



Confidence 2011
24-25 May 2011, Krakow

The Son of STUXNET. a.k.a. “The Very Next Scenarios”

Presented by:

Raoul Chiesa

Senior Advisor on Cybercrime Issues at the

United Nations

Interregional Crime & Justice

Research Institute (UNICRI)

Member of the

Permanent Stakeholders Group (PSG)

@ European Network & Information

Security Agency (ENISA)

Design & Concept:

Jart Armin & Raoul Chiesa

CONFidence, Krakow , May 24th, 2011



* Agenda

- * **Disclaimer**
- * **The Authors**
- * **Introduction, Reasons for this talk**
 - * Bye bye, Wargames...
 - * Evolution of Cyber Attacks
 - * Information Warfare
 - * Shared points between Cybercrime & InfoWar
 - * Countries at stake
- * **New concepts for a new era**
 - * The Paradigm Shift
 - * Digital Weapons comparison
 - * A case study: Stuxnet
- * **Q&A**
- * **Extra Material (About UNICRI; Stuxnet technical details)**



*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 local 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 IT underground scene since 1986
- * Advisor @ UNICRI since 2004
- * ENISA PSG (2010-2012)
- * Founder, @ Mediaservice.net - *Independent Security Advisory Company.*
- * Founder, Board of Directors at: CLUSIT (Italian Information Security Association), ISECOM, OWASP Italian Chapter
- * TSTF.net Associate Partner
- * Member: ICANN, OPSI/AIP, EAST
- * Supporting: Team Cymru, APWG, ...

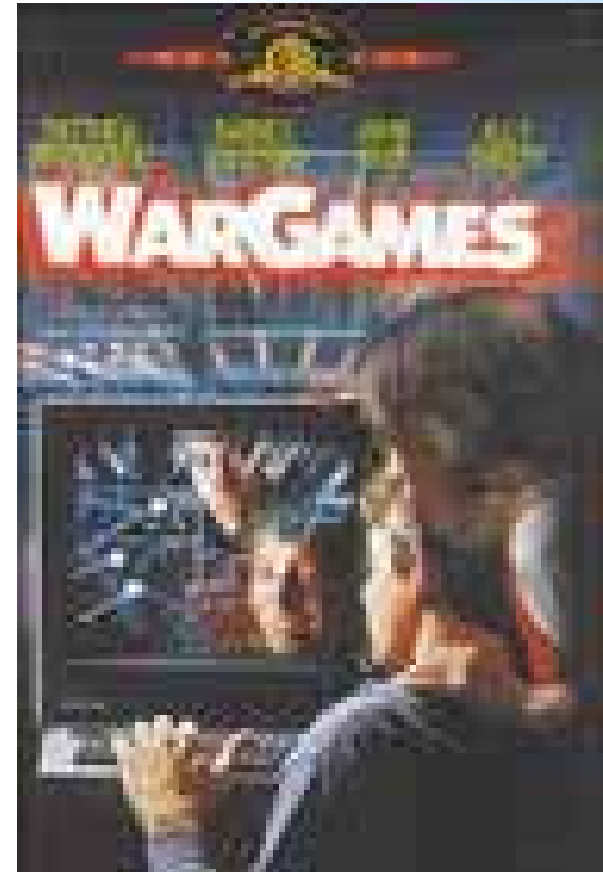


*The Authors - Jart Armin

- * Independent Security Expert & 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!

* Once upon a time...

- * In **1983**, the movie “Wargames” went out.
- * At least **2 generations of teenagers** began “playing hacking” because of this movie.
- * In the script, the lead character was nearly able to launch a “**global thermo-nuclear**” war.
- * All of us we’ve used to **laugh** at that movie...
- * Nevertheless, the IT attacks launched in the last 25 years, **still mainly relay** on the hacking-techniques shown in the movie.
- * It’s the **history**, played in “repeat mode”.



❑ Hacking with friends



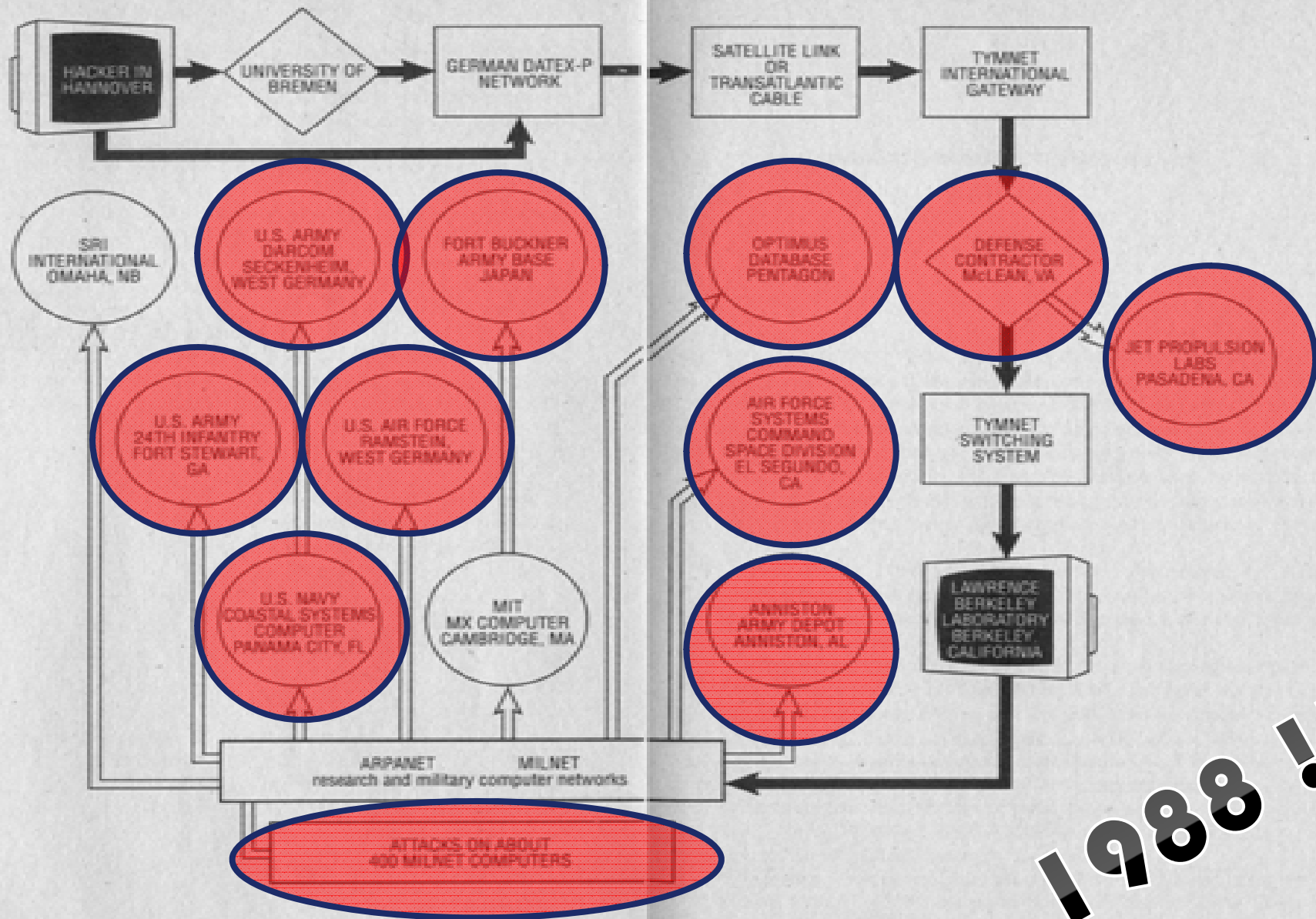
❑ Wardialling PSTN & Toll-Free / Port Scanning / X.25 scanning



