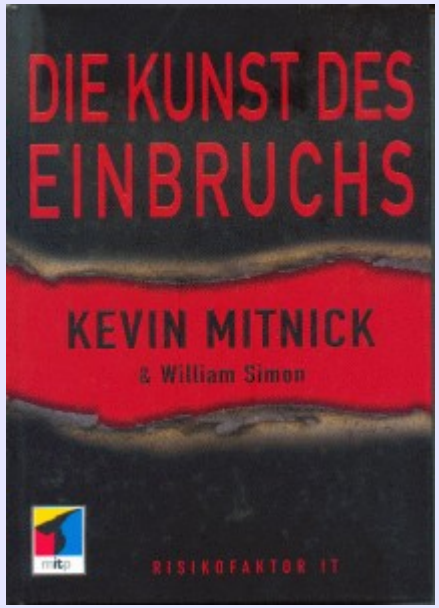
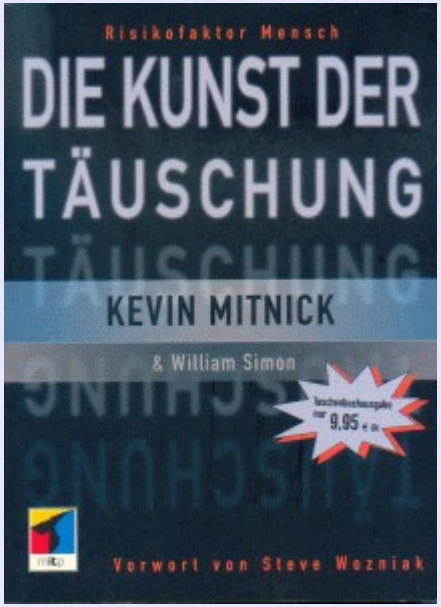
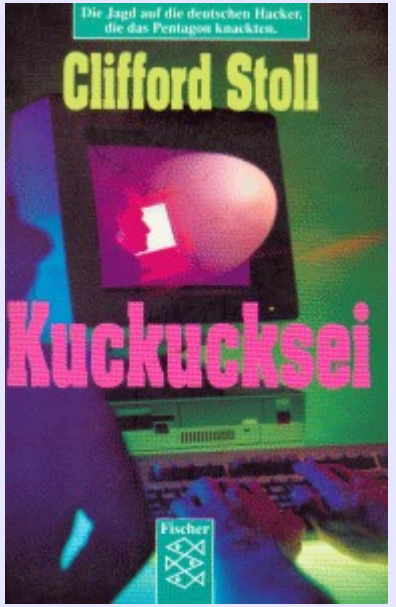
Dieter Kochheim

Cybercrime und Cyberwar

1941... 43	D, GB, USA		Z3, ENIAC, Colossus
1957	USA	!	Phreaking ›
1963	USA	!	Telefonanlagen-Hacking
~ 1966			„akademisches“ Hacking
1969	USA		ARPANET
1976			Dokumentation des Hacker-Jargons
1978	USA		1. Spam
1981	D		Chaos Computer Club
1982		!	Virus für Apple
1984	D		CCC: Onlinebanking-Manipulation (Demo)
	USA		Hackermagazin „2600-Magazine“
	USA		Cult of the Dead Cow
1985	D	!	KGB-Hack ›
		!	Gotcha: Trojaner löscht Festplatte
1986		!	Bootvirus für DOS
1987		!	Lehigh: speicherresidenter Virus







***Mitnick: Kunst des Einbruchs* (2005)**

Telefondienste, Spielautomaten, modernes Hacking

***ders.: Kunst der Täuschung* (2003)**

soziale Techniken, Social Engineering

***Stoll: Kuckucksei* (1989)**

Zwischen 1985 und 1989 drang die hannoversche Hackergruppe um Karl Koch und Markus Hess im Auftrag des KGB auf der Suche nach nützlichen Informationen weltweit in verschiedene Computersysteme des Militärs, von Hochschulen und Unternehmen ein.

