FOCUS 10
SECURITY CONFERENCE

Cyber Insecurity:
Unlawful Profits, Activism and Extremist Campaigns on the Internet

David Marcus
Director, Security Research and Communications
McAfee

François Paget
Senior Threat Researcher
McAfee

McAfee®

Cyber Insecurity

- Cybercrime
- Hactivism
- Cyber-War
- Cyber Terrorism
- Conclusion

Definitions

Organized Crime: The UN Convention of November 15th, 2000, called the "Palermo Convention" defines an "organized criminal group" as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit."

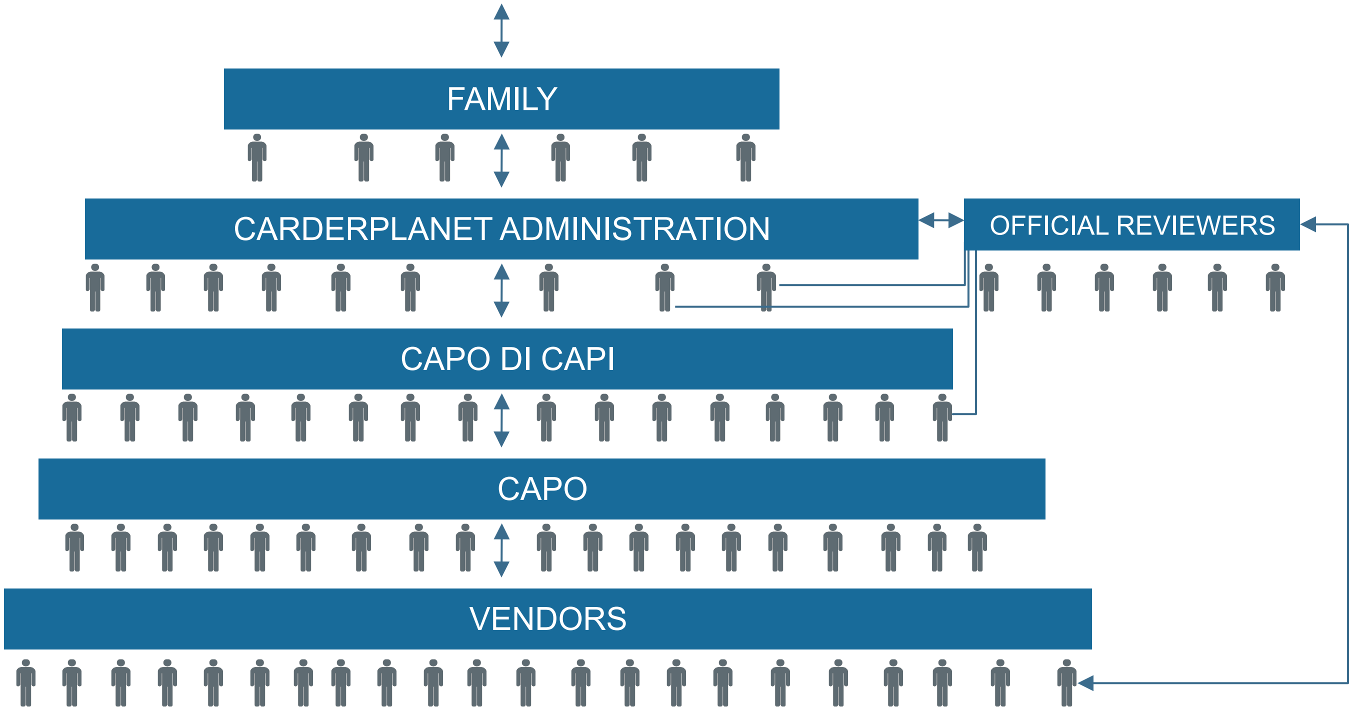
Definitions

Cybercrime: One cybercrime definition that is commonly accepted in Europe was provided by the European Commission *"Toward a general policy on the fight against cybercrime."* It refers to *"criminal offences committed by means of electronic communication networks and information systems or against such networks and systems."*

Cybermafia: Although the term "mafia" is often misused, the term "cybermafia" in every day language has become a simple synonym for an "organized cybercrime group."

Example: CarderPlanet—Odessa 2001-2005

- In May, 2001, 150 criminals from Eastern Europe held a meeting in an Odessa restaurant
- They realized that the internet had created new opportunities for money laundering and making a profit for their business
- They prepared to hatch an international criminal group: CarderPlanet



Organisation of CarderPlanet, based on the mafia model (Source NICSA - FBI - SSA Michael J. McKeown)

Example: Le Club—Pennsylvania 2002-2008

- On February, 18th 2009, Nicholas “Nicky the Hat” Cimino, the head of a loan sharking and illegal gambling organization, pled guilty

