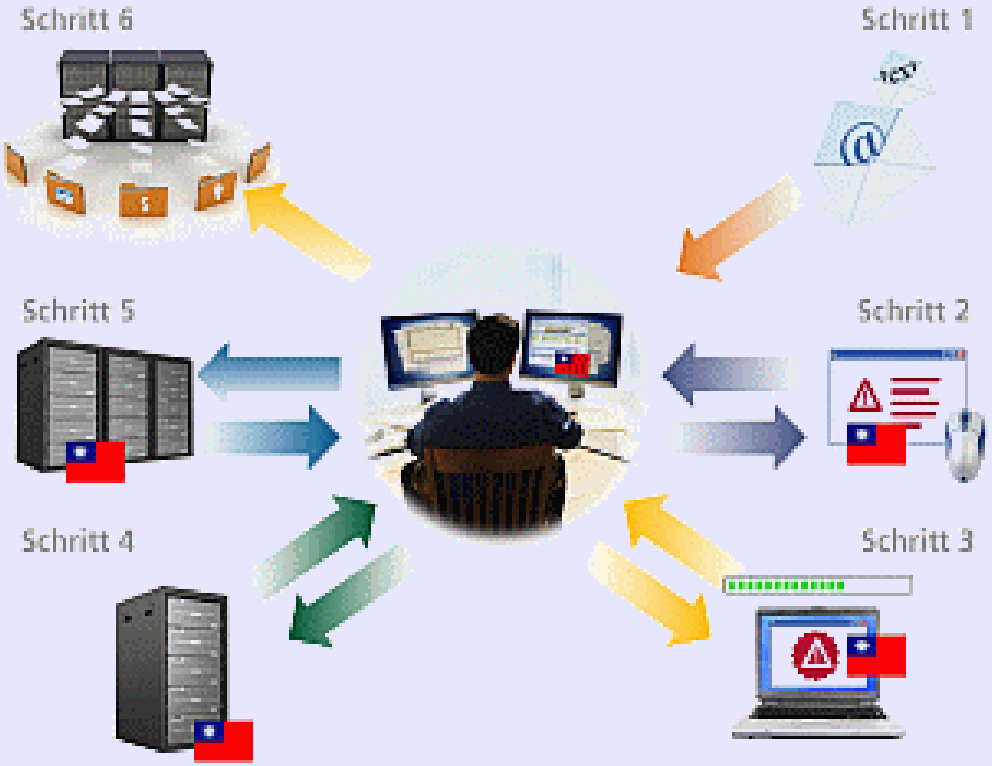
Aurora:

Gezielter Angriff chinesischer Herkunft gegen Google und rund 30 weitere Unternehmen Anfang 2010.

Ziel: vertrauliche Unternehmens-informationen, Industriespionage

Weg: gestufter Angriff

- **E-Mail**
- **Link zu infizierter Website**
- **Starter injiziert Exploit in Browser**
- **Download von Malware, die als Grafik getarnt ist**
- **Verbindung mit einem Botnetz in Taiwan**
- **Datenzugriff**
- **Ausbreitung im lokalen Netz**



Besonderheiten:

- **Zero-Day-Exploit**
- **detaillierte Kenntnisse über die IT-Infrastruktur der angegriffenen Unternehmen**

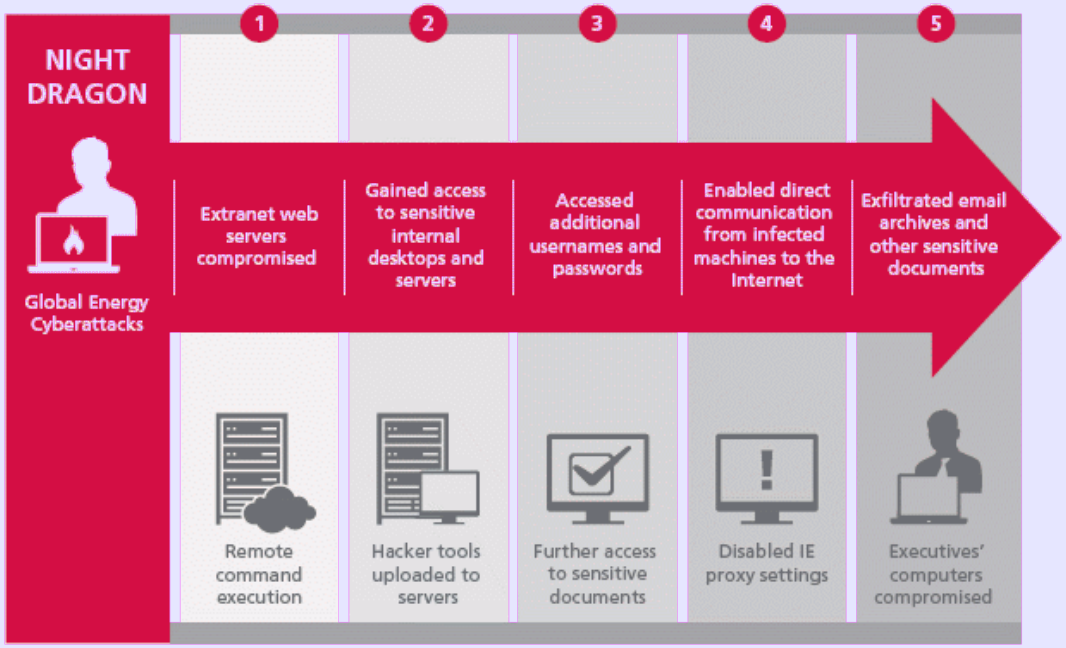
Quelle: McAfee

Night Dragon

Night Dragon:

Gezielter Angriff chinesischer Herkunft gegen Energie- und Ölverarbeitende Unternehmen seit Herbst 2009.