1989	Rus	Virenepidemie
1990		polymorpher Virus
	Bulgarien !	Hacker-Fabriken
1995	D	SoftRAM
	USA	2600-Magazine, bösartige Codes: WM/Cap, W32/Donut, W2K/Stream, W64/Rugrat, SymbOS/Cabir
	China	Webseite: Voice of the Dragon
1996	USA	Cult of the Dead Cow
... 2002	USA !	Gambino-Familie: Pornographie im Internet ›
	D !	Phishing
1997	China	Goodwell gründet die Green Army (3.000 Mitgl.)
	D !	Dialer
1998	Rus !	Virus-Fabriken ›
	D !	Grabbing
		Napster. Filesharing

White Paper

McAfee

Cybercrime and Hacktivism

By François Paget

McAfee Labs™

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:

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“.

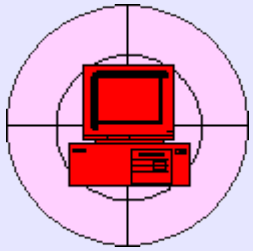
1998	D	CCC: Klonen eines verschlüsselten Mannesmann-Handys (Demo)
1999	Rus	HangUp-Team (Galaiko, Petrichenko, Popow)
	D	Compuserve-Urteil
2000	!	Skimming mit Kartenlesegeräten
	China	Peng Yinan gründet „Javaphile“
	China	Lion (Lin-Yong) gründet Honker Union of China
2001	China	DoS-Angriff von Javaphile gegen die Webseite des Weißen Hauses
	China	Honker greift westliche Webseiten an
… 2008	China	Honker greift im Mai 2008 die regimekritische Webseite Tsering Woeser aus Tibet an
2001	Rus !	Gründung von CardersPlanet ›

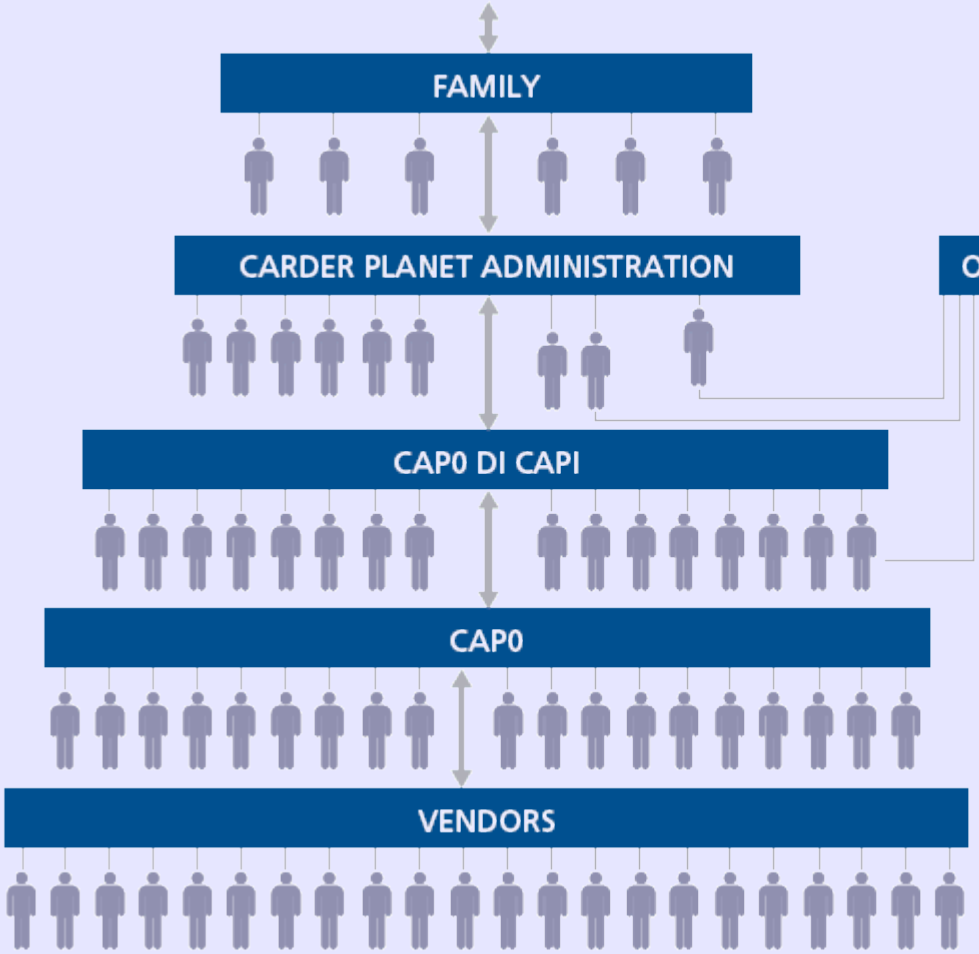
Paget:

