ConfidEncE 2.0
November 29th-30th 2010
Prague,Czech Republic

Public Release

Cybercrime, CyberWar, Information Warfare: What's this all about, from a hacker's perspective?

New rules for a new world…

Presented by:
Raoul Chiesa, @ Mediaservice.net

Design & Concept:
Jart Armin & Raoul Chiesa

CONfidence 2.0
Prague, November 30th, 2010

Agenda

- **Disclaimer**
- **The Authors**
- **Reasons for this talk**
- **Introduction**
  - Cybercrime
  - CyberWar & Information Warfare
  - Shared points
- **What you see is NOT what you get?**
  - Countries at stake
  - Legends (North Korea)
- **New concepts for a new era**
  - Hackers & Cybercrime
  - Evolution and Size of Cyberattacks
  - From Cybercrime to CyberWar
  - The Paradigm Shift
  - An example: Stuxnet
  - Digital Weapons comparison
  - CyberWar Defense
  - Opportunity for Hackers
  - Learning from the history
- **References**
- **Q&A**

*Disclaimer

*Disclaimer

- The information contained within this presentation **does not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- The statistical data presented **belongs to** the Hackers Profiling Project by **UNICRI** and **ISECOM**.
- Quoted trademarks belongs to **registered owners**.
- The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of **UNICRI** or others **United Nations** agencies and institutes, nor the view of **ENISA** and its **PSG** (Permanent Stakeholders Group).
- Contents of this presentation **may be quoted or reproduced**, provided that the **source of information is acknowledged**.

The Authors - Raoul nobody"Chiesa

- On the underground scene since 1986
- Senior Advisor on cybercrime at the United Nations (UNICRI)
- ENISA PSG Member (2010-2012)
- Founder, @ Mediaservice.net – Independent Security Advisory Company and @ PSS – a Digital Forensics Company
- Founder, Board of Directors at: CLUSIT (Italian Information Security Association), ISECOM, OWASP Italian Chapter
- TSTF.net member
- Member: ICANN, OPSI/AIP, EAST
- CONfidence speaker non-stop since 2007 (Krakow & Warsav, now Prague :)

The Authors - Jart Armin

* Independent Security & Malware researcher
* Senior Partner at CyberDefcon
* Specialized in Cyber threats analysis and Cybercrime intelligence for Internet industry and government agencies
* Well-known 'cause of his exposure and analysis on RBN (Russian Business Network) – hostexploit.com, RBNexploit.com
* Introduced as "one of the world's top hacker hunters" by RU.TV
* Heavily mentioned in Thomas Menn's book, "Fatal System Error" (2010) along with Steve Santorelli (Team Cymru) and other nice folks!

* Reasons for this talk

* Speaking along with a lot friends, it looks like the ".mil" world developed a deep interest towards these topics…

- ✓ 2001/2002: First interest shown back from USA (after 9/11), focused on hacker's resources in order to attack and/or infiltrate Al Qaeda;
- ✓ 2003-2005: observed a huge escalation of USA and Israel Secret Services, asking for 0-days, seeking for information resources among elite hackers, asking for Iran & Pakistan hacking;
- ✓ 2005: China's attacks to USA go public, escalating during 2007-2010 (UK, Germany, France, Italy);
- ✓ 2008/2010: USA & Canada leading (since the last 2/3 years), an increasing attention related to National Critical Infrastructures, followed by UK, EU, Israel, India, Australia;
- ✓ 2010: Italian Committee for the National Security of the Republic audited myself (March/May);
- ✓ 2009/2010: NATO Cyber Coalition running CyberDefense 2010 (CyberShot 2009) along with C4 Command (Rome);
- ✓ 2011: Swiss Cyber Storm III.

- ✓ TODAY - Intelligence Agencies hiring "leet hackers" in order to:
  - ✓ Buy/develop 0-days;
  - ✓ Launch attacks on terrorists and/or suspected ones;
  - ✓ Protect National Security;
  - ✓ Informing & Training Local Governments.

* Thus, hackers becoming kind of "e-ambassadors", "e-strategy consultants" towards .mil and .gov environments, or "e-mercenaries", training "e-soldiers"…

Introduction

* Just like you got used to words such as:
  * "Paranoia" (that's into your DNA, hopefully!)
  * "Information Security" (198x)
  * "Firewall", "DMZ" (1994/5)
  * "Pentesting" (1996/7)
  * "xIDS" (2001-2003)
  * "Web Application Security" (2006-2009)
  * "SCADA&NCIs" (2008-201x)
  * "PCI-DSS" (2009-201x)
  * Botnets (2008-2010)
  * ……..
* In the next (ten?) years, you will hear non-stop about:
  * NGC – Next Generation Cybercrime
  * CyberWar
  * Information Warfare
  * NGW – Next Generation Warfare

Information Operations terminology

- SIGINT = Signals Intelligence
- COMINT = Communication Intelligence
- ELINT = Electronic Intelligence
- FISINT = Foreign Instrumentation Signals Intelligence
- OSINT = Open Source Intelligence
- PSYOPS = Psychological Operations
- IMINT = Imagery Intelligence
- MASINT = Measurement Signal Intelligence
- HUMINT = Human Intelligence
- GEOSPATIAL Intelligence = Analysis and Presentation security-relevant Activities

Information Operations terminology / 2

* IO = Information Operations
* IW = Information Warfare
* IA = Information Assurance
* C2 = Command and Control
* C2IS = Command and Control Information Systems
* C2W = Command and Control Warfare
* C3 = Command, Control, Communication
* C3I = Command, Control, Communication and Intelligence
* C4 = Command, Control, Communication and Computers
* C4I = Command, Control, Communication, Computers and Intelligence
* C4I2 = Command, Control, Communication, Computers, Intelligence and Interoperability
* C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
* C5I = Command, Control, Communication, Computers, Combat Systems and Intelligence

Information Operations terminology / 3

- I = Intelligence
- S&R = Surveillance and Reconnaissance
- RSTA = Reconnaissance, Surveillance and Target Acquisition
- STA = Surveillance and Target Acquisition
- STAR = Surveillance, Target Acquisition and Reconnaissance
- ERSTA = Electro-Optical Reconnaissance, Surveillance and Target Acquisition
- STANO = Surveillance, Target Acquisition and Night Observation
- ISR = Intelligence, Surveillance and Reconnaissance
- ISTAR = Intelligence, Surveillance, Target Acquisition, and Reconnaissance

Information Operations terminology / 4

- OPSEC = Operational Security
- INFOSEC = Information Security
- COMSEC = Communications Security
- PHYSSEC = Physical Security (Human, Physical)
- HUMSEC = Human Security
- SPECSEC = Spectrum Security

  and includes:
  - EMSEC = Emissions Security (cables on the air)
  - ELSEC = Electronic Communications
  - SIGSEC = Signals
- C-SIGINT = Counter-Signals Intelligence
- ECM = Electronic Countermeasures
- EMI = Electromagnetic Interference
- IBW = Intelligence-based Warfare
- IEW = Intelligence and Electronic Warfare

* That's it!

* Questions??

* Thanks for your attention guys!

Kidding ;)

*Welcome to Cybercrime

*Let's laugh before we start ;)

"How'd you know I was in for cyber crime?"