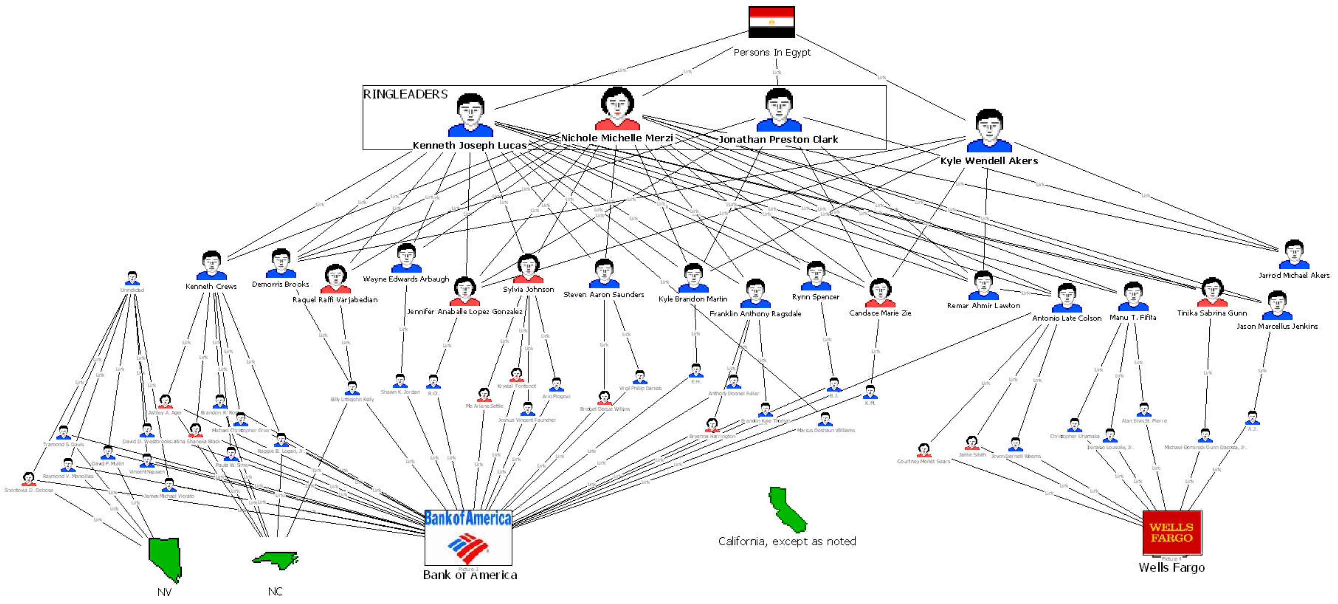
- With the support of the Philadelphia crime family, their criminal activities generated a turnover of around $1 million per month

- The illegal betting and gambling network extended as far as California and even to an offshore website whose domain name has not been disclosed

Source: http://www.attorneygeneral.gov/press.aspx?id=3796

Example: Egyptian Phishing Gang
Operation Phish Phry 2007-2009

- In a widespread crackdown on an intricate phishing scam, FBI agents charged more than 50 people in Nevada, North Carolina and California with running a phishing operation that had ties to suspected cybercriminals in Egypt. The FBI said a raid by Egyptian authorities charged another 47 hackers who allegedly sent out phishing email messages directing victims to malicious web pages designed to look like legitimate banking websites



Flow chart created with i2 Analyst's Notebook by Gary Warner

Source: http://garwarner.blogspot.com/2009/10/fbis-biggest-domestic-phishing-bust.html

Example: Romanian Gangs

Operation Valley of the Kings 2010

- On Tuesday, April 6, 2010, the Romanian Police announced the arrest of 70 members of three separate organized cyber crime groups. Since 2006 these groups have stolen funds from citizens of Spain, Italy, France, New Zealand, Denmark, Sweden, Germany, Austria, the United States, Canada, and Switzerland - primarily through online auction fraud. International authorities have identified more than 800 victims with more than 800,000 Euros worth of losses

- The criminals were using the Internet to sell fictional electronic, luxury cars, yachts, villas and even airplanes. Recent sales included a BMW X5, Lexus and Infiniti vehicles, and even a recreational aircraft that sold for 67,000 Euros to a rich American

Cyber Insecurity

- Cybercrime
- Hactivism
- Cyber-War
- Cyber Terrorism
- Conclusion

Definitions

Activism:

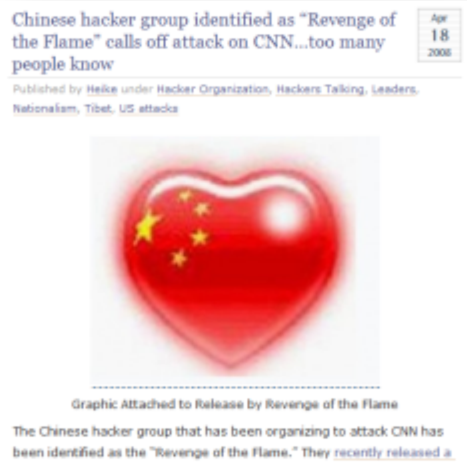
- Political involvement emphasizing direct action
- Actions taken by Greenpeace activists who set out to sea to get in the way of whaling expeditions or by the youths who tried to put out the Olympic flame during its world tour in 2008 are modern examples of activism

Hacktivism:

- A contraction of “hacker” and “activism,” a term created in 1996 by a group named the Cult of the Dead Cow
- Although the phenomenon has existed for more than fifteen years, the 2007 distributed denial of services (DDoS) attacks against Estonia brought worldwide attention to the subject