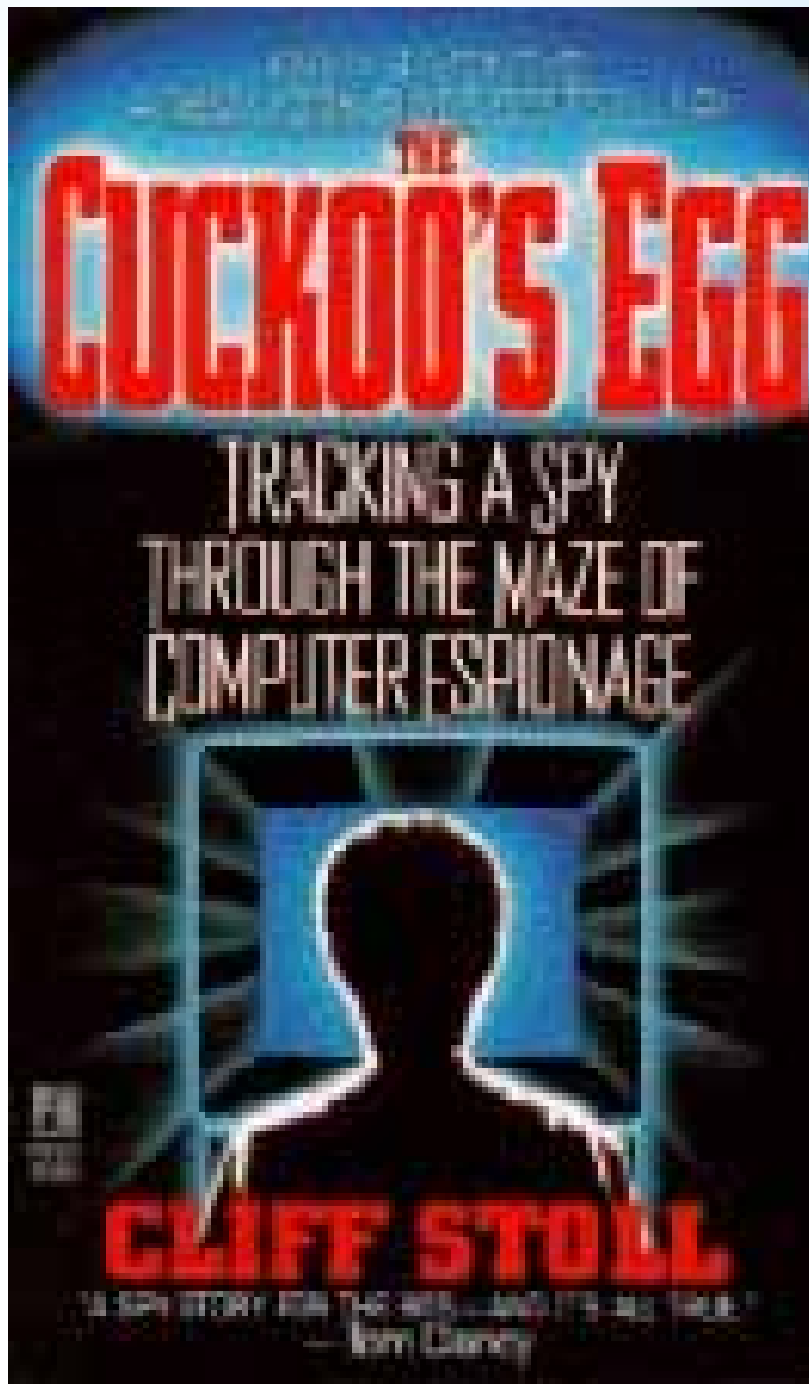
❑ ...Getting access.



* 5 years later...



© Jart Armin & Raoul Chiesa, 2011



* Reasons for this talk

* Speaking along with a lot of 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 2009/2010) 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 along the years you've 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)
- * etc. etc.