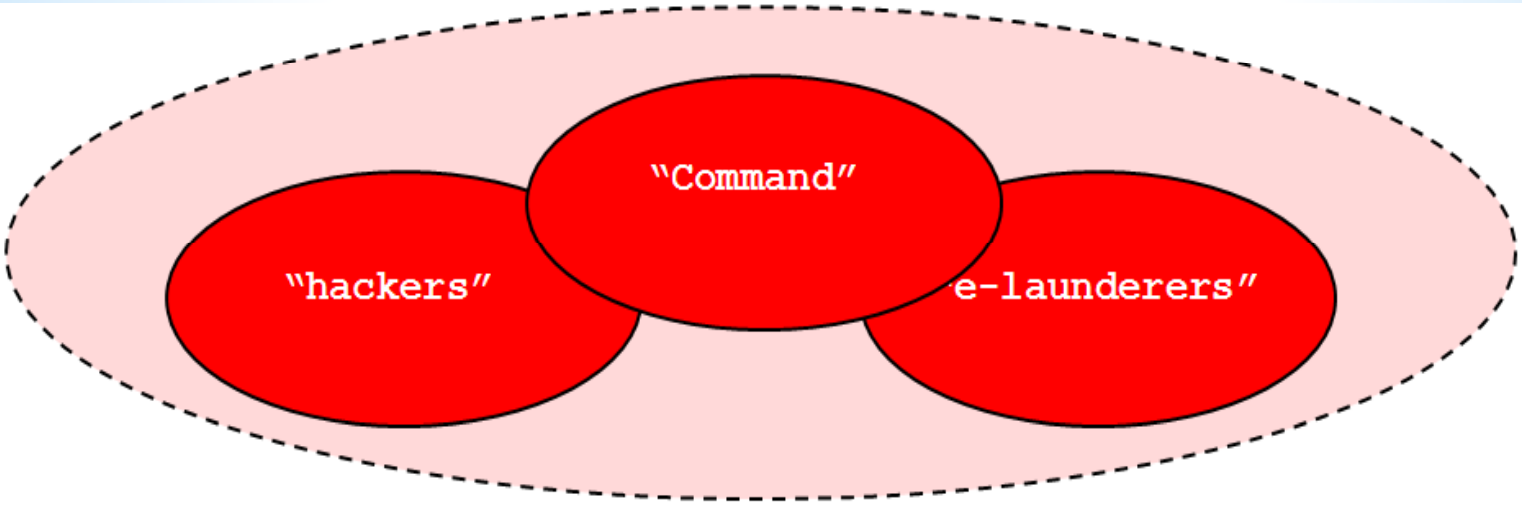
*What is cybercrime?

- Running **criminal actions**, using **IT** and **TLC assets**, having the **goal** to illegally **acquire information** and **transform** them **into money**.

- Examples:

  - ✓ Identity Theft (Personal Info)
  - ✓ Credit Identity Theft (Financial Info: e-banking logins, CC/CVV, etc)
  - ✓ Hacking towards e-commerce, e-banking, Credit Processing Centers
  - ✓ Malware (Virus, Worm, Spyware, Key Loggers, Rogue AV, Botnets, Mobile)
  - ✓ Hacking on-demand
  - ✓ DDoS attacks (blackmail)
  - ✓ Spam
  - ✓ Counterfiting (medicinals, luxury, products & services
  - ✓ Gambling (not authorized by local Authorities)
  - ✓ Generic Porn (fake sites, etc)
  - ✓ Minors and children pornography

*Cybercrime Biz Model



Phase 1

- Performing hacking
- Developing malware
- Building botnets

Phase 2

- Perform ID-theft
- Collect Personal Info
- Collect financial info

Phase 3

- Execute e-crimes
- e-banking
- e-commerce

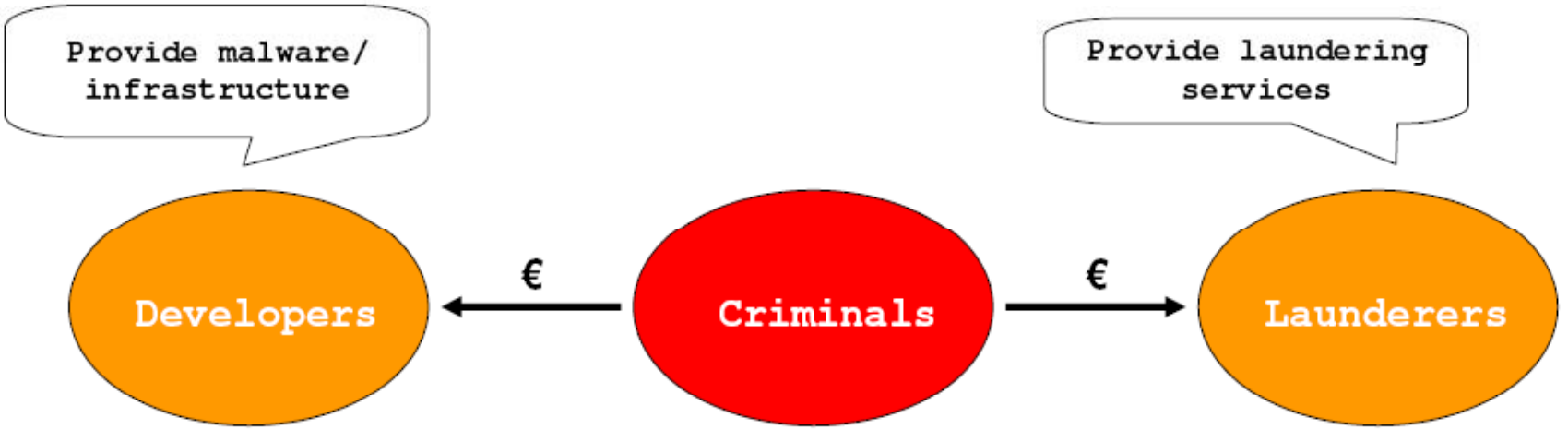
Phase 4

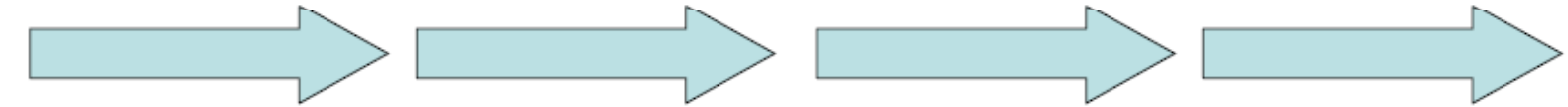
- Get the proceedings
- Setup e-laundering network
- Channel illegal gains

Underground Economy

- trade stolen goods, stolen information, malware, tools, expertise, skills

Cybercrime Business Model II





•Performing hacking	•Perform ID-theft	•Execute e-crimes	•Get the proceedings
•Developing malware	•Collect Personal Info	•e-banking	•Setup e-laundering net
•Building botnets	•Collect financial info	•e-commerce	•Channel illegal gains

Underground Economy

• trade stolen goods, stolen information, malware, tools, expertise, skills

From Wikipedia

* **Computer crime - From Wikipedia, the free encyclopedia**
(Redirected from Cybercrime: **http://en.wikipedia.org/wiki/Cybercrime**)

* **Computer crime** refers to any crime that involves a computer and a network, where the computers may or may not have played an instrumental part in the commission of the crime (Moore 2000). **Netcrime** refers, more precisely, to criminal exploitation of the Internet [1]. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, child porn, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.
* On the global level, both governments and non-state actors continue to grow in importance, with the ability to engage in such activities as **espionage**, financial theft, and other cross-border crimes sometimes referred to as **cyber warfare**. The international legal system is attempting to hold actors accountable for their actions, with the International Criminal Court among the few addressing this threat.[2]

*Zooming in…

* It looks like we're speaking about **different actors**, whose **goals**, **targets,** and **criminal models** are **different** from the cybercrime ones!