Example: The Chinese Teams

Defacements: The western media has highlighted the fact that some Chinese groups have more than 300,000 members



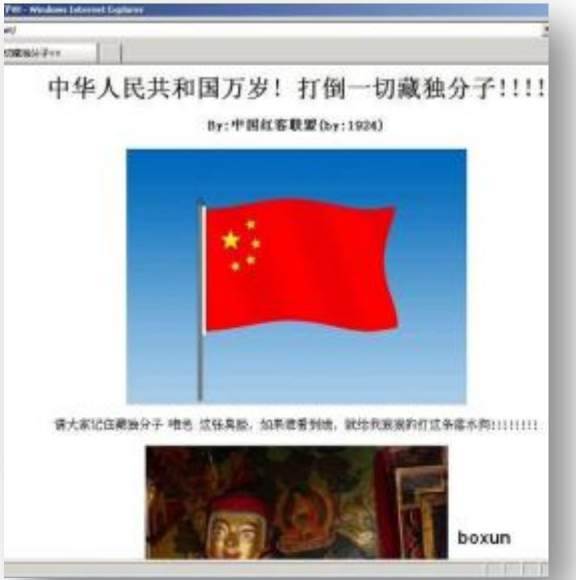
Chinese hacker group identified as "Revenge of the Flame" calls off attack on CNN...too many people know

Apr 18 2008

Published by Heike under Hacker Organization, Hackers Talking, Leaders, Nationalism, Tibet, US attacks

Graphic Attached to Release by Revenge of the Flame

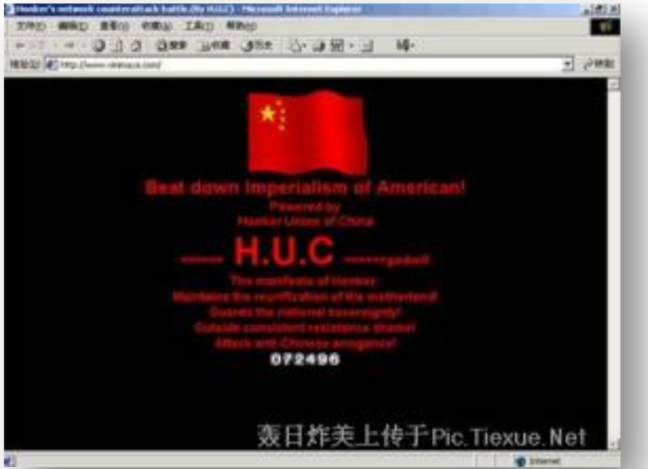
The Chinese hacker group that has been organizing to attack CNN has been identified as the "Revenge of the Flame." They recently released a



中华人民共和国万岁！打倒一切藏独分子！！！！

By:中国红客联盟(by:1924)

请大家记住藏独分子 唯色 这张鸟脸，如果谁看到她，就给我狠狠的打这条落水狗!!!!!!!!



Hacker's network counterattack battle.(By H.U.C) - Microsoft Internet Explorer

Beat down imperialism of American!

Powered by

Hacker Union of China

—— H.U.C ——godwill

The manifesto of Hacker:

Maintains the reunification of the motherland!

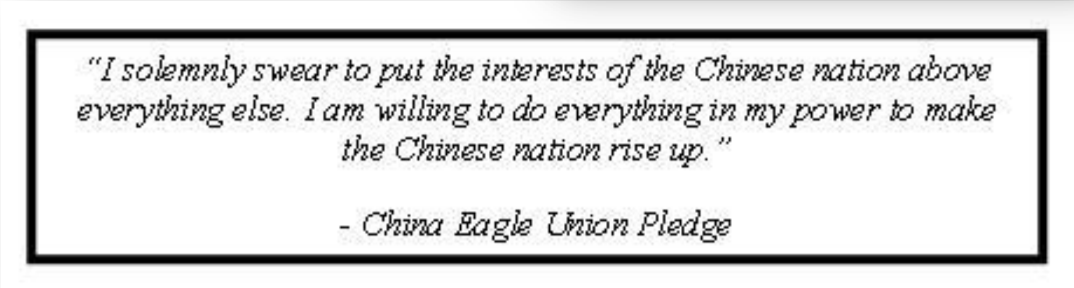
Guards the national sovereignty!

Outside consistent resistance shame!

Attack anti-Chinese arrogance!

072496

轰日炸美上传于Pic.Tiexue.Net

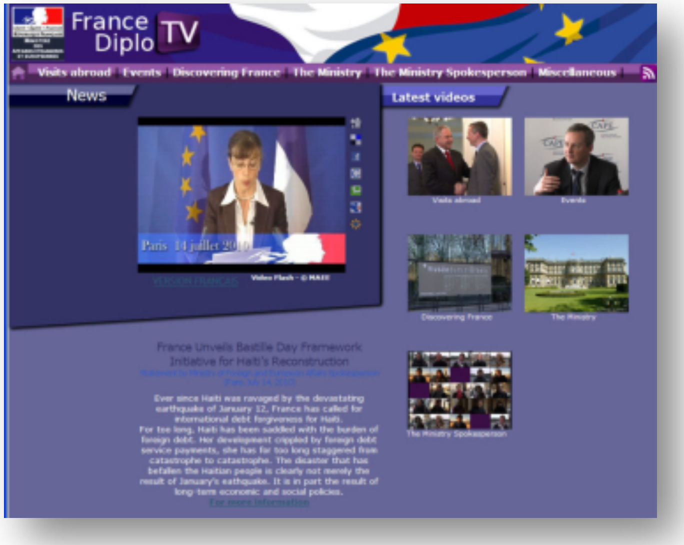


> *"I solemnly swear to put the interests of the Chinese nation above everything else. I am willing to do everything in my power to make the Chinese nation rise up."*
>
> *- China Eagle Union Pledge*