* ...in the next (five to ten) years, you will hear non-stop about:

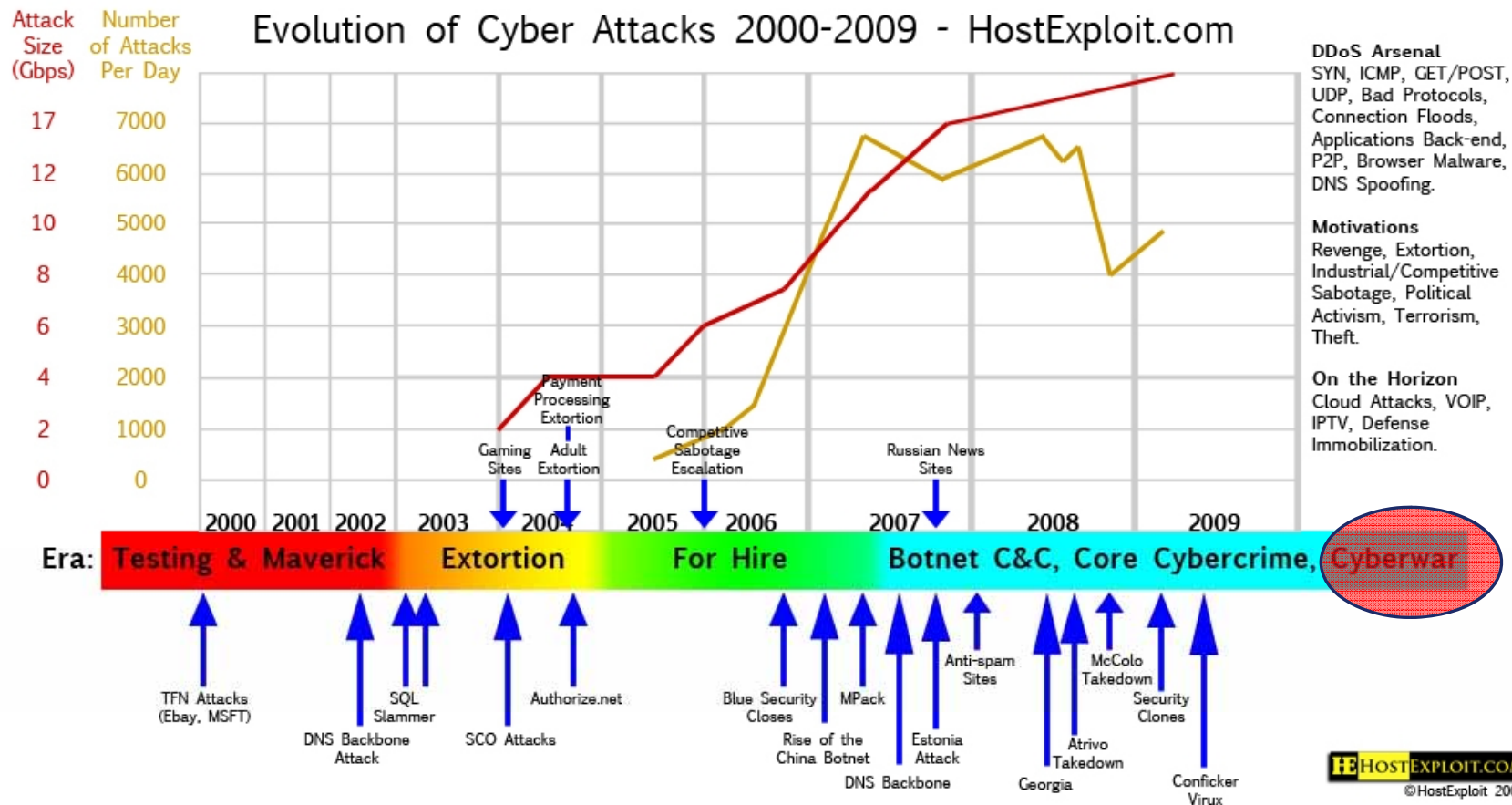
- * NGC - Next Generation Cybercrime
- * CyberWar
- * Information Warfare
- * NGW - Next Generation Warfare

	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 (2004-2011)

* TODAY: bye bye, “Wargames”

- * No more “Wargames”
 - * (even if: Wargames 2010 went out, and Bruce Willis got the support of an “hacker” in the latest Die Hard): the “romantic hackers” are gone, forever ☹
- * Then Stuxnet appeared
 - * (May-June 2010).
- * ...and **everything changed.**
- * **WHY??**
 - * **An unexpected** attack.
 - * An unexpected **target** (SCADA, Nuclear Plant).
 - * The **very first time** something like this was happening.



* Evolution of Cyber Attacks

* 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**.

Uh? Stopping a Nuclear Plant is not “dominate information”...

* 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..**
- * Think about **Estonia, Georgia**...what will be next?

* Shared Points between Cybercrime & InfoWar

- * **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 + ad-hoc exploiting.
- * **(attacker’s perspective) Nothing changes that much.** There’s more chances to hack 1000 broadband users instead of 10.000 PCs from a company’s network.
- * It’s still the **digital weapon** they need in order to **launch attacks** (DDoS, Keyloggers, 0-Days, etc).

* Being military “trendy”

OUT ☹

Single operational pic
Autonomous ops
Broadcast information push
Individual
Stovepipes
Task, process, exploit, disseminate
Multiple data calls, duplication
Private data
Perimeter, one-time security
Bandwidth limitations
Circuit-based transport
Single points of failure
Separate infrastructures
Customized, platform-centric IT

IN ☺

Situational awareness
Self-synchronizing ops
Information pull
Collaboration
Communities of Interest
Task, post, process, use
Only handle information once
Shared data
Persistent, continuous IA
Bandwidth on demand
IP-based transport
Diverse routing
Enterprise services
COTS based, net-centric capabilities
Scouting elite hacker parties?

* Countries at stake

- USA
- UK, Canada, France, Germany, Switzerland, Italy
- Brazil
- Israel, Palestinian National Authority
- Zimbabwe
- Middle East: “friendly” countries (UAE, Saudi Arabia...)
- North Africa / Africa generally speaking (WW Soccer Games 2010)
- China
- India
- Pakistan
- North Korea (DPRK)
- South Korea
- Iran
- Kyrgyzstan
- Myanmar
- Russia, Estonia, Georgia
- Rwanda

“Low Risk”

“Average Risk”

“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			<i>Probable</i>	X
Cyberwarfare training	X	X	X		X	
Cyberwarfare exercises/simulations	X	X				
Collaboration with IT industry and/or technical universities	X	X	X		X	X
IT road map	<i>likely</i>	X				
Information warfare units	X	X		X		
Record of hacking 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?!? **Seriously??**
- * 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 **BTs** 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."