*Intelligence

*From wikipedia:

(http://en.wikipedia.org/wiki/Intelligence agency)

- An **intelligence agency** is a governmental agency that is devoted to the information gathering (known in the context as "intelligence") for purposes of national security and defense. Means of information gathering may include espionage, communication interception, cryptanalysis, *cooperation with other institutions*, and **evaluation of public sources**. The assembly and propagation of this information is known as intelligence analysis.
- Intelligence agencies can **provide the following services** for their national governments:
  - provide **analysis** in areas relevant to national security;
  - give **early warning** of impending **crises**;
  - **serve** national and international crisis management by helping to **discern the intentions** of current or potential opponents;
  - **inform** national defense planning and military operations**;**
  - **protect secrets**, both of their own sources and activities, and those of other state agencies;
  - and may act covertly to **influence the outcome of events in favor of** national interests**.**
- Intelligence agencies are also **involved** in defensive activities such as counter-espionage or counter-terrorism.
- Some agencies are accused of being involved in assassination, arms sales, coups d'état, and the placement of misinformation (propaganda) as well as other covert operations, in order to support their own or their governments' interests.

*InfoWar / 1

http://en.wikipedia.org/wiki/Information_warfare

Discussion: Information... | PI: Come ti cracko l'aut... | Schedule « 2010 CONFi... | agenda [0ct0b3rf3st] | Security Summit :: Italia... | Information warfar...

New features | Log in / cr

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article

Interaction
About Wikipedia
Community portal
Recent changes

Article | Discussion | Read | Edit | Search

Information warfare

From Wikipedia, the free encyclopedia

The examples and perspective in this article **deal primarily with the United States and do not represent a worldwide view of the subject**. Please improve this article and discuss the issue on the talk page. *(March 2010)*

This article **is missing citations or needs footnotes**. Please help add inline citations to guard against copyright violations and factual inaccuracies. *(July 2008)*

*InfoWar / 2

*From wikipedia:

(http://en.wikipedia.org/wiki/Information_warfare)

Information warfare is the **use and management of information** in pursuit of a **competitive advantage over an opponent**.

Information warfare may involve **Collection** of tactical information, assurance(s) that one's own information is valid, spreading of **propaganda** or disinformation to demoralize the enemy and the public, undermining the quality of opposing force information and denial of information-collection opportunities to opposing forces.

Information warfare is closely linked to **psychological warfare**.

Contents [hide]

* "Cyber WarFare"...uh?

* **Ironically, if we look for "Cyber WarFare" on Wikipedia, they got it! While, it's listed into the "computer crimes" category: weird!!!**

The U.S. Department of Defense (DoD) notes that cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.

*Information WarFare

*What is Information WarFare?

* Very simply, we are speaking about the so-called Warfare, applied to the *cyberspace*.

* Defending information and communication networks, acting like a deterrent towards "information attacks", while not allowing the enemy to do the same.

* So we are speaking about "Offensive Information Operations", built against an adversary, 'till being able to dominate the information during a war contest.

Information WarFare: why?

* It is an extremely **new** and **dynamic war scenario**, where those metrics and views used before it are now really **obsolete**.

* Typically, these operations are **decentralized** while **anonymous**.

* The “entry fee” cost is **extremely low**, while it supplies a **huge power**.

* ...and after all, there’s always the possibility of **denying what has happened**..

* Information Warfare: the Estonia case

* Basically, what happened in **Estonia**?

* In 2007, after a Russian statue has been moved from its original location in Tallinn, "**hacktivists**" joined their efforts, launching **electronic attacks** (DDoS, web defacements) towards Estonia's critical infrastructures such as **banks**, **Public Administration (PA)** web sites, etc.

* Estonia, being an extremely **young country**, since its creation decided to really invest on IT, supplying **all** of the services to the citiziens via **on-line resources**.

* The result of the attacks has been **devastating** in a country where Internet is used for everything: **long lines** out of the banks and PA offices, panic around the country.
* The same thing happened to **Georgia the next year** (2008)
* Russian government has always **denied** any possible role in both attacks.

*What does it mean being under DDoS attack?

ping: mfa.gov.ge

location	result	min. rrt	avg. rrt	max. rrt
Florida, U.S.A.	Okay	59.4	59.9	60.5
Amsterdam, Netherlands	Okay	149.3	164.6	275.4
Melbourne, Australia	Okay	173.8	174.5	175.0
Singapore, Singapore	Okay	208.5	214.0	238.6
New York, U.S.A.	Packets lost (100%)			
Amsterdam2, Netherlands	Packets lost (100%)			
Austin1, U.S.A.	Packets lost (100%)			
London, United Kingdom	Packets lost (100%)			
Stockholm, Sweden	Packets lost (100%)			
Cologne, Germany	Packets lost (100%)			
Chicago, U.S.A.	Packets lost (100%)			
Austin, U.S.A.	Packets lost (100%)			
Amsterdam3, Netherlands	Packets lost (100%)			
Krakow, Poland	Packets lost (100%)			
Paris, France	Packets lost (100%)			
Copenhagen, Denmark	Packets lost (100%)			
San Francisco, U.S.A.	Packets lost (100%)			
Vancouver, Canada	Packets lost (100%)			
Madrid, Spain	Packets lost (100%)			
Shanghai, China	Packets lost (100%)			
Lille, France	Packets lost (100%)			
Zurich, Switzerland	Packets lost (100%)			
Munchen, Germany	Packets lost (100%)			
Cagliari, Italy	Packets lost (100%)			
Hong Kong, China	Packets lost (100%)			
Johannesburg, South Africa	Packets lost (100%)			
Porto Alegre, Brazil	Packets lost (100%)			
Sydney, Australia	Packets lost (100%)			
Mumbai, India	Packets lost (100%)			
Santa Clara, U.S.A.	Packets lost (100%)			

Shared Points between Cybercrime & CyberWar

- **PC Zombies** (botnets) -> they take advantage of the "standard user", both in a **Corporate** or **home** (broadband) scenario.
- "**0-days**": until today, **all of them** were on MS Windows.
- "0-days": 'till now, no "unknown vulnerability" exploited (yet). We're heavily talking about IE 6.0 (!) bugs and so on…
- (**attacker's perspective**) **nothing changes that much**. There's more chances to hack 100 broadbands users instead of 1000 PCs from a company's network.
- It's still the digital weapon he needs to launch attacks (DDoS, Keyloggers, etc).

*WYSINWUG

*What you see is NOT what you get...

*Countries at stake

- USA (…everywhere, always!)
- UK, Canada, France, Russia, Switzerland

"Low Risk"

- Brazil
- Israel & Palestinian National Authority
- Zimbabwe
- Middle East: "friendly" countries (UAE, Saudi Arabia…)

"Average Risk"

- China
- India
- Pakistan
- North Korea (DPRK)
- South Korea
- Iran
- Tatarstan
- Kyrgyzstan
- Ingushetia (ex URSS)
- Myanmar
- Russia (Estonia, Georgia)

"High Risk"

*...it's outta there. Already. Now.

Summary of nation-state cyberwarfare capabilities

	China	India	Iran	N. Korea	Pakistan	Russia
Official cyber-warfare doctrine	X	X			Probable	X
Cyberwarfare training	X	X	X		X	
Cyberwarfare exercises/simu-lations	X	X				
Collaberation with IT industry and/or technical universities	X	X	X		X	X
IT road map	likely	X				
Information warfare units	X	X		X		
Record of hack-ing other nations	X					X

Adapted from Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States," Institute for Security Technology Studies, Dartmouth College, December 2004.