Example: France Disinformation—Typosquatting

- On July 14, 2010 (Bastille Day), a bogus site using the logo and style and many of the video contents of the official French Foreign Ministry web site goes online
- The lead video item on the hoax site is a film of a young, pompous woman announcing a series of diplomatic initiatives that never existed

www[.]diplomatiegov.fr



France Unveils Bastille Day Framework Initiative for Haiti's Reconstruction

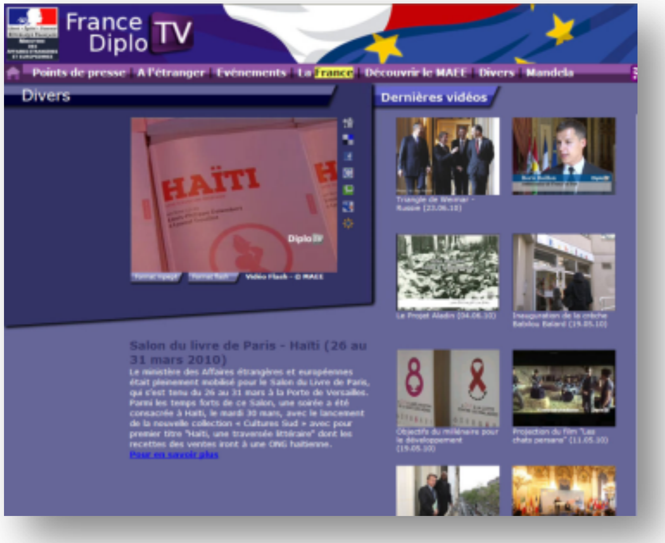
Statement by Ministry of Foreign and European Affairs Spokesperson (Paris, July 14, 2010)

Ever since Haiti was ravaged by the devastating earthquake of January 12, France has called for international debt forgiveness for Haiti.
For too long, Haiti has been saddled with the burden of foreign debt. Her development crippled by foreign debt service payments, she has for too long staggered from catastrophe to catastrophe. The disaster that has befallen the Haitian people is clearly not merely the result of January's eathquake. It is in part the result of long-term economic and social policies.
For more information

Fake

True

www[.]diplomatie.gouv.fr


France Diplo TV
Points de presse
A l'étranger
Evénements
La France
Découvrir le MAEE
Divers
Mandela
Divers
Dernières vidéos
HAÏTI
Diplo TV
Format mpeg4
Format flash
Vidéo Flash - © MAEE
Triangle de Weimar - Russie (23.06.10)
Le Projet Aladin (04.06.10)
Inauguration de la crèche Babilou Balard (19.05.10)
Objectifs du millénaire pour le développement (19.05.10)
Projection du film "Les chats persans" (11.05.10)

Salon du livre de Paris - Haïti (26 au 31 mars 2010)