Former Duma speaker Nikolai Kuryanovich, 2007



* Cyber War

* Cybercrime to Cyberwar Tools of the Trade



* Botnet & drone armies



* DDoS



* Trojans & Worms



* Malware



* Server hacking



* Encryption



* Extortion & Ransom



* Man in the Middle

Countries

- * Russia
- * USA
- * France
- * Israel
- * UK
- * China
- * India
- * Pakistan
- * Ukraine
- * Malware Factories

Activities

- * Cyber crime tools
- * Communications Intelligence
- * National knowhow defence
- * Transition from Industrial tools
- * Hired Cyber mercenaries
- * Industrial espionage
- * Counter cyber attacks
- * Cyber army
- * Botnet armies
- * Contract developers (x 4 worldwide)

* Cyber Weapons capability

Countries

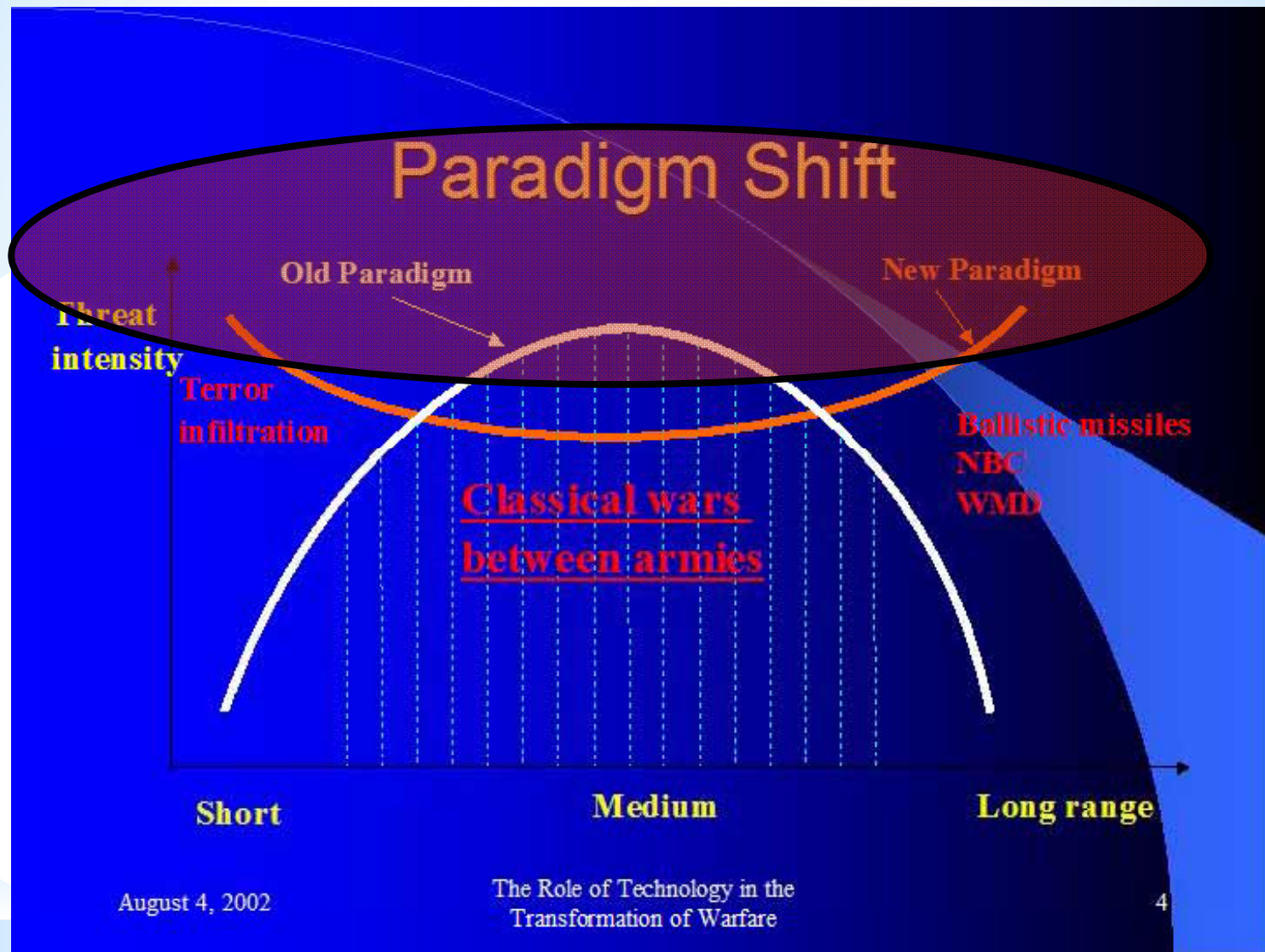
- * UN Member States = 197
- * Vulnerable?
- * **197 !!!!**

Weapon Vulnerability

- * Hacking
- * DDoS
- * Botnets
- * Defacement
- * Web site Hijacking & Redirection
- * DNS & BGP hijacking
- * BlackEnergy
- * Darkness
- * Stuxnet

* Nations exposed to
Cyber Weapons

* Why? The Paradigm Shift





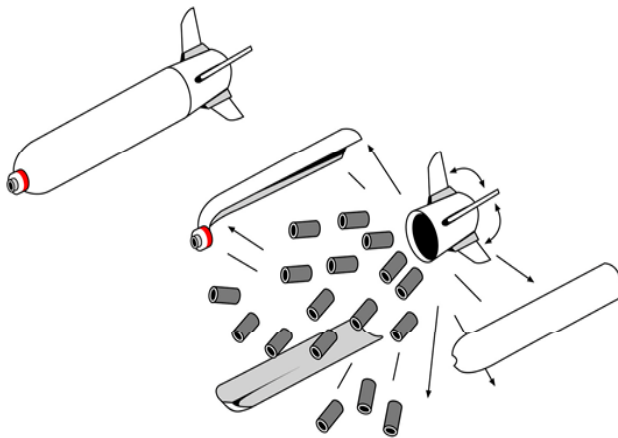
* Cyberwar: the weapons of choice

* 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

The "Ad"