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

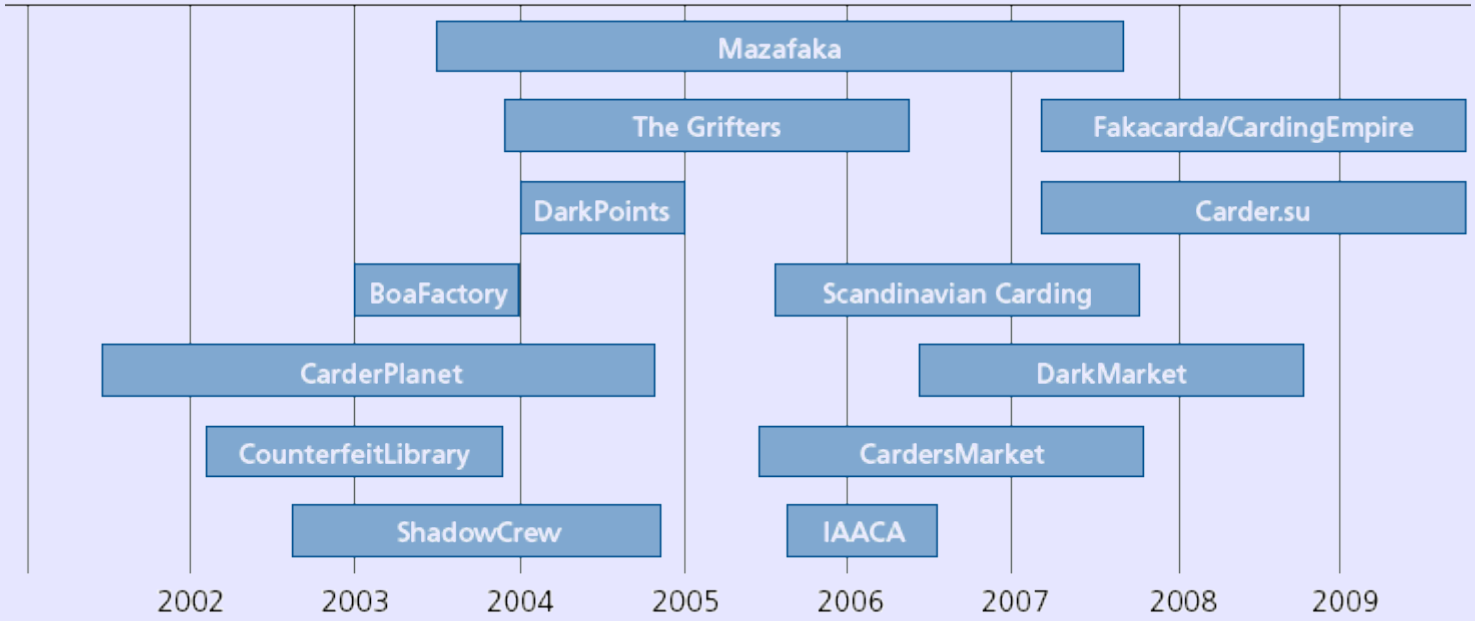
- Bezahlen mit ausgespähten Kreditkartendaten
- Phishing (Onlinebanking)
- Skimming (Cashing)
- Identitätsdiebstahl im Allgemeinen