* Legends

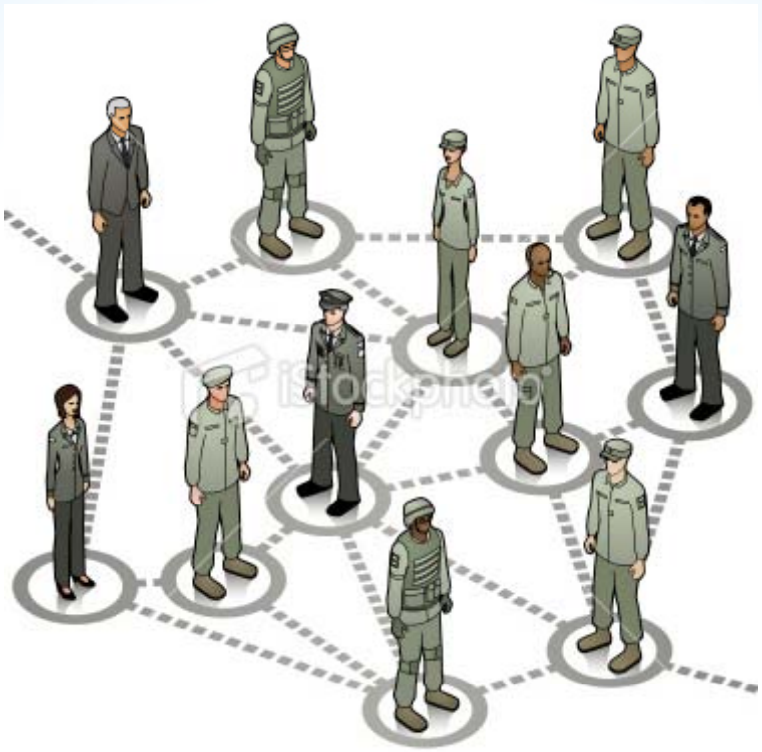
* "North Korea will soon attack many countries using IT attacks, since they have the best hackers of the whole world."

* Uh?!? WTF???

* That's weird, when speaking about a country which is **totally isolated** from the Internet, where its "cellular network" recalls more a DECT infrastructure…(**no BTSs** out of PongYang).

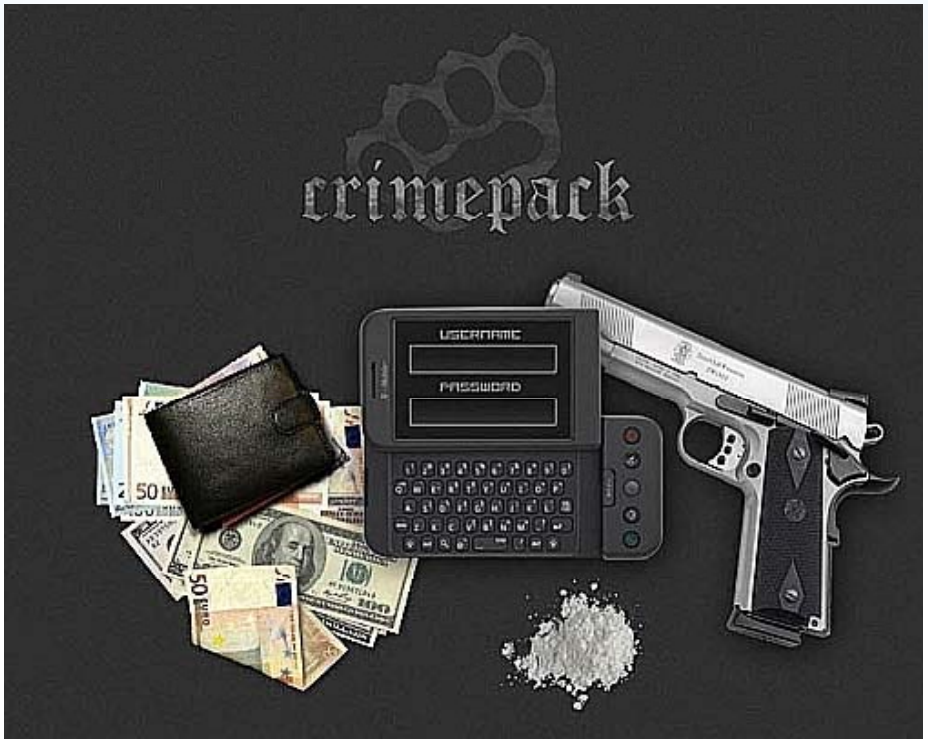
* See Mike Kemp's slides from CONfidence 2010 @ Kracow.

*New concepts, for a new era



"In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers.
This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces. **"**

Duma, 2007



*Hackers & Cybercrime

Hacker's evolution

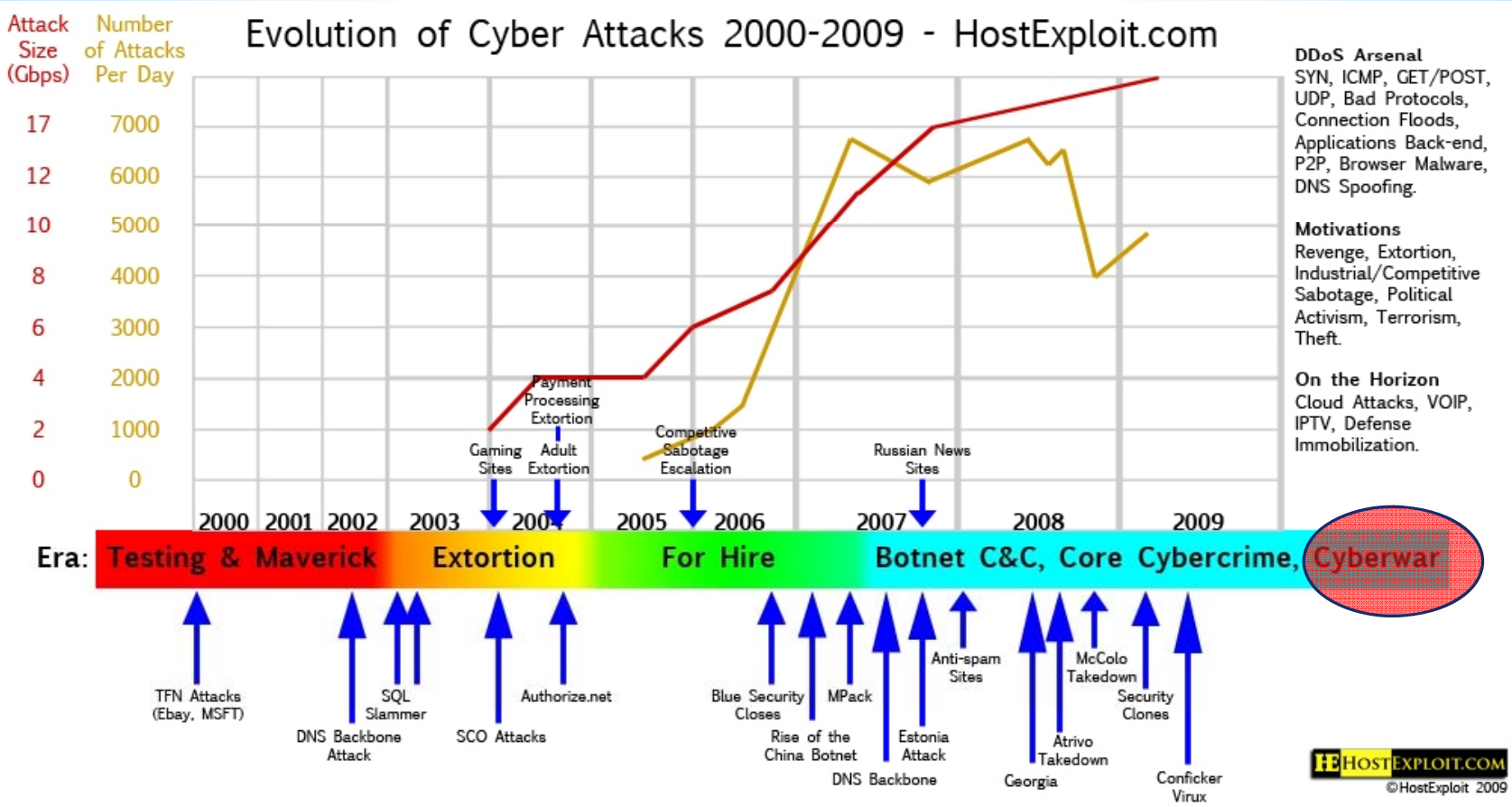
* "Hackers" are today somehow "deprecated", meaning that many CxOs are missing those "romantic" figures.
  * Driven by: Know-how needing (OS, networks, protocols), having fun, being cool, 'cause it was "trendy".