Good time of the day dear citizens of DL
We are offering a quality DDoS Service
We have the best combination of quality and service!
We accept any targets regardless of their theme!
Regular customers will get special conditions
On average, we charge \$50 per 24 hour period
All depends on the complexity of the attacked site
We accept payments via Webmoney
For people interested in permanent job positions
we have a special job offer that you will not decline
We are online 24 hours a day
Commands:
[+] ping commands are fine tuned to perfection
[+] Downloading Flood (new*)
[+] POST flood (new*)
[+] http attack on host
[+] icmp attack on host
[+] port attack
our contacts
[mail]: SMileFrince@yandex.ru
[jabber]: smile@darkdna.net (new*)
[icq]: 966-999

"Fire-Power"

- * 30 bots overwhelm an average web site
- * 1,000 bots - large web site
- * 5,000 bots - even when using anti-ddos, blocks, and other preventive measures
- * 15,000 bots can theoretically bring down vkontakte.ru (Russian Facebook)
- * Example of Conficker worm reached 10.5 million bots



* Darkness DDoS Botnet

*Entering Cyber War?

* A case study: 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 (speculations)

- * 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)

Cyber Weapons - Stuxnet

An F16 just flew over a
1st World War Battlefield



* 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**.

* News (April 26th, 2011)

- * It looks like IRAN has been “attacked” **again** (?)
- * “IRAN has detected a second *spy virus* **designed to harm government systems**, a senior Iranian military official said.”
 - * <http://www.bloomberg.com/news/2011-04-26/iran-discovers-second-virus-aimed-at-damaging-government-systems.html>
 - * <http://topics.bloomberg.com/iran/>
- * “Iran announces **discovery of new cyber attack**, started by mistake **from a strange PDF sent by friends of mine.**”
 - * http://www.silobreaker.com/iran-announces-discovery-of-new-cyber-attack-5_2264522225149280265

***Then suddenly the “news”
disapperead....?!?**



Cyberwar Defense

* Avoiding being a victim of cyberwar

Control of:

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

- * 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

*Extra Material



What is UNICRI?

United Nations Interregional Crime & Justice Research Institute

A United Nations entity established in 1968 to support countries worldwide in crime prevention and criminal justice

UNICRI carries out applied research, training, technical cooperation and documentation / information activities

UNICRI disseminates information and maintains contacts with professionals and experts worldwide

Emerging Crimes Unit (ECU): cyber crimes, counterfeiting, environmental crimes, trafficking in stolen works of art...

**Fake Bvlgari & Rolex
Viagra & Cialis (aka)**

Water syst

**Guess how they update each others?
Email, chat&IM, Skype...**

UNICRI & Cybercrime



Overview on UNICRI projects against cybercrime

Hackers Profiling Project (HPP)

SCADA & NCI's security (CIP)

Digital Forensics and digital investigation techniques

Cybersecurity Trainings at the UN Campus



* Ad-hoc Trainings on SCADA security at the United Nations



unicri

advancing security, serving justice,
building peace



mediaservice.net
CORPORATE SECURITY & IMAGE

FIRST COMPREHENSIVE TRAINING PROGRAMME on

CYBER CRIMES

evaluating new threats, assessing your REAL security

- **Information Security (InfoSec)**
- **Hacker Profiling Project (HPP)**
- **Digital Forensics**
- **SCADA and NCI**

2011

http://www.unicri.it/emerging_crimes/cybercrime/

From February 2010 @ UN Campus in Turin, Italy

www.unicri.it/wwd/cybertraining

* On Hacker's Profiling



© Jart Armin & Raoul Chiesa, 2011

The Hackers Profiling Project (HPP)



HPP purposes

Analyse the hacking phenomenon in its several aspects (technological, social, economic) through technical and criminological approaches

Understand the different motivations and identify the actors involved

Observe those *true* criminal actions “in the field”

Apply the profiling methodology to collected data (4W: who, where, when, why)

Acquire and disseminate knowledge

The Hackers Profiling Project (HPP)



Project phases - starting: September 2004

1 - Theoretical collection:
Questionnaire

2 - Observation:
Participation in IT underground security events

3 - Filing:
Database for elaboration/classification of data (phase 1)

4 - Live collection:
Highly customised, new generation Honey-net systems

5 - Gap analysis:
of data from: questionnaire, honey-net, existing literature

6 - HPP “live” assessment
of profiles and correlation of modus operandi through data from phase 4

7 - Final profiling:
Redefinition/fine-tuning of hackers profiles used as “de-facto” standard

8 - Diffusion of the model:
elaboration of results, publication of the methodology, raising awareness

The Hackers Profiling Project (HPP)



Project phases - detail

PHASE	CARRIED OUT		DURATION	NOTES
1 - Theoretical collection	YES	ON-GOING	16 months	Distribution on more levels
2 - Observation	YES	ON-GOING	24 months	From different points of view
3 - Filing	ON-GOING		21 months	The hardest phase
4 - “Live” collection	TO BE COMMENCED		21 months	The funniest phase ☺
5 - Gap & Correlation Analysis	YET TO COME		18 months	The Next Thing
6 - “Live” Assessment	PENDING		16 months	The biggest part of the Project
7 - Final Profiling	PENDING		12 months	“Satisfaction”
8 - Diffusion of the model	PENDING		GNU/FDL ;)	Methodology’s public release

The Hackers Profiling Project (HPP)

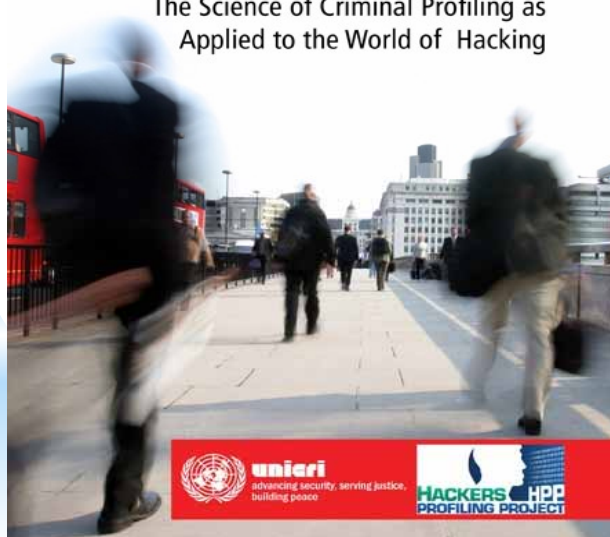


Profiling Hackers - the book

RAOUL CHIESA • STEFANIA DUCCI • SILVIO CIAPPI

PROFILING HACKERS

The Science of Criminal Profiling as
Applied to the World of Hacking



Content

- Introduction to criminal profiling and cyber-crime
- To be, to think and to live like a hacker
- The Hacker's Profiling Project (HPP)
- Who are hackers? (Part I-II)

Who is it for?