Ziel: Informationen über Reserven, Fördermengen, Strategien.



Weg: gestufter Angriff

- SQL-Injection gegen Webserver
- Infiltration des Active Directory
- Abschalten des Proxyservers
- Abschalten der Sicherheitsein-stellungen im Browser
- Fernzugriff aus China mit Command & Control - Server
- Durchgriff auf mobile Endgeräte durch VPN-Tunnel

Besonderheiten:

- besondere Kenntnisse über die IT-Infrastruktur der angegriffenen Unternehmen
- Infiltration gesicherter Netzverbindungen

Quelle: McAfee

Stuxnet

Stuxnet:

gezielte Sabotage der iranischen Atomanreicherungsanlage in Natanz

mindestens zwei Programmierer-teams seit 2007

keine Programmierer aus der Malware-Szene (Israel, USA)

Infiltration per USB-Sticks bei Mitarbeitern von Firmen, die am Bau der Atomanlagen beteiligt sind (seit Sommer 2009)

erfolgreiche Verzögerung und Behinderung der Fertigstellung

Stuxnet

Stuxnet:

- autonome Malware
- keine Anbindung ans Internet
- mehrere Schwachstellen, die bis zum Sommer 2010 unbekannt waren – Zero-Day-Exploits
- bislang unbekannte Rootkits
- gezielte Sabotage von mindestens zwei Industrieanlagensteuerungen von Siemens („Sprengköpfe“)
- Einkaufskosten allein für Exploits und Rootkits: sechsstellig
- Gesamtkosten: siebenstellig

Der Quellcode fand reges Interesse bei den Entwicklern von Malware und bei IT-Söldnern

WikiLeaks

WikiLeaks:

gegründet 2006
Whistleblowing-Plattform für regimekritische Dokumente aus China und anderen totalitären Staaten.

bis 2009:
vor Allem Einzeldokumente

Berico, HBGary Federal, Palantir

WikiLeaks ist keine Einzelperson und keine einzelne Organisation, sondern ein Netzwerk aus Personen und Organisationen, die nur deshalb zusammenarbeiten, um nicht nachverfolgbar massenhaft vertrauliche Dokumente zu veröffentlichen.

John Young

Wikileaks ist eine Geschäftsorganisation, die vorgibt, eine gemeinnützige Organisation zu sein.

WikiLeaks

2010 – Schlag auf Schlag

- Video aus der Kamera des Bordgeschützes eines Hubschraubers: Beschuss von irakischen Zivilisten und Journalisten
- Afghanistan-Krieg
- Irak-Krieg
- diplomatische Depeschen
- Guantanamo-Protokolle (April 2011)

Reaktionen auf WikiLeaks

Reaktionen auf WikiLeaks:

- CIA, März 2008:
  unterminieren, zerstören
- November 2010
  - Amazon, Sperrung Hostspeicher
  - DDoS gegen WikiLeaks
- Dezember 2010
  - Sperre gegen wikileak.org
  - mehr als 1.000 Mirrors
  - Kontensperren
  - Anonymous:
    DDoS gegen Amazon und Banken
- Januar 2011:
  - HBGary Federal:
    Analyse Anonymous-Anhänger
  - Palantir u.a.
    aggressive Strategie gegen WikiLeaks
- Februar 2011:
  - Anonymous hackt
    HB Gary Federal

Anonymous

kopfloses Kollektiv

besteht aus kleinen stabilen Gruppen und Einzelpersonen

2008: Aktionen gegen Scientology

2010: DDoS gegen Org. Amerikanischen Filmproduzenten – MPAA – und AiPlex Software

Operation Payback

Nachrichtenportal Crowdleaks (zunächst: Leakspin)

Hack gegen HBGary Federal

2011: Unterstützung des Aufstandes in Ägypten

OPSony, OPRecon

Payback, die neue Dimension:

Ein radikaler Teil der Internetgemeinde fordert die Einhaltung von Spielregeln ein! Unternehmen wie Amazon und große Finanzdienstleister können sich nicht mehr wie gewohnt selbstgerecht zurücklehnen, sich auf mehr oder weniger berechtigte AGB-Verstöße berufen, die ihnen so lange nicht aufgefallen sind, wie sie noch in Ruhe Geld verdienen konnten, oder gefahrlos politischem Druck aus dem Mainstream nachgeben. Die Angriffe von Anonymous machen sie zum Angriffsobjekt alternativen Wohlverhaltens. Das ist schmerzhaft!

Gegendruck

Manfred Messmer

Kein Staat, kein Unternehmen, keine Rechtsordnung kann akzeptieren, dass ein anarchistischer Schwarm von ein paar Tausend Usern sich auf willkürlich ausgewählte Unternehmen, staatliche und private Organisationen stürzt und deren Webseite – das heißt heutzutage deren Geschäftstätigkeit – für Stunden oder gar Tage lahmlegt.

Exploit-Handel

Exploit-Händler

- HP Tipping Point
- iDefense (Verisign)
- Vupen

Luigi, das kostet Dich etwas!

Das französische Unternehmen Vupen erstellt potenziellen Kunden eine Sicherheitsanalyse. Wenn der Kunde aber nicht zahlt, dann erhält er keine weiteren Informationen über die gefundenen Schwachstellen oder ihre Abwehr.

In der Branche wird ein bisschen von Erpressung gemunkelt.