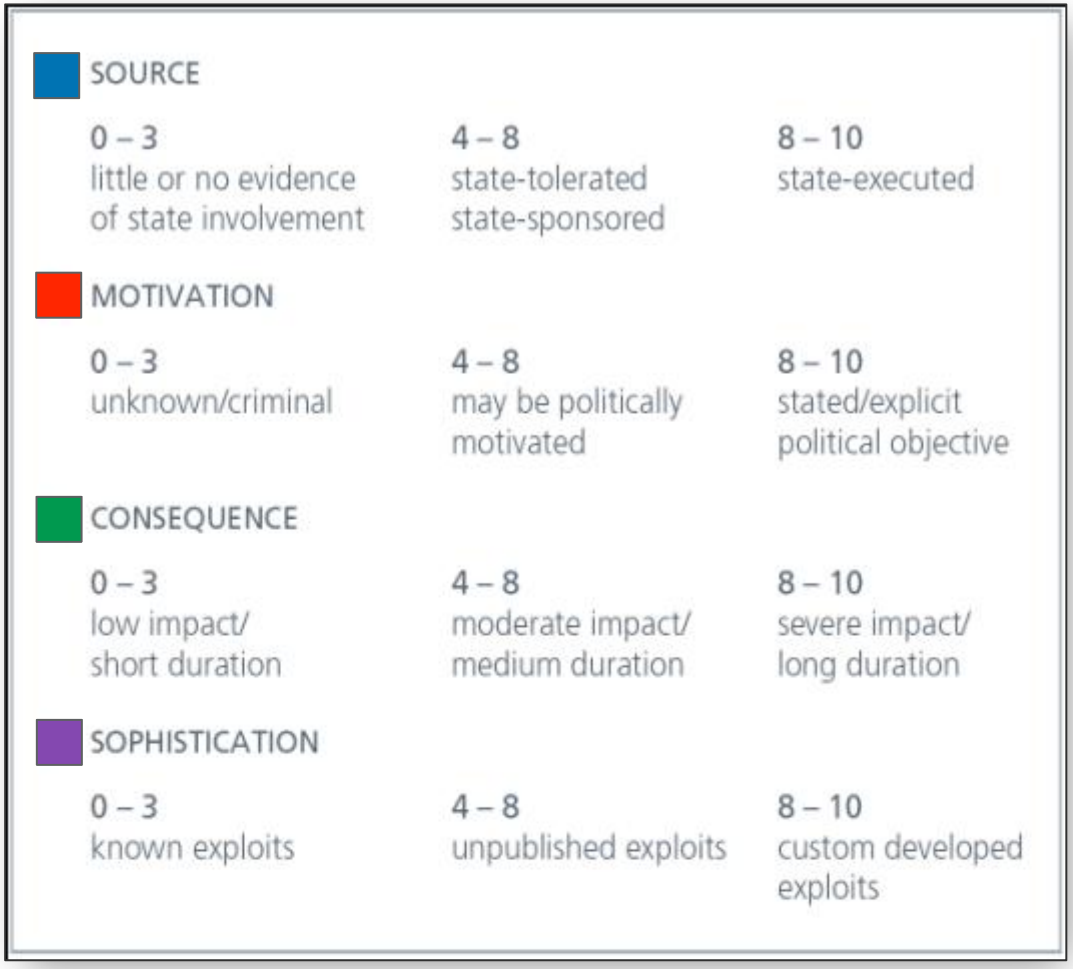
Le ministère des Affaires étrangères et européennes était pleinement mobilisé pour le Salon du Livre de Paris, qui s'est tenu du 26 au 31 mars à la Porte de Versailles. Parmi les temps forts de ce Salon, une soirée a été consacrée à Haïti, le mardi 30 mars, avec le lancement de la nouvelle collection « Cultures Sud » avec pour premier titre "Haïti, une traversée littéraire" dont les recettes des ventes iront à une ONG haïtienne.
Pour en savoir plus

Cyber Insecurity

- Cybercrime
- Hactivism
- Cyber-War
- Cyber Terrorism
- Conclusion

Definition: Attributes of Cyber-War

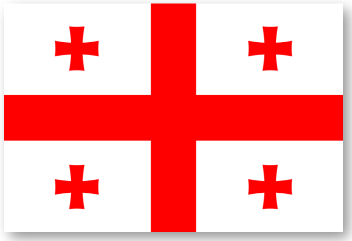
- Source: The attack must be carried out or supported by a State
- Motivation: The attack is motivated by political reasons
- Consequence: The attack causes damage
- Sophistication: The attack requires custom methods and/ or complex planning



🟦 SOURCE		
0 – 3 little or no evidence of state involvement	4 – 8 state-tolerated state-sponsored	8 – 10 state-executed
🟥 MOTIVATION		
0 – 3 unknown/criminal	4 – 8 may be politically motivated	8 – 10 stated/explicit political objective
🟩 CONSEQUENCE		
0 – 3 low impact/ short duration	4 – 8 moderate impact/ medium duration	8 – 10 severe impact/ long duration
🟪 SOPHISTICATION		
0 – 3 known exploits	4 – 8 unpublished exploits	8 – 10 custom developed exploits

Examples: The Estonian & Georgian Rings
A Model for Future Conflicts?

- Attacks were carried out by civilians
- In step with military operations
- Carried out with the help of major Russian cybercrime organizations
- Attacks intentionally limited in their scope
- A desire to hide this new model of conflict's true capacity for harm



- On May 2008, seven allied countries, members of NATO, set up a center of expertise and training on cyber-risks

- On March, 2009 State Duma Deputy Sergei Markov revealed that his assistant – who will remain nameless - launched the Estonian attack. The unnamed assistant is likely to be Konstantin Goloskokov, commissar of the "Nashi" Youth Democratic Anti-Fascist Movement in Moldova and Transnistria, who –the same month - admitted to orchestrating the attack

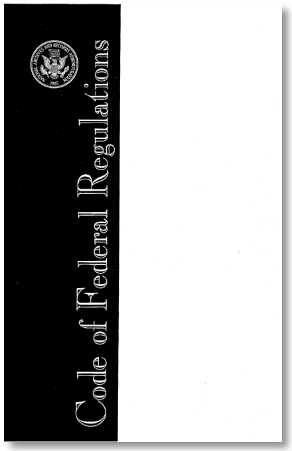
J
is
p
n
p

Cyber Insecurity

- Cybercrime
- Hactivism
- Cyber-War
- Cyber Terrorism
- Conclusion

Definitions

Terrorism: The US Code of Federal Regulations defines terrorism as *"...the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."* (28 C.F.R. Section 0.85)



Code of Federal Regulations

Cyber Terrorism: *"However, mere terrorist use of information technology is not regarded as cyberterrorism. The true threat of "Cyberterrorism" will be realized when all the factors that constitute a terrorist attack, coupled with the use of the Internet, are met.*

"Cyberterrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda."