Professionals involved in the networking activity, police detectives, university professors and students of law interested in criminal psychology as well as primary school and high school teachers dealing with potential hacker students. More in general, this book is designed for anyone interested in understanding the mechanisms behind cyber crimes and criminal psychology.

• Profiling Hackers: the Science of Criminal Profiling as applied to the World of Hacking

ISBN: 978-1-4200-8693-5-90000

Evaluation and correlation standards

Modus Operandi (MO)

Lone hacker or as a member of a group

Motivations

Selected targets

Relationship between motivations and targets

Hacking career

Principles of the hacker's ethics

Crashed or damaged systems

Perception of the illegality of their own activity

Effect of laws, convictions and technical difficulties as a deterrent

The Hackers Profiling Project (HPP)



Detailed analysis and correlation of profiles - table #1

PROFILE	RANK	IMPACT LEVEL		TARGET	
Wanna Be Lamer	Amateur	NULL		End-User	
Script Kiddie		LOW		SME	Specific security flaws
Cracker	Hobbiest	MEDIUM	HIGH	Business company	
Ethical Hacker		MEDIUM		Vendor	Technology
Quiet, Paranoid Skilled Hacker		MEDIUM	HIGH	On necessity	
Cyber-Warrior	Professional	HIGH		“Symbol” business company	End-User
Industrial Spy		HIGH		Business company	Corporation
Government agent		HIGH		Government	Suspected Terrorist
				Strategic Company	Individual
Military Hacker		HIGH		Government	Strategic Company

The Hackers Profiling Project (HPP)



Detailed analysis and correlation of profiles - table #2

Profile	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

Must-read books / 1

During the different phases of bibliography research, the Authors have made reference (also) to the following publications and on-line resources:

- **H.P.P. Questionnaires 2005-2011**
- **Fatal System Error: the Hunt for the new Crime Lords who are bringing down the Internet**, Joseph Menn, Public Affairs, 2010
- **Stealing the Network: How to Own a Continent, (an Identity), (a Shadow)** (V.A.), Syngress Publishing, 2004, 2006, 2007
- **Stealing the Network: How to Own the Box**, (V.A.), Syngress Publishing, 2003
- **Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier**, Suelette Dreyfus, Random House Australia, 1997
- **The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage**, Clifford Stoll, DoubleDay (1989), Pocket (2000)
- **Masters of Deception: the Gang that Ruled Cyberspace**, Michelle Stalalla & Joshua Quinttner, Harpercollins, 1995
- **Kevin Poulsen, Serial Hacker**, Jonathan Littman, Little & Brown, 1997
- **Takedown**, John Markoff and Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996
- **The Fugitive Game: online with Kevin Mitnick**, Jonathan Littman, Little & Brown, 1997
- **The Art of Deception**, Kevin D. Mitnick & William L. Simon, Wiley, 2002
- **The Art of Intrusion**, Kevin D. Mitnick & William L. Simon, Wiley, 2004
- **@ Large: the Strange Case of the World's Biggest Internet Invasion**, Charles Mann & David Freedman, Touchstone, 1998

Must-read books / 2

- **The Estonia attack: Battling Botnets and online Mobs**, Gadi Evron, 2008 (white paper)
- **Who is “n3td3v”?**, by Hacker Factor Solutions, 2006 (white paper)
- **Mafiaboy: How I cracked the Internet and Why it's still broken**, Michael Calce with Craig Silverman, 2008
- **The Hacker Diaries: Confessions of Teenage Hackers**, Dan Verton, McGraw-Hill Osborne Media, 2002
- **Cyberpunk: Outlaws and Hackers on the Computer Frontier**, Katie Hafner, Simon & Schuster, 1995
- **Cyber Adversary Characterization: auditing the hacker mind**, Tom Parker, Syngress, 2004
- **Inside the SPAM Cartel: trade secrets from the Dark Side**, by Spammer X, Syngress, 2004
- **Hacker Cracker**, Ejov Nuwere with David Chanoff, Harper Collins, 2002
- **Compendio di criminologia**, Ponti G., Raffaello Cortina, 1991
- **Criminalità da computer**, Tiedemann K., in Trattato di criminologia, medicina criminologica e psichiatria forense, vol.X, Il cambiamento delle forme di criminalità e devianza, Ferracuti F. (a cura di), Giuffrè, 1988
- **United Nations Manual on the Prevention and Control of Computer-related Crime**, in International Review of Criminal Policy Nos. 43 and 44
- **Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale**, Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001
- **Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques**, Turvey B., Knowledge Solutions Library, January, 1998
- **Malicious Hackers: a framework for Analysis and Case Study**, Laura J. Kleen, Captain, USAF, US Air Force Institute of Technology
- **Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology**, Täterpro