Quelle: c't

IT-Söldner

Empfehlungen von Palantir, HBGary Federal und Berico:

- Gießen Sie heißes Öl zwischen die befeindeten Gruppen.
- Desinformation. Erstellen Sie Nachrichten über die Aktionen, um sie zu sabotieren oder die gegnerische Organisation zu diskreditieren. Nutzen Sie gefälschte Unterlagen und beschweren Sie sich dann über die Fehler.
- Zeigen Sie die Mängel in der Sicherheit der Infrastruktur.
- Schreiben Sie entlarvende Geschichten. Wenn Sie Glauben finden, dass der Gegner unsicher ist, dann ist er fertig.
- Cyber-Angriffe gegen die Infrastruktur zur anonymen Einsendung von Dokumenten. Dies würde das Projekt töten. …
- Medien-Kampagnen, um die radikale und rücksichtslose Natur der Wikileaks-Aktivitäten offenzulegen. Anhaltender Druck.
- Tut nichts gegen die Fanatiker, aber sät Bedenken und Zweifel unter den Gemäßigten.
- Sucht nach Lecks. Verwenden Sie soziale Medienprofile und identifizieren Sie riskantes Verhalten Ihrer Mitarbeiter.

professionelles Hacking

HBGary Federal

Informationsüberwachung des Datenverkehrs in Firmennetzen

Eindringen in fremde Datennetze (Exploits, Rootkits, Spionage)

Infiltration sozialer Netze mit künstlichen Persönlichkeiten

Auswertung von sozialen Netzen

Personifizierung von Anonymous-Anhängern

Anonymous-Hack

professioneller Angriff

Social Engineering

Veröffentlichung der Recherchen von Aaron Barr und der Firmen-Mails

graue Bezahlsysteme

Geldtransfer
- Western Union
- MoneyGram
- MoneyBookers

Verrechnungssysteme
- eGold, eSilver, ePlatinium
- WebMoney
- MoneyBookers
- Neteller

Bezugsscheine
- PaysafeCard
- ukash

Kreditkarten auf Guthabenbasis
- Wechselstuben
- vereinzelt keine Identitätsprüfung
- Beute aus dem Geldautomaten an der nächsten Ecke

eigene Bank gründen

Konto unter Alias

Gegenwehr

2007: Israelischer Luftangriff auf in Syrien vermutete Atomanlagen
begleitet von einem Totalausfall der syrischen Radarabwehr

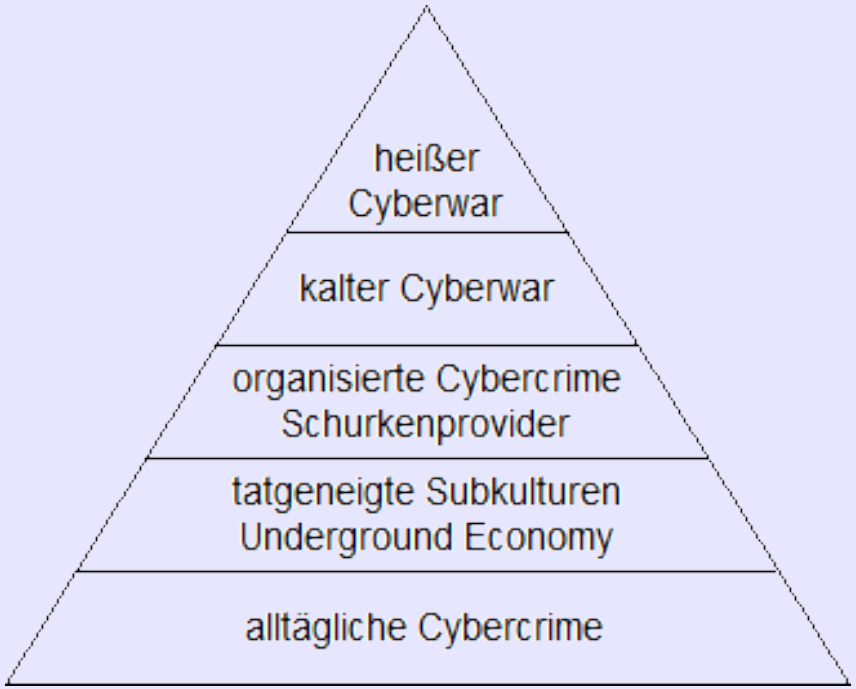
2009: McCollo abgeschaltet
Spam-Aufkommen deutlich verringert

2011: Rustock-Botnetz abgeschaltet
auf Initiative von Microsoft

2011: Cyber-Abwehrzentrum unter Leitung des BSI

2011: Cybergenom-Projekt der DARPA
digitaler Fingerabdruck Trojaner in jedem elektronischen Bauteil Hardware Trojanische Pferde - HTH