United States Senate
Committee on the Judiciary

Testimony of

Mr. Keith Lourdeau

FBI Deputy Assistant Director
Cyber Division

Cyber Terrorism: Does It Even Exist ?

McAfee

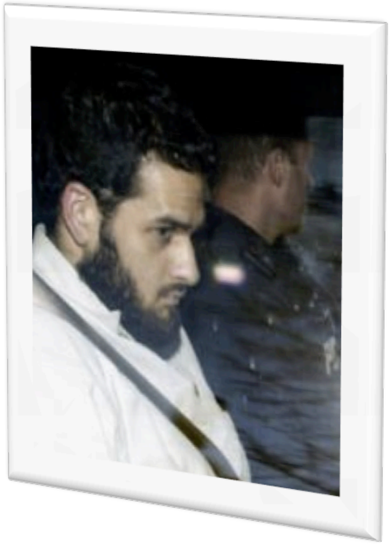
Internet and ITC How They are Used	Happened already ?	Comments
As a means of linking up	☑	• E-mails, forums, cell phones, PDA
As a means of propaganda	☑	• Information and support • Media relay (with increasing use of multimedia) • A weapon to discredit • A weapon to incite hatred • Anti-sites, black propaganda
As a means of financing	☑	• To raise funds • To exploit IT systems (credit cards, blackmail - extortion), money laundering, etc.) • To access confidential personal data
As an information-gathering platform for an operation (and pre-selection of targets)	☑	• On-line information (almanacs, photos, plans of public and/or industrial sites) • Cyber-geography (e.g. national routers, Google earth, network and telecom infrastructures)
As a target for direct action in the real sense (destruction, attribution of resources)	NO	• General discourse focused on mass destruction and/ or a systemic threat (collapse of the Internet, shutdown of a particular business at the national level) • The action might be more limited/targeted. It might be repetitive and/or the prelude to a combined attack …or even attrition spread over time

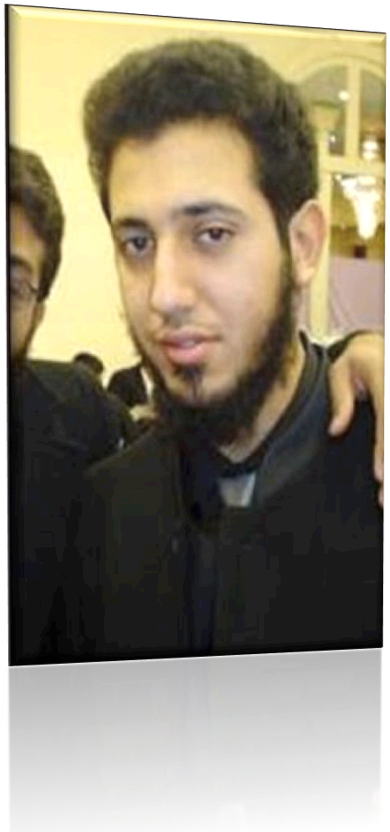
Source CLUSIF (France)

Examples: Cyber Terrorism in Canada

The Khawaja case

Momin Khawaja, a 30-year-old Canadian software engineer was found guilty in a case known as the U.K. fertilizer bomb plot. The events occurred between 2002-2004. Khawaja reportedly experimented with remote-controlled detonation devices. On March 12, 2009, he was sentenced to 10 years and six months in prison





The Toronto 18 case

Zakaria Amara is considered the ringleader of the Toronto 18 extremist Muslim group which planned Al-Qaeda-style bombings of Toronto landmarks in 2006. Amara stated he had learned how to construct a fertilizer bomb over the Internet and planned to use it on the Toronto Stock Exchange. On January 18, 2010 he was sentenced to life in prison. On his computer, police found satellite photos of the Parliament buildings, road maps of the area and instructional videos on making bombs