* Nowadays' attackers often belong to the Organized Crime, being both an active or passive actor.
  * Driven by: money.

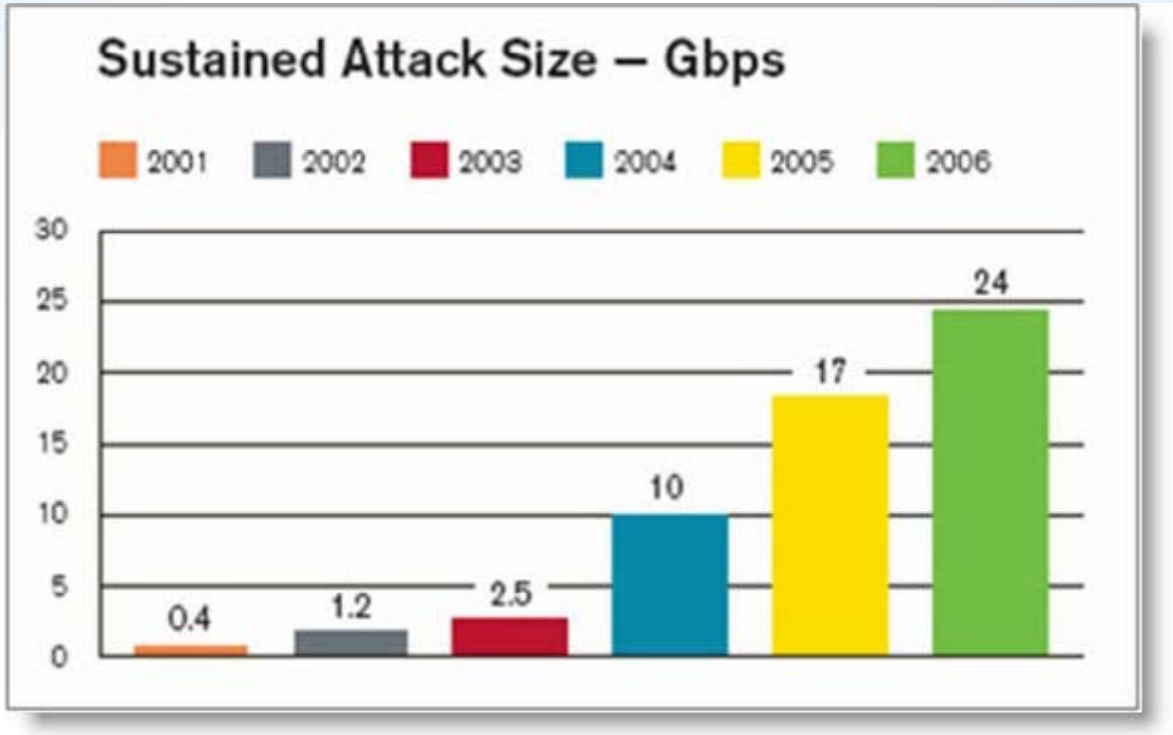
* Results: a weird hack-ecosystem, composed by different actors. i.e.:
  - ✓ Romania's crime gangs in Italy passed the ATM skimmers biz to Nigerian ppl, getting paid back with cocaine (Italy, February 2009);
  - ✓ Nigerian guys cash out the money from cybercrime activities (carding, skimming, etc..) and buy human organs (kidneys) from Nigeria, then sell them in EU (Turin, Italy, September 2010).

	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

*Hackers Profiling



*Evolution of Cyber Attacks



*Size of Cyber Attacks

*Being military "trendy"

OUT ☹	IN ☺
Single operational pic	Situational awareness
Autonomous ops	Self-synchronizing ops
Broadcast information push	Information pull
Individual	Collaboration
Stovepipes	Communities of Interest
Task, process, exploit, disseminate	Task, post, process, use
Multiple data calls, duplication	Only handle information once
Private data	Shared data
Perimeter, one-time security	Persistent, continuous IA
Bandwidth limitations	Bandwidth on demand
Circuit-based transport	IP-based transport
Single points of failure	Diverse routing
Separate infrastructures	Enterprise services
Customized, platform-centric IT	COTS based, net-centric capabilities
	Scouting elite hacker parties?