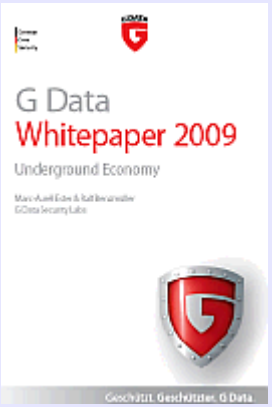




Paget:

CarderPlanet ist als Organisation nach dem Vorbild der russischen Mafia hierarchisch aufgestellt. Ihre Basis bilden die Mitglieder des Forums. Darüber folgen zwei Schichten mit „Köpfen“ und „Köpfen der Köpfe“. Das Führungsmanagement besteht aus den Administratoren, die im Wesentlichen auch die „Reviewer“ stellen. Sie achten auf die kriminellen Geschäfte der Mitglieder und darauf, dass die Carder-Organisation ihren „gerechten“ Anteil bekommt. An der Spitze der Pyramide steht die Gründungsfamilie und vor allem ihr Gottvater Dmitry Golubov.





2006: Moritz Jäger, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel

2009: Marc-Aurél Ester, Ralf Benzmüller, G Data Whitepaper 2009. Underground Economy, G Data

2010: dies., Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data
Dieter Kochheim, Cybercrime, Cyberfahnder
ders., Netzkommunikation, Cyberfahnder

2002	USA	Gambino, Lucchese, topbetters.com Offshore-Sportwetten, Casino ›
2003	USA !	Webshop ProdexTeam: Entwicklung und Verkauf von Trojanern; Haxdoor, Nuclear Grabber ›
	Rus	HangUp-Team: Berbew (Trojaner), Scob (JavaScript-Wurm)
	Rus	Shkola Hackerov ("Hacker-Schulen")
2004	Rus !	HangUp-Team: Korgo (einer der ersten Homebanking-Trojaner)
	D	CCC: Schwachstellen im OBSOC System, DTAG
	D	Sasser
	Marokko	Team Evil: Angriffe gegen israelische und amerikanischen Websites, pro-palästinensische Nachrichten
	Rus	Rock Phish: Phishing
… 2006		150 Mio. US-$ Beute; 1/2 aller Angriffe weltweit

Paget:

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

Paget:

Haxdoor war weltweit die erste Malware, die Rootkits einsetzte und in der Lage war, Bankdaten abzufangen. Die schwedischen Bank Nordea verlor 2006 1,1 Millionen US-$ wegen eine der Haxdoor-Varianten.

2004	Rus !	AllofMP3-Website; London Times online: 5,5 Mio. Kunden, Umsatz: 30 Mio. US-$
2005	Kanada, Belize	betsc.com: Sportwetten ›
	USA !	TJX-Hack ›
	weltweit	Finanzagenten
2006	D	CCC: Manipulation des Nedap-Wahl-Computers
	Rus !	Russian Business Network - RBN ››
	Rus !	RBN + HangUp-Team: Gozi-Botnet (mit SSL)
		Mazafaka (9.000), ShadowCrew (4.000), DarkMarket (2.000): Dumps, gefälschte Pässe, Reiseschecks und Schul-Diplome
	Israel	Team Good vs. Team Evil
		McAfee: Organisierte Cybercrime ›››

Paget:

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.

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.