Examples: Cyber Terrorism in Canada
The Saïd Namouh case

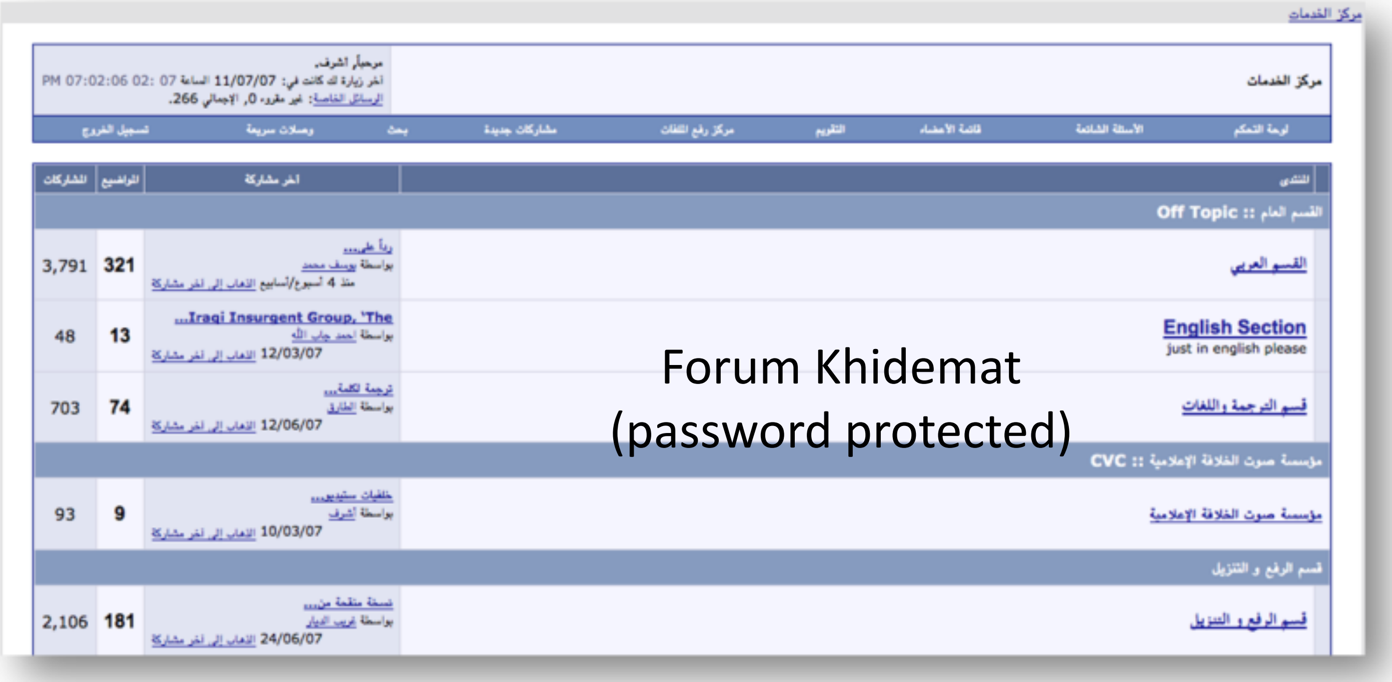
Saïd Namouh was sentenced to life in prison on February 17, 2010

He participated with zeal and enthusiasm in the planning of terrorist acts and the distribution of jihadist propaganda. He was a video maker working for the Global Islamic Media Front (GIMF)

Namouh, described as an al-Qaeda member, was found guilty of conspiring to commit a bombing attack in Europe, attempting to extort the governments of Austria and Germany with video threats (in March 2007), participating in a terrorist group, and aiding terrorist activities. He also helped in the making of a video related to the Alan Johnston ransom demand (May 2007)

Examples: Cyber Terrorism in Canada
The Saïd Namouh Case

- Experts demonstrated how he took part in hundreds of pro-jihad discussions on the Internet. Under the name Ashraf, he was one of 73 members of the Khidemat forum, an online workshop for the GIMF. A few days after his arrest, his 640 contributions disappeared



مركز الخدمات

مركز الخدمات

مرحباً أشرف.
آخر زيارة لك كانت في: 11/07/07 الساعة 07 :02 07:02:06 PM
الرسائل الخاصة: غير مقروء 0, الإجمالي 266.

المنتدى	آخر مشاركة	المواضيع	المشاركات
القسم العام :: Off Topic			
القسم العربي	رداً على... بواسطة يوسف محمد منذ 4 أسبوع/أسابيع الذهاب إلى آخر مشاركة	321	3,791
English Section just in english please	Iraqi Insurgent Group, 'The... بواسطة أحمد جاب الله 12/03/07 الذهاب إلى آخر مشاركة	13	48
قسم الترجمة و اللغات	ترجمة لكلمة... بواسطة الطارق 12/06/07 الذهاب إلى آخر مشاركة	74	703
مؤسسة صوت الخلافة الإعلامية :: CVC			
مؤسسة صوت الخلافة الإعلامية	خلفيات ستيديو... بواسطة أشرف 10/03/07 الذهاب إلى آخر مشاركة	9	93
قسم الرفع و التنزيل			
قسم الرفع و التنزيل	نسخة منقحة من... بواسطة غريب الديار 24/06/07 الذهاب إلى آخر مشاركة	181	2,106

Forum Khidemat
(password protected)

Examples: Cyber Terrorism in Canada
The Saïd Namouh case

- Inside his computer, the investigative work was difficult because many of the folders, filenames, and contents were in Arabic characters. However, they easily discovered maps and flag pictures of the United States that the defendant used in some of the videos he helped create

Sources (screenshots and video):
D. Dudemaine - Public
Prosecution Service of Canada

Examples: Cyber-Terrorism in Canada
Al-Qaeda is Engaged in Online Military Training

الجبهة الإعلامية الإسلامية العالمية
Global Islamic Media Front

الجبهة الإعلامية الإسلامية العالمية
Global Islamic Media Front

Examples: Cyber Terrorism in Canada
Al-Qaeda is Engaged in Online Military Training

Islamic groups also distribute the necessary tools to see the jihad through to the end. They develop and distribute their own VPN and encryption software. The jihadist movements are reluctant to use standard encryption software such as PGP because they fear a backdoor within the implementation

Global Islamic Media Front
Software

Technical Security Squadron

Presents

GIMF Software
MOJAHEDEEN SECRETS
SECURE COMMUNICATION

Secure Communication
Over Networks

(NOW IT IS SAFE TO COMMUNICATE!)