Cybercrime to Cyberwar Tools of the Trade

* Botnet & drone armies

* DDoS

* Trojans & Worms

* Malware

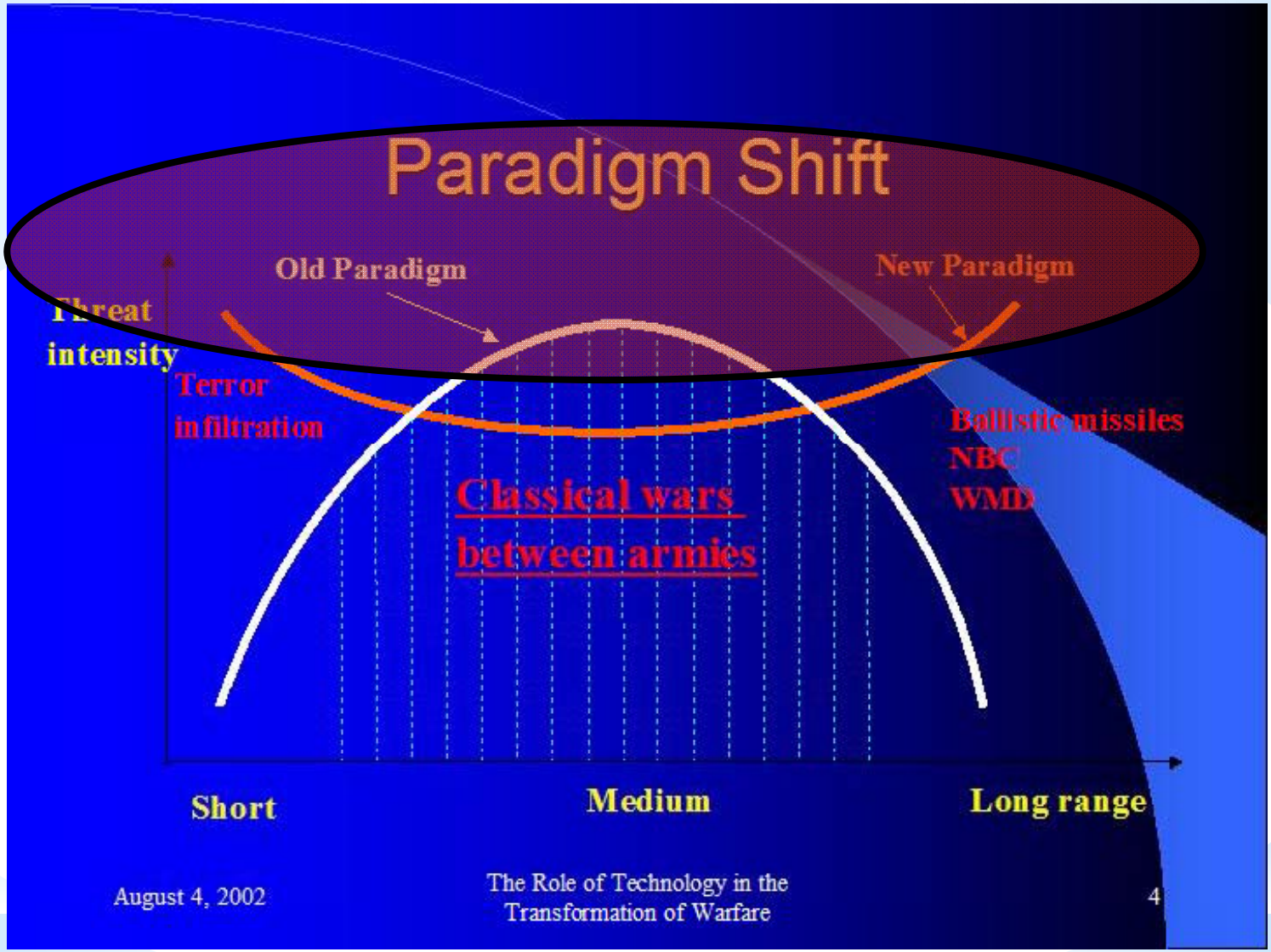
* Server hacking

* Encryption

* Extortion & Ransom

* Man in the Middle

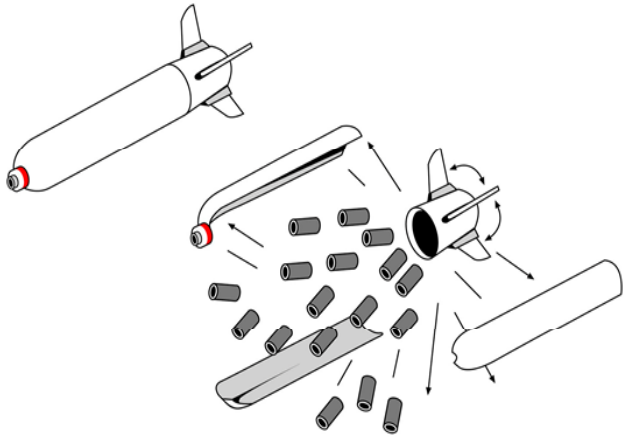
*Why? The Paradigm Shift



* Cyberwar - The Weapons of Choice

Black Energy

* Cluster Bomb



Stuxnet

* Cruise Missile

* Comparison of Weapons

Black Energy

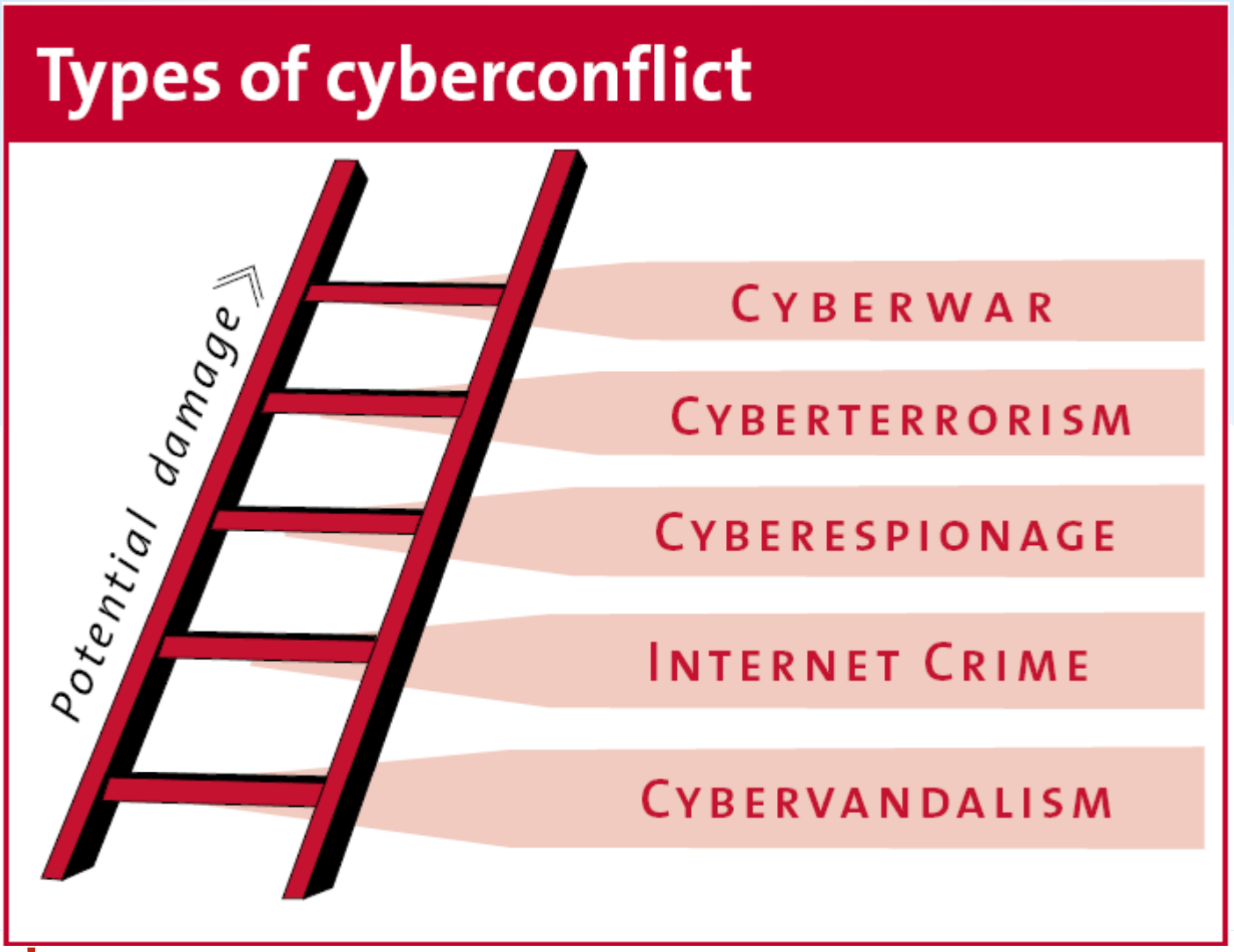
Multiple targets, loud and noisy

* Massive DDoS
* Loss of digital communication
* Cloning of state communications
* Create confusion

Stuxnet

Laser Guided, precision, and stealth

* Compromise infrastructure
* Industrial Sabotage
* Loss of confidence in systems
* Create confusion



*Attacks escalation chart

*An example: Stuxnet (facts)

- Stuxnet is a specialized malware, **solely** targeting:
  - **SCADA systems** running **Siemens SIMATIC WinCC**. Such systems monitor and control industrial technology and infrastructure
  - **SIMATIC Siemens STEP 7** software for process visualization and system control
- Uses **several vulnerabilities** in the underlying MS Windows operating system for infection and propagation
- Infection works via **USB-drives** or **open network shares**
- **Hides the content** of the malware on infected systems
- Allows **full remote control** & P2P capabilities
- **Only Siemens SCADA Step 7** & in particular centrifuges

An example: Stuxnet (speculation)

- Industrial sabotage
- Cyberwar tool kit
- USA, Israel, India, China…….who else? Maybe the Aliens?? ;)
- Atomstroyexport (TrojanDownloader.Agent.IJ trojan)
- 19790509 in the Windows registry (US & USSR sign Salt 2 treaty, limiting nuclear weapons) – not a US date format
- Experiment gone wrong
- PoC (proof of concept)

A new paradigm shift. Why?