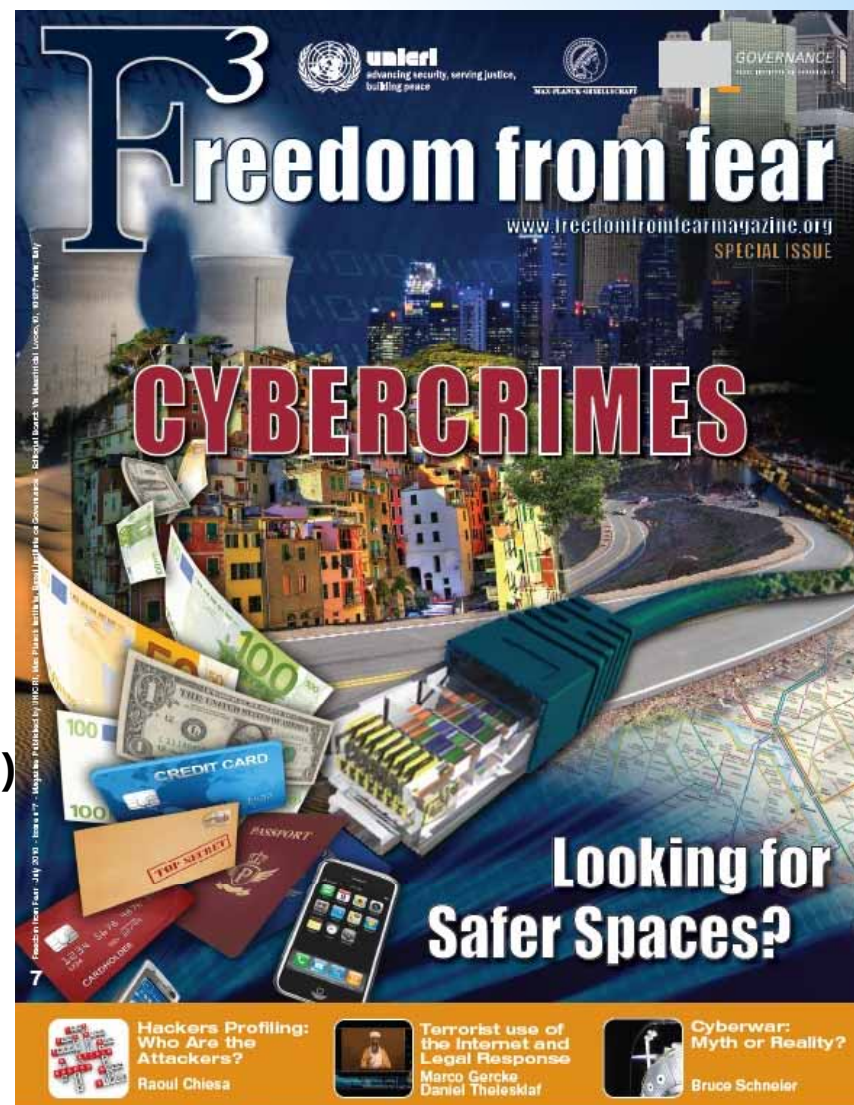
And...a gift for you all here at CONfidence 2011 Krakow! ☺

Get your own, FREE copy of “F3” (Freedom from Fear, the United Nations magazine) issue #7, totally focused on Cybercrimes!

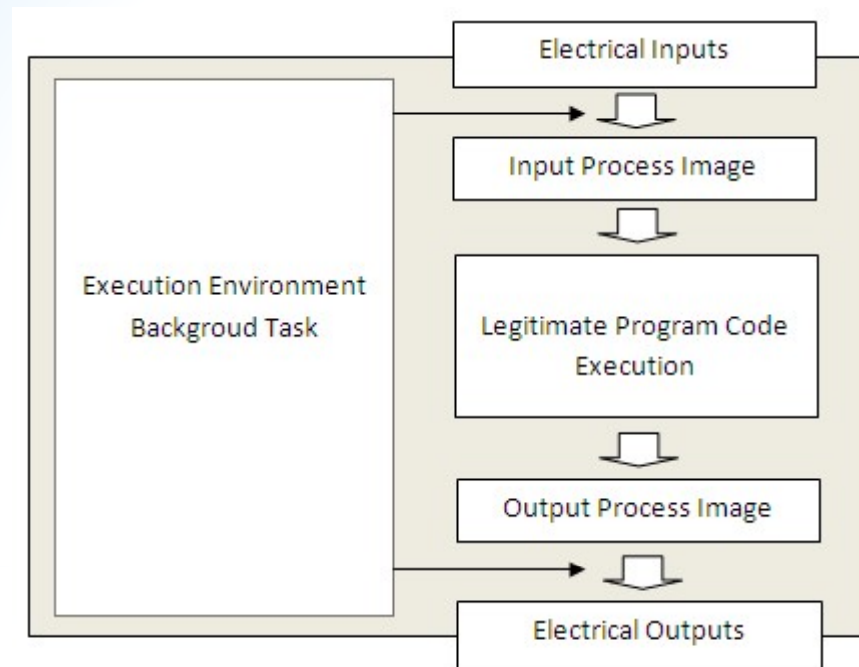
DOWNLOAD:

www.FreedomFromFearMagazine.org

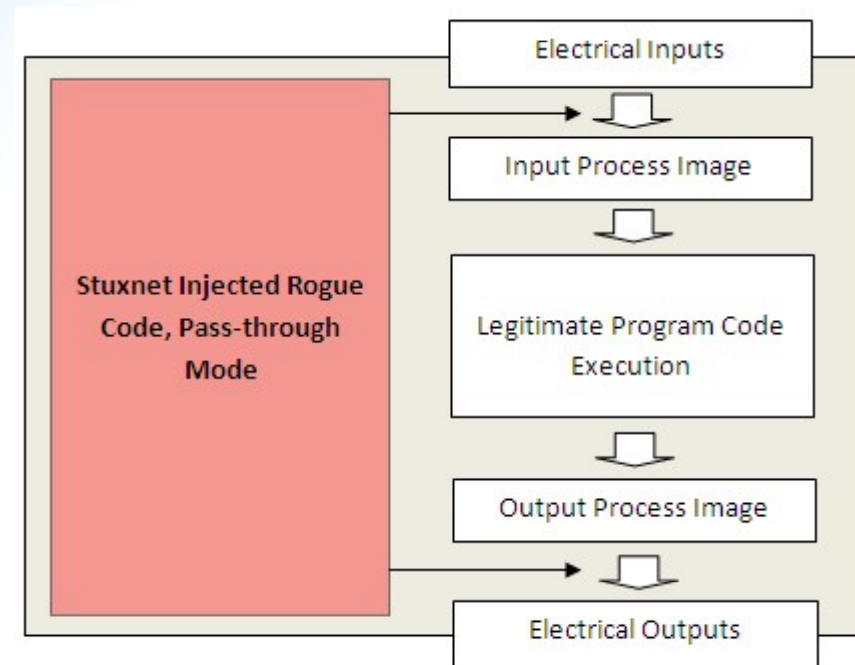
Or, email me and I will send you the full PDF (10MB)