الجبهة الاعلامية الاسلامية العالمية

تقدم

برنامج أسرار المجاهدين

أسرار المجاهدين
أسرار المجاهدين
MUJAHEDEEN SECRETS
Version 1.0

أول برنامج اسلامي للتراسل الآمن عبر الشبكة

خصائص البرنامج
أفضل خمس خوارزميات في علم التشفير
مفاتيح تشفير متماثل بطول 256 بت
مفاتيح تشفير لاتماثل بطول 2048 بت
ضغط بيانات مدمج
[illegible]

لا تنسونا من صالح دعائكم

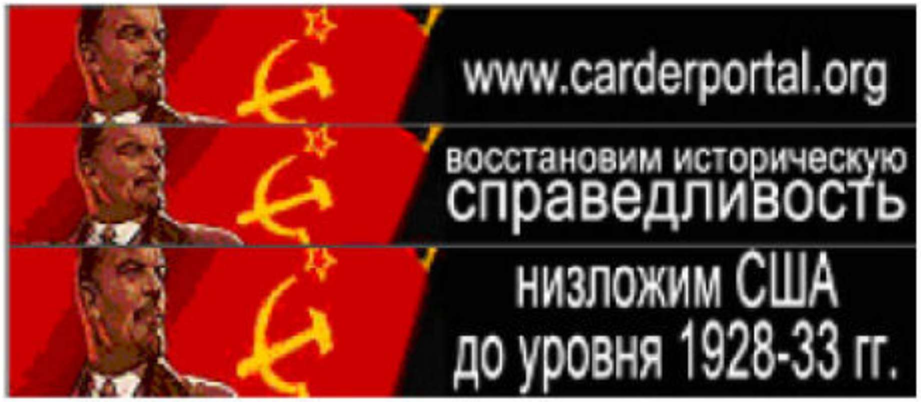
Cyber Insecurity

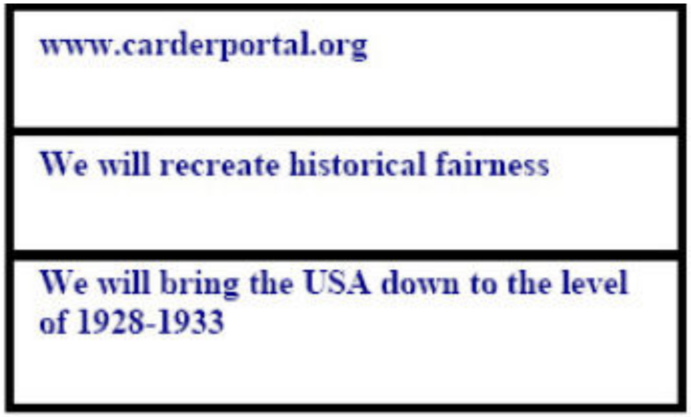
McAfee

- Cybercrime
- Hactivism
- Cyber-War
- Cyber Terrorism
- Conclusion

Cyber Insecurity—Interconnections Exist Between Cybercrime & Cyber-War

The nationalist leanings of some cybercriminals can be seen on their forum banners.


www.carderportal.org
восстановим историческую справедливость
низложим США до уровня 1928-33 гг.



www.carderportal.org

We will recreate historical fairness

We will bring the USA down to the level of 1928-1933

Links Exists Between Cybercrime and Cyber-War

– The Torpig authors are known but not arrested. According to French police, *"The political authorities in Kiev and the Kremlin prefer to keep their mafia close at hand, even using them to stick their noses into some Georgia banks, not necessarily friends...".*

Cyber Insecurity: Private Sector from Democratic States are the Next Main Target

SCADA (Supervisory Control And Data Acquisition) on the Front Line

- January 2008: generation of power outages (source CIA)
- May 2008 - Wonderware Suitelink vulnerability: A third of the planet's factories can be controlled by cybercriminals
- July 2010 – The Stuxnet worm targets systems running WinCC SCADA software. It is signed with a real signature of Realtek Semiconductor, one of the biggest producers of computer equipment.

Cyber Insecurity: Mind the Disinformation

- Since end of June 2010, media are talking about a possible new online magazine distributed by Al-Qaeda to English speaking sympathizers. Only the first three pages are readable

- After we analyze the PDF, we are reserved regarding the origin of this document. We doubt it was an Al-Qaeda creation. Nowadays cybercrime and hacktivism are invading the Internet, but don't forget disinformation

INSPIRE

…And Inspire the Believers

May Our Souls be Sacrificed for You!
Shaykh Anwar al-'Awlaki

» Exclusive Interview with Shaykh Abu Basir

» Make A Bomb in the Kitchen of Your Mom
The AQ Chef

» Asrar al-Mujahideen 101
Terrorist

» The West should ban the Niqab Covering its Real Face
Yahya Ibrahim

INSPIRE

26 May our souls be sacrificed for you!

Letter from the editor

INSPIRE

…And Inspire the Believers

Topics Cont.

Other

McAfee®