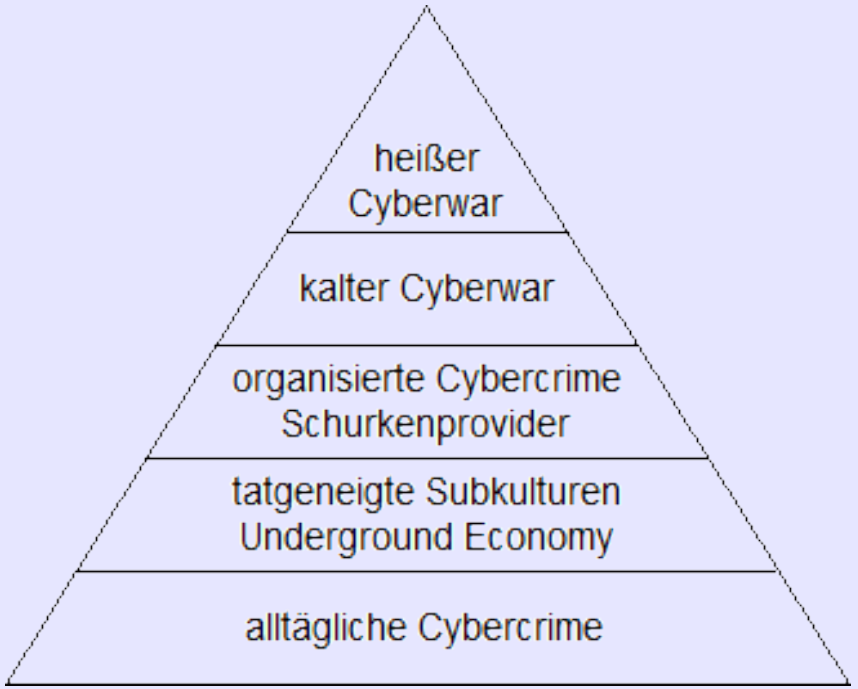
Entwicklungsmodell Cybercrime-Cyberwar



Myriam Dunn Cavelty

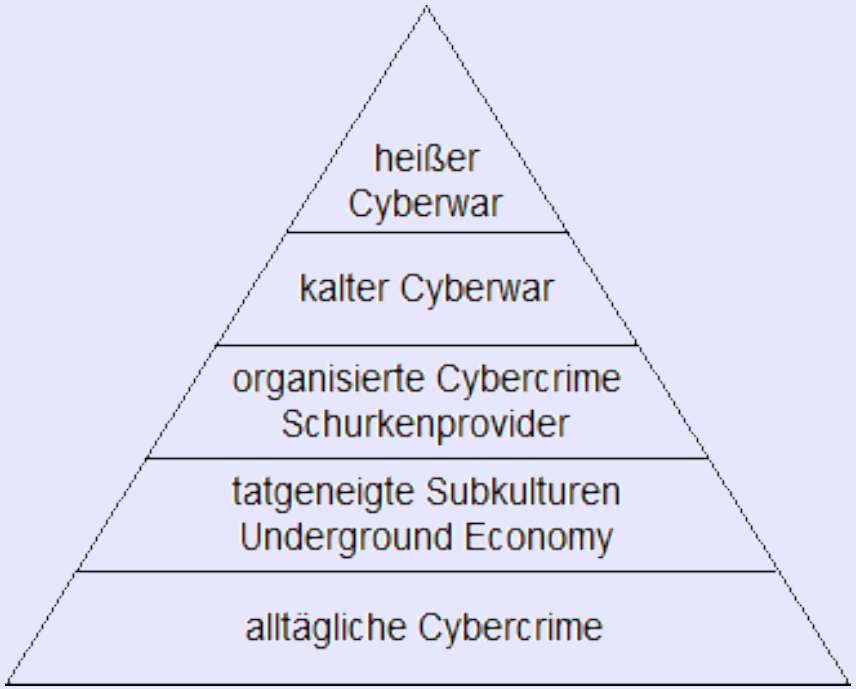
Aber das Verunstalten von Webseiten ist kein Cyberwar. DDoS-Attacken, auch wenn Banken betroffen sind, sind kein Cyberwar. Das Ausspionieren von Regierungsgeheimnissen oder der Klau von Wirtschaftsgeheimnissen mithilfe von Computern ist kein Cyberwar. Elektronische Kriegsführung ist nicht Cyberwar. Das Verbreiten von halb wahrer oder nicht wahrer Information im Krieg ist kein Cyberwar. Nicht einmal die Sabotage einer Industrieanlage mithilfe von ausgeklügelter Malware ist Cyberwar.

allgemeine Internetkriminalität



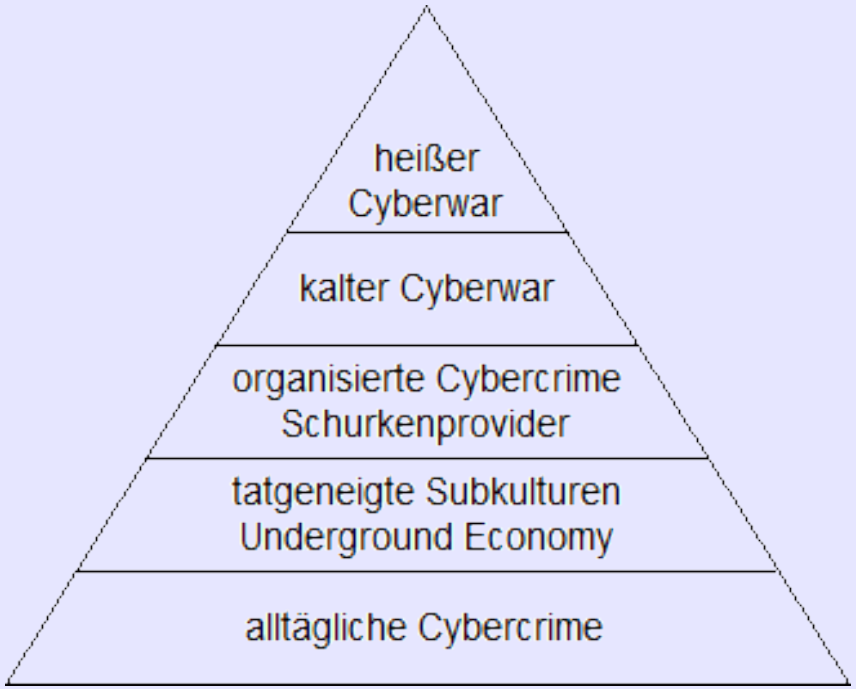
- Datendiebstahl *(Konten, Banking)*
  - Identitätsdiebstahl
  - Phishing
  - Finanzagenten
- „eBay“-Betrug
  - falsche Produktbeschreibungen
  - Vorauszahlungsbetrug
- Warenbetrug
  - falsche Identitäten
  - Fake-Adressen
  - Warenagenten
  - Packstationen
- Carding, Skimming
- Geldwäsche
  - „graue“ Zahlungssysteme
  - Kreditkarte auf Guthabenbasis