* A **new class** and **dimension** of **malware**
* **Not only** for its **complexity** and **sophistication**
* The attackers **have invested a substantial amount of time and money** to build such a complex attack tool (average: 1 MLN US$)
* Can be considered as the "**first strike**", i.e. one of the first organized, well prepared attacks **against major industrial resources**
* MITM (man in the middle) attacks on **PLCs**, **industrial devices**, and **embedded systems**
* **Potential associated** with Wi-Fi & for radio-frequency identification (RFID) hacking, - “smart-meter” hijacking and much more (think about SCADA-related industry: Water Companies, Energy Power plants, Highways, etc, etc.)

What did Stuxnet mean?

- The **first time** that mass-media wrote about "Industrial Automation & SCADA security".
- Stuxnet "helped", **Intelligence Agencies** & **Military Forces** to think about "**the next [IT] war**" - also helping government contractors.
- Stuxnet helped also **security researchers** to "track back the attack" to a **state sponsored attack tool**.
- Stuxnet may be a **basis for future extortion.**
- **Blueprint** for the next generation of malware.

*Fresh news ☹

DEBKAfile
We Start Where the Media Stop | Est. 2000

Max your DEBKA - Register Here!
User Name Password Forgot password? Log In

VJ VIRTUAL JERUSALEM THE PLACE WHERE JEWS CLICK

Home | Hebrew | DEBKA-Weekly | News Alerts | Review | Advertise | About Us | Contact | Search

Mon November 29, 2010 Breaking News: Netanyahu appoints Tamir Pardo new Mossad chief • He served as deputy of director Meir Dagan who retires after 8

Related Articles

Nuclear scientist killed in Tehran was Iran's top Stuxnet expert

DEBKA*file* Special Report November 29, 2010, 2:49 PM (GMT+02:00)
Tags: Iranian nuclear scientists ›› Top Stuxnet expert ››

World


Targeted nuclear scientist's car

Exclusive from DEBKA*file*'s intelligence sources:

Prof. Majid Shahriari, who died when his car was attacked in North Tehran Monday, Nov. 29, headed the team Iran established for combating the Stuxnet virus rampaging through its nuclear and military networks. His wife was injured. The scientist's death deals a major blow to Iran's herculean efforts to purge its nuclear and military control systems of the destructive worm since it went on the offensive six months ago. Only this month, Stuxnet shut down nuclear enrichment at Natanz for six days from Nov. 16-22 and curtailed an important air defense exercise.

Prof. Shahriari was the Iranian nuclear program's top expert on computer codes and cyber war. .

Another Iranian nuclear scientist, Prof. Feredoun Abbassi-Davani, and his wife survived a second coordinated attack with serious injuries. He is Dean of Students, a key political post at the university

Ali Salehi, Director of Iran's Nuclear Energy Commission, reacted bitterly that there is a limit to Iran's patience and whoever committed the murder is playing with fire. Tehran held US intelligence and the Israeli Mossad for responsible for the scientist's death.

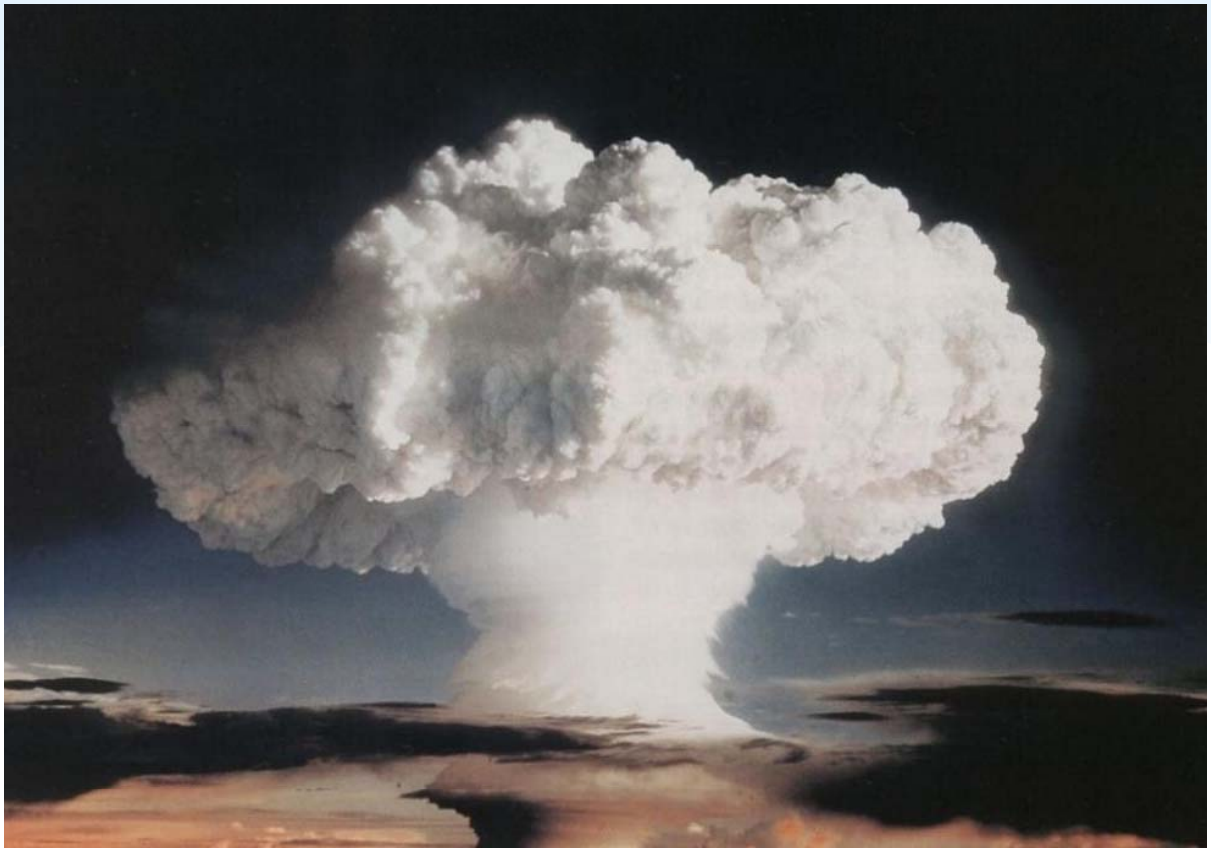
Tehran's official account of the attacks is only half-correct, are sources report. There were indeed two motorcycle teams of two riders each who shadowed the scientists' vehicles on their way to their laboratories and offices at Beheshti Basij Forces University in North Teheran early Monday. It was initially reported that the motorcyclists sped past them, attached explosives to the targeted Peugeots and were gone before they exploded.

However, the first photos of the scientists' vehicles showed them to be riddled with bullet holes rather than explosive damage, meaning they were hit by drive-by shooters.

It is important to note that the attacks took place in the most secure district of Tehran, where the top-secret labs serving Iran's nuclear facilities are located. They must therefore have been set up after exhaustive and detailed surveillance.