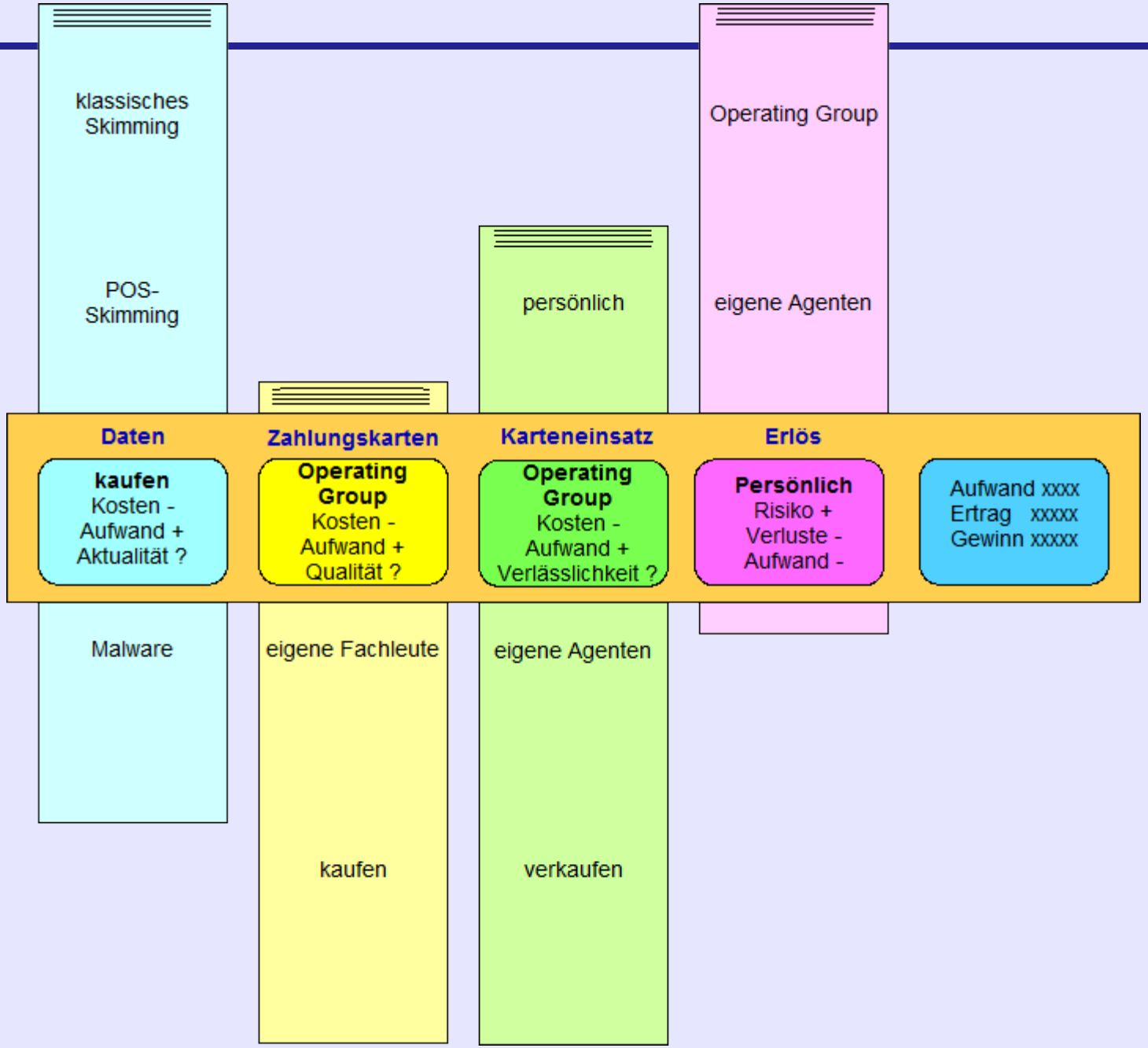
Kochheim:

Das, was ich Zwischenhändler nenne, 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.

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.



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**

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.

Typen:

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

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.

2007		Pharming (Website Injection)
	Rus	RBN verschwindet von der Bildfläche
	Estland	Hactivism-Angriff
		Malware-Baukästen
2008	China	Olympia: Revenge of the Flame vs. CNN.com
	Türkei	Fußball-EM: Nationalisten / Defacement
	Litauen, Georgien	DDoS
	Rus	RockPhish: Online-Phishing
	USA	Atrivo (Spam) und Colo (alles) abgetrennt
	NATO	Cyberdefense-Zentrum in Tallinn / Estland
	USA !	Angriff gegen 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

2009		Twitter-Wurm: JS/Twettir
	Rus	Solntsevskaya, Dolgopruadnanskaya: 25 % aller wissenschaftlichen-technischen Hochschul-Absolventen finden Arbeit bei der Mafia
	Schweden	PirateBay: größte kostenlose Filesharing-Plattform
	Rus	Geldautomaten mit Trojaner infiziert
2010	!	Stuxnet

Kochheim:

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.