gewerbsmäßige Internetkriminalität



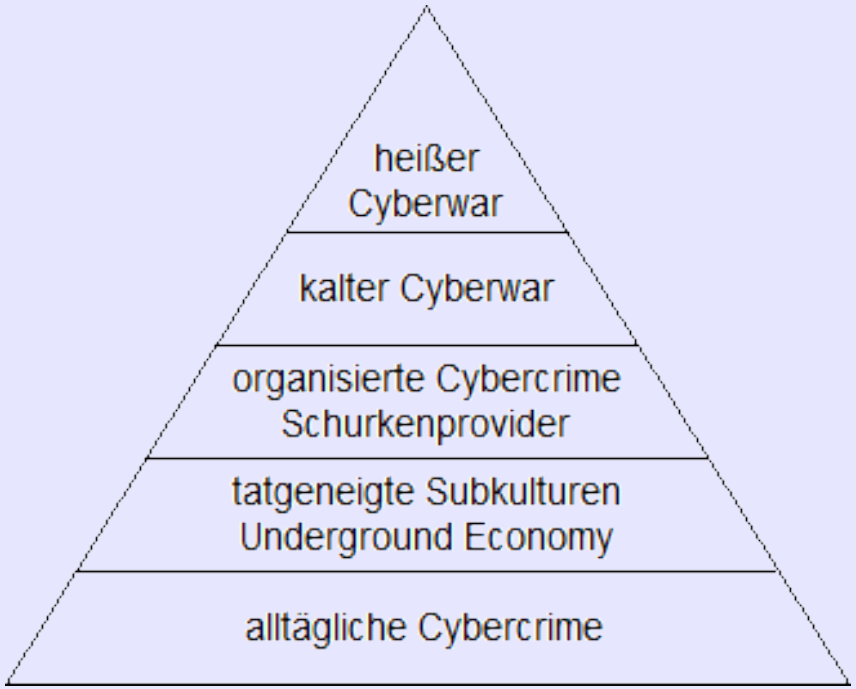
- **Board-Administratoren**
- **Malware-Entwickler**
  (Operating Groups)
- **Exploit-, Rootkit-Händler**
- **Projektleiter *(Koordinatoren)***
- **Webshop-, Inkassodienste**
- **„Wechselstuben“**
- **Hacktivisten**

organisierte Internetkriminalität



- **Board-Betreiber**
- **Botnetz-Betreiber**
- **Schurkenprovider**

kalter Cyberwar

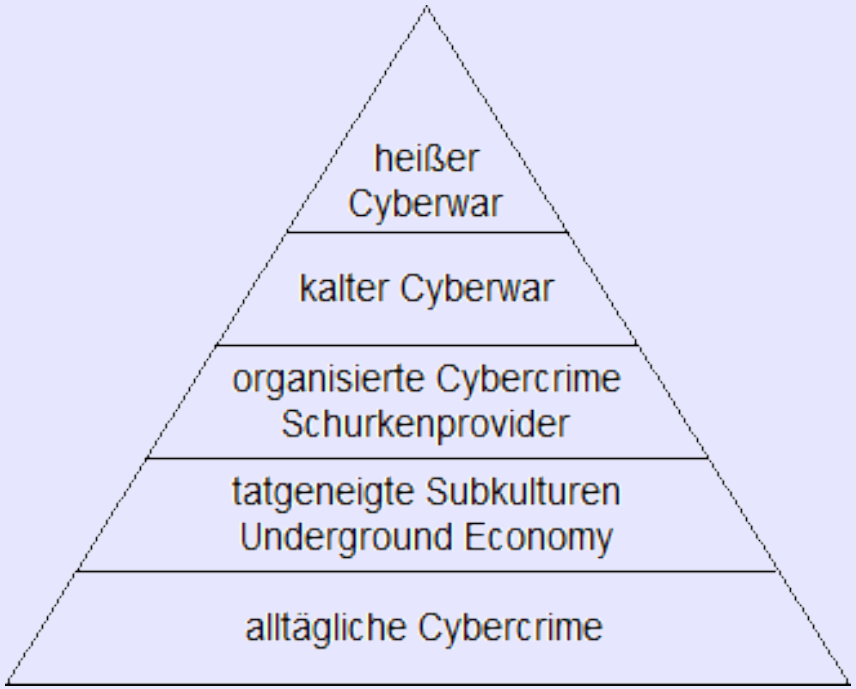


taktische Phase des Kräftemessens
Was kann ich bewirken?
Wie sind die Gegner aufgestellt?
Wie reagieren sie?