Top Stories

- Israel pushed for US to approve strike on Iran
- Few shockers in WikiLeaks' first batch of classified diplomatic files
- South Korea rejects talks, North threatens merciless blows
- Hariri walks into the Iranian web abandoned
- Brits declared war on Stuxnet. Americans say: Use it on North Korea
- Stuxnet knocks Natanz out for a week, hits Iran's air defense drill
- Washington spurns Tokyo's demand to punish North Korea
- Syrian, Hizballah's guided missiles defy Israel's aerial supremacy



* Cyberwar Defense

Avoiding being a victim of cyberwar

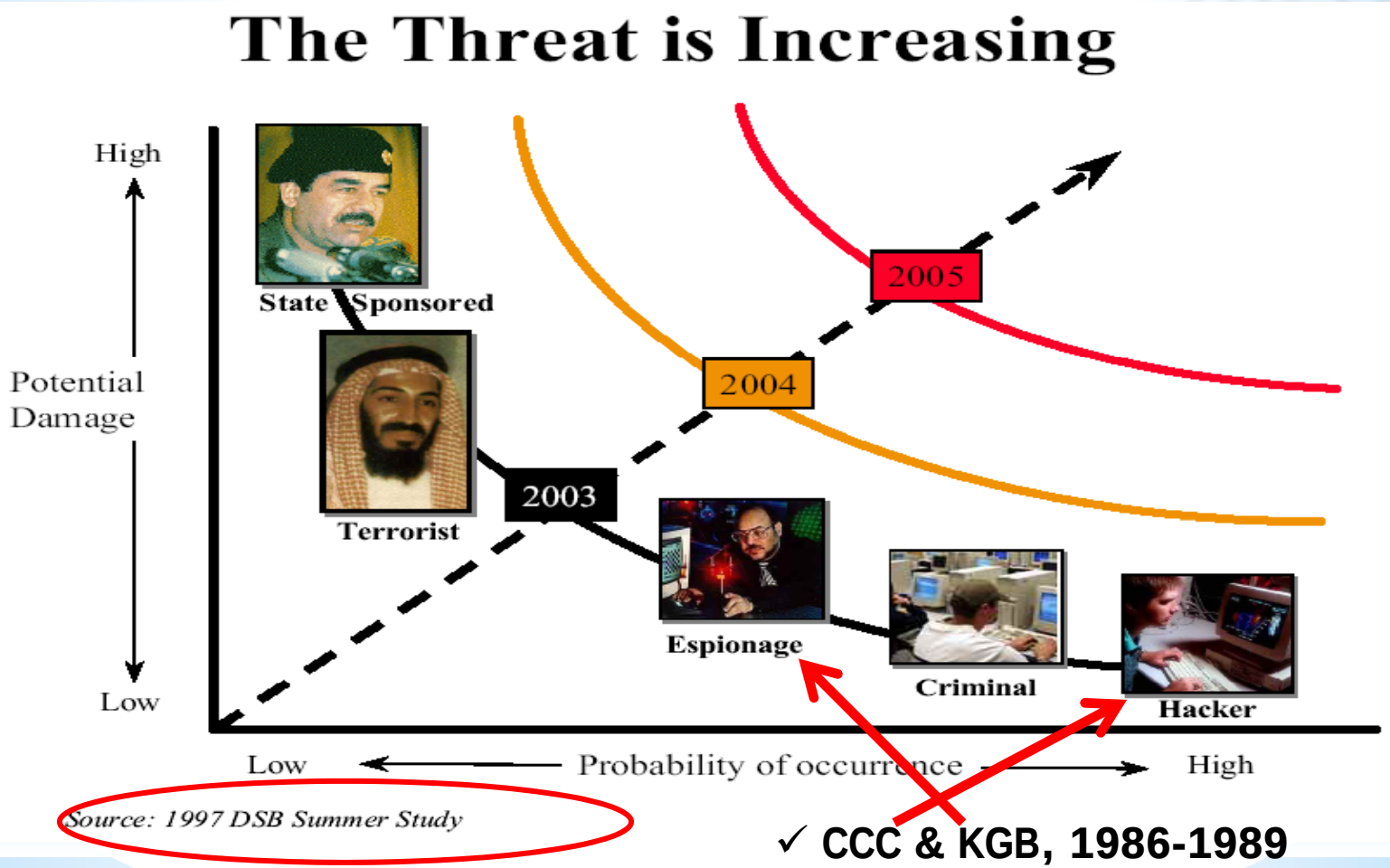
Control of:

- **Cybercrime** (learning from it, then applying its logic to InfoWar)
- Critical **industrial** infrastructure & **contractors**
- **Over reliance** on single routing of communications
- MITM (man in the middle) – gaps **in the systems**
- **Mobile** computing & **thumb drives**
- Important Internet servers and **national communications infrastructure**
- **Improved** Encryption & access

Opportunity for hackers

- The "job of your life": **being paid** in order to **hack remote systems**, while being also **legally authorised** to do it!!! ☺
- The 0-days market will **benefit from this**
- Military and Government organizations **already began hiring hackers** for consulting, Red Teams building, etc
- **Standards** such as the **OSSTMM** (ISECOM) may be **easily applied** and used in this **scenario**, while it's not a "standard pentest" LOL

*Learning from the history



*Learning from the history/2

- ✓ CCC&KGB (‘80s)
- ✓ Vodafone Greece attack
- ✓ Telecom Italia / Kroll infowar
- ✓ Estonia Cyber-war (2007)
- ✓ Russia-Georgia Cyber-war (2008)
- ✓ North-Korea Attacks (2009)
- ✓ Google-China Operation Aurora (2010)
- ✓ Iran / ? – STUXNET (2010)

*Learning from the history/3

- US/Israel Hacking US (February 1998)
  - "Solar Sunrise"
  - DoD, Air Force, Navy, Marine Corps
- Russia (ex KGB building) Hacking US (Sept 1999)
  - „Moonlight Maze"
  - Classified naval codes, missile guidance systems info
- China Hacking US (2003-2005)
  - "Titan Rain"
  - Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, NASA
- South Korea (Oct 2004)
  - Engaged lots of military hackers
- Russia (May 2007)
  - Russia attacks Estonia government, DDoS
  - Parliament, Ministries, Banks and Media
- Czech Republic (June 2007)
  - Hackers broadcast "nuclear bomb" on morning's prime time national television (alike "The war of the worlds"...)

* Pics gallery for our Chinese friends ;)


Chinese Hacker
抗议麦当劳官方网站将台湾列为国家，台湾是中国不可分割的一部分，任何企图将台湾从分裂中国分裂出去，阻碍海峡统一的妄想都必将覆灭！！我们只有一个中国！！！
www.china-defense-mashup.com

Shanghai Jiao Tong University


兵信息化素养
事高科技人才
www.china-defense-

CENSORED IN THE PUBLIC VERSION OF THIS PRESENTATION

(YOU SHOULD HAVE ATTENDED CONFIDENCE 2.0 @ PRAGUE!!)

CENSORED IN THE PUBLIC VERSION OF THIS PRESENTATION

(YOU SHOULD HAVE ATTENDED CONFIDENCE 2.0 @ PRAGUE!!)

CENSORED IN THE PUBLIC VERSION OF THIS PRESENTATION

(YOU SHOULD HAVE ATTENDED CONFIDENCE 2.0 @ PRAGUE!!)

CENSORED IN THE PUBLIC VERSION OF THIS PRESENTATION

(YOU SHOULD HAVE ATTENDED CONFIDENCE 2.0 @ PRAGUE!!)

CENSORED IN THE PUBLIC VERSION OF THIS PRESENTATION

(YOU SHOULD HAVE ATTENDED CONFIDENCE 2.0 @ PRAGUE!!)

*Acknowledgments

* All of the **InfoSec community** for their never-ending support
* **Indianz** (indianz.ch) for a couple of slides and ideas I grabbed from him
* An **anonymous US friend** for its cool grammar check ☺
* **ALL** of the **wonderful CONfidence staff**
* Local **vodka**
* The hotel's **barman**
* **Local stuff** better not mention here ;)

* Jart Armin: jart@cyberdefcon.com
* Raoul Chiesa: chiesa@UNICRI.it

CyberDefcon – Cybercrime Clearing House & EU Early warning Coalition

UNICRI - United Nations Interregional Crime and Justice Research Institute

ENISA -the European Network and Information Security Agency

The opinions hereby expressed are those of the Authors and do not necessarily represent the ideas and opinions of the United Nations, the UN agency "UNICRI", ENISA, ENISA PSG, nor others.

*Contacts, Questions