weitere „Mitspieler“

- **organisierte Kriminalität**
- **Nachrichtendienste**
- **Militär**
- **Paramilitär**
- **Terroristen**
- **Hacktivisten**
- **Wirtschaftsunternehmen**
- **Söldner**

heißer Cyberwar



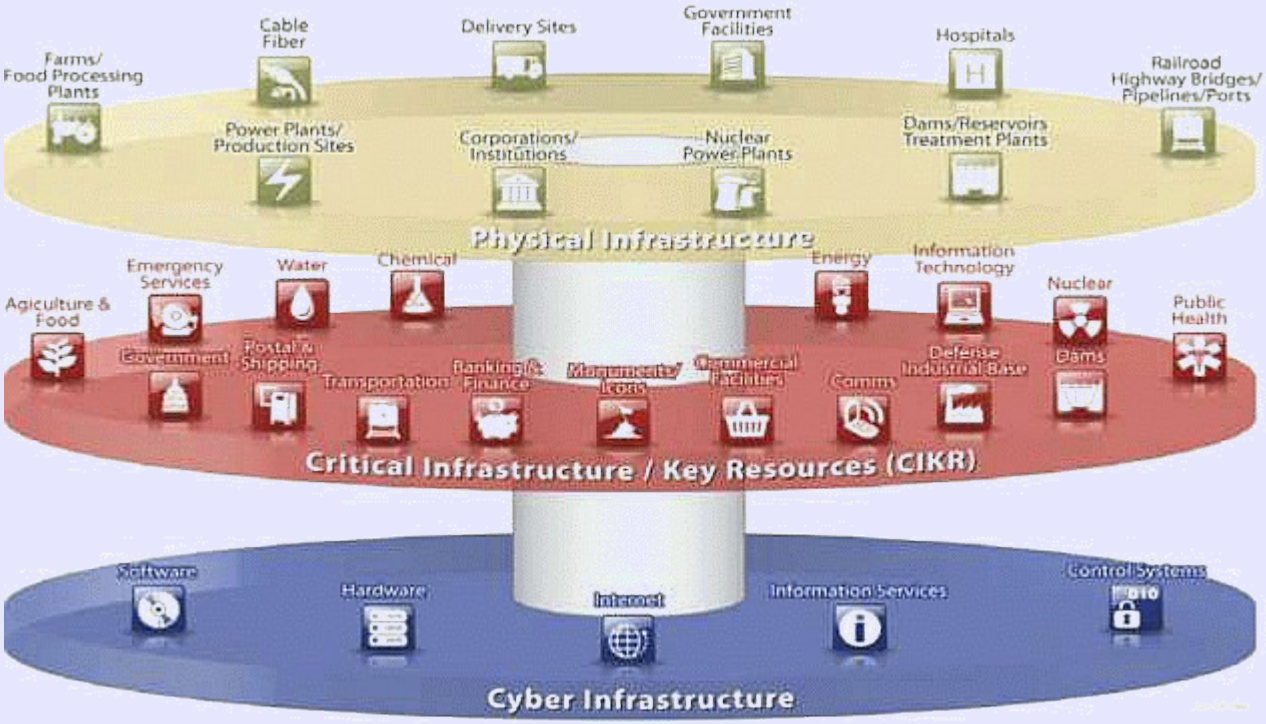
Cyberwar ist der strategische Einsatz der Informations- und Kommunikationstechnik mit dem Ziel, Gegner und Opfer existenziell zu schädigen, also nicht nur ihre Datenverarbeitung und Netzkommunikation zu stören oder auszuschalten, sondern ihre Funktionstüchtigkeit insgesamt.

Erst in der Heißen Phase des Cyberwar dürften neben den bekannten Methoden der Cybercrime ganz verstärkt terroristische und militärische Einsätze zu erwarten sein.

Kritische Infrastrukturen

Kritische Infrastrukturen

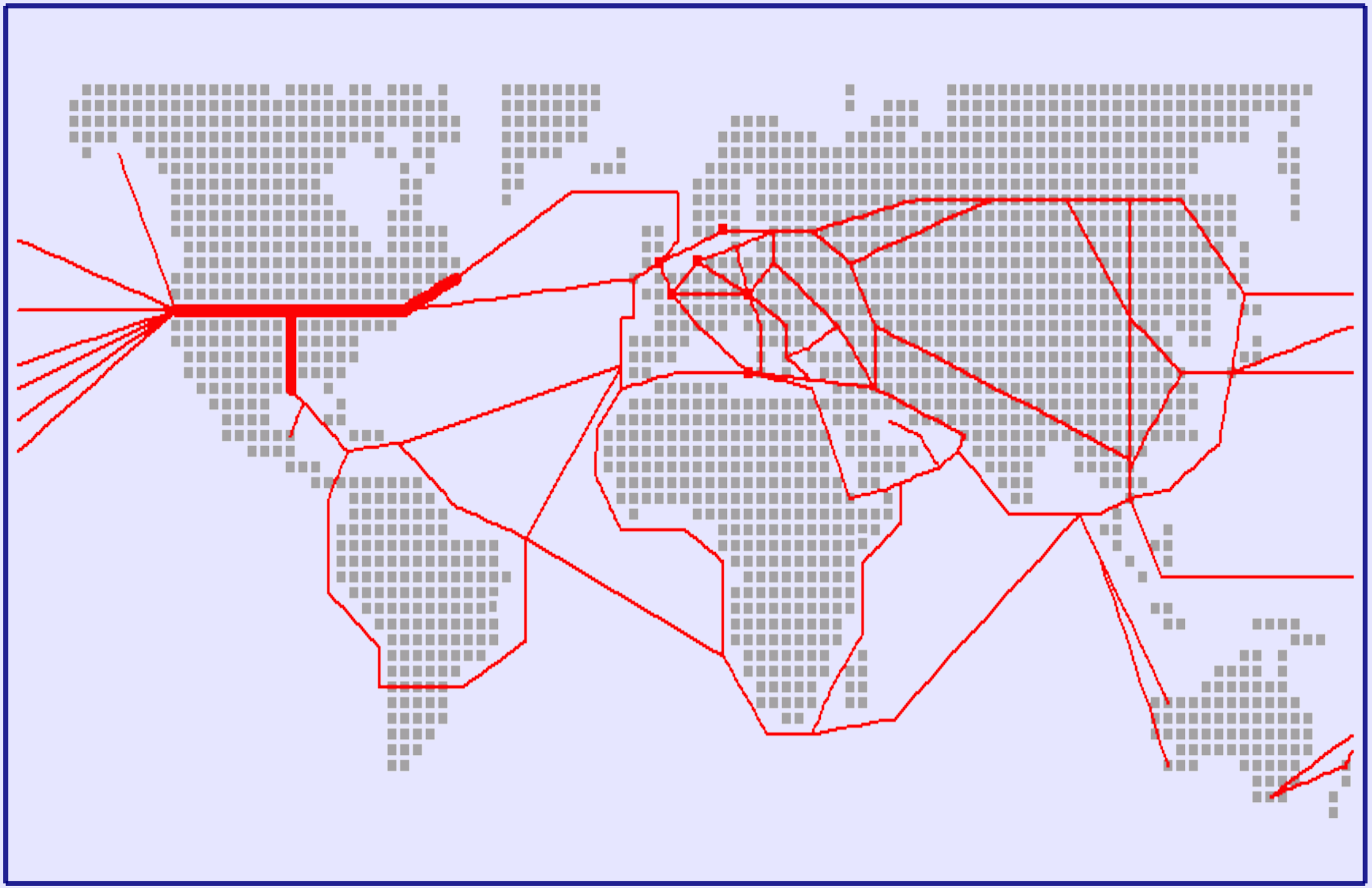
- TK-Ifrastruktur
- produzierendes Gewerbe
- öffentliche Grundversorgung



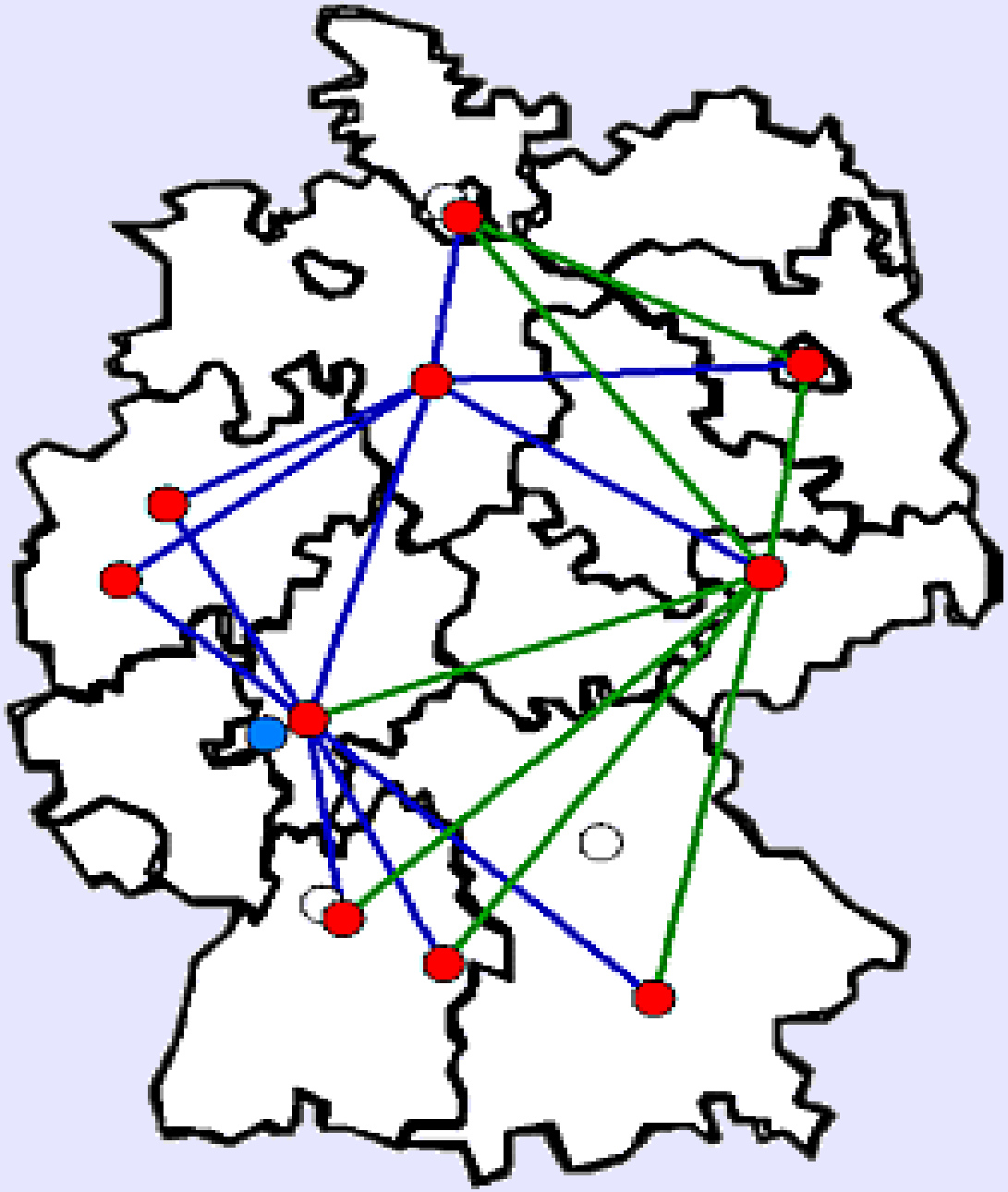
Duale Welt

- gegenseitige Durchdringung
- Abhängigkeiten

„Internetz“



Backbone der DTAG



Cyberwar-Debatte

James A. Lewis

Es ist nicht korrekt, alles gleich als 'Krieg' oder 'Angriff' zu bezeichnen, was im Internet an schlechten Dingen passiert.

Raoul Chiesa

Cyberwar-Aktivitäten sind gezielte Attacken auf eine andere Nation. Diese Angriffe können entweder staatlich gefördert oder durch politische und religiöse Gruppen und Ideale getrieben sein. In jedem Fall ist beim Angriff auf einen Staat die Armee für die Verteidigung zuständig.

Paul B. Kurtz

Die Grenze zwischen Internetkriminalität und Internetkrieg verschwimmt heute immer mehr, weil manche Staaten kriminelle Organisationen als nützliche Verbündete betrachten.

Sandro Gaycken

Schwache Staaten könnten Serien solcher Angriffe nutzen, um die Kräfte starker Gegner kontinuierlich zu schwächen. Es können damit gigantische Ablenkungen produziert werden. Wirtschaften können in langfristigen Operationen geschädigt werden. Es ließen sich Konflikte anheizen, andere Staaten agitieren.

Bedrohungen des Cyberspace

US Air Force, LeMay Center

Akteure

- **nationalstaatliche Bedrohung**

  Sabotage und Blockade von Infrastrukturen

  Spionage

  durch nationalstaatliche Einrichtungen oder beauftragte Dritte

- **transnationaler Akteure**

  grenzüberschreitende Kommunikation

  terroristische Aktionen

- **kriminelle Organisationen**

  stehlen Informationen zum eigenen Gebrauch oder um sie mit Gewinn zu verkaufen.

- **Einzelpersonen und kleine Gruppen**

  akademische Hacker, Schwachstellensucher

  Hacker mit politischen Motiven

  destruktive Hacker (Defacement)

  Malware-Programmierer

Bedrohungen des Cyberspace

US Air Force, LeMay Center

Methoden

- **traditionelle Bedrohungen**

  klassische militärische Konflikte, die normalerweise von anderen Staaten ausgehen

- **irreguläre Bedrohungen**

  asymmetrische Bedrohungen nutzen den Cyberspace, um mit unkonventionellen Mitteln traditionelle Vorteile zu erzielen

  Guerilla-Operationen

- **katastrophale Bedrohungen**

  Umgang mit Massenvernichtungswaffen

- **disruptive Bedrohungen**

  durch innovative und neue Technologien

- **natürliche Bedrohungen**

  Naturkatastrophen

- **unbeabsichtigte Bedrohungen**

  menschliche Fehler

  Unfälle

Vielen Dank für die Aufmerksamkeit!

Dieter Kochheim

cyberfahnder.de

Anhang:
Rechtspolitische Diskussionspunkte

Struktur der Strafverfolgung

Die Verfolgung der allgemeinen Internetkriminalität ist eine Aufgabe für alle Strafverfolger

- Aus- und Fortbildung
- Informationsaustausch
- technische und rechtliche Unterstützungsdienste

Die Verfolgung der gewerbsmäßigen Internetkriminalität ist eine Aufgabe für spezialisierte Staatsanwälte

- besondere Ausbildung
- personelle und sachliche Ressourcen
- bilden das Personal für die Aus- und Fortbildung

Die Verfolgung der organisierten Internetkriminalität ist eine Aufgabe von Schwerpunkt-Staatsanwaltschaften und Zentralstellen

- Methoden der OK-Ermittlungen
- Koordination
- internationale Zusammenarbeit

Strafverfahrensrecht

Der Strafverfolgung müssen effektive Instrumente zur Verfügung stehen

- Eingriffsvoraussetzungen
- Straftatenkataloge
- Entscheidungsprozesse
  - Vier-Augen-Prinzip
  - Berichtswesen

- Eingriffsermächtigungen
  - nicht offene Personalermittlungen
  - Tarnnamen für Ermittler
  - Einsatz von Privatpersonen
  - Grenzen der Tatprovokation
  - Keuschheitsprobe
- Datensammlung
- Legalitätsprinzip *(Nebentäter)*
- technische Mittel
  - Onlinedurchsuchung
  - aktive Suchprogramme
  - Datenzugriff im Ausland
- Verkehrsdaten
  - Auskünfte über Bestandsdaten
  - Zugriff auf Verkehrsdaten

Strafrecht

Revision des materiellen Cyber-Strafrechts

- **Strafbarkeit im Vorbereitungsstadium**
- **Hardware als Betrugswerkzeug**
- **Datenhehlerei**
- **klare Strukturen**

Vernetzung

kriminalstrategische Aufgaben der Staatsanwaltschaft

- **äußerst stark von der Polizei besetzt**

diensteübergreifende Arbeitsgruppen und Informationsaustausche

- **Verwertbarkeitsprobleme**
- **operatives Cyber-Abwehrzentrum**

internationale Zusammenarbeit

- **vereinfachte Rechtshilfe**
- **Eingriffsmaßnahmen im Ausland**