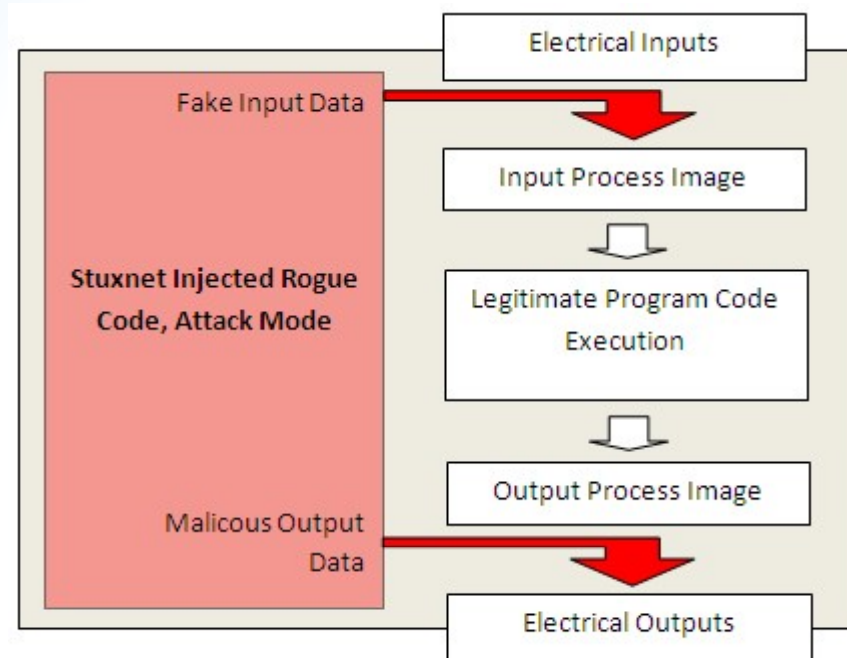
* Light zooms on Stuxnet



* Stuxnet - Attacked System - Normal Operation



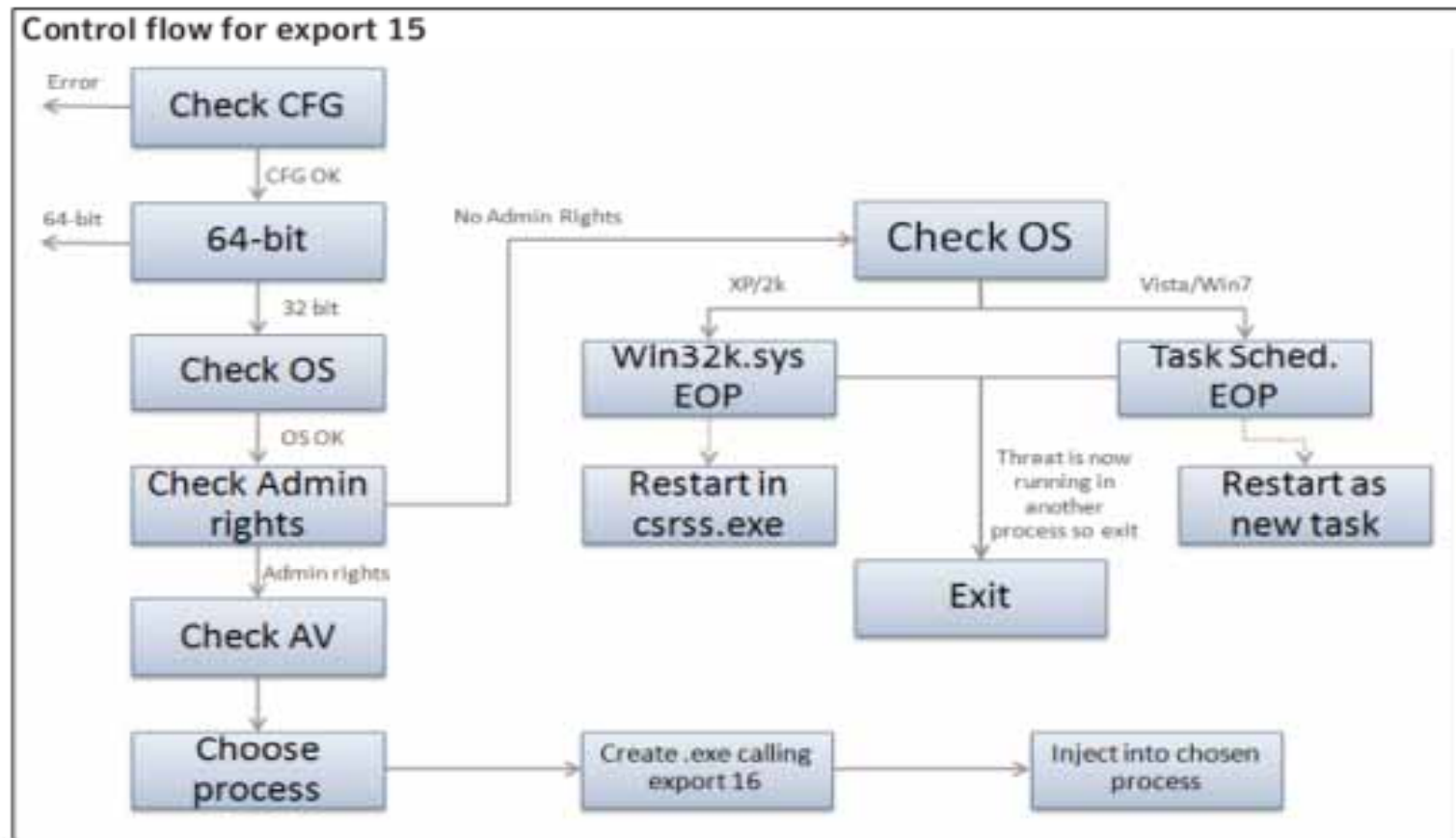
* Stuxnet - Attacked System MITM - Attack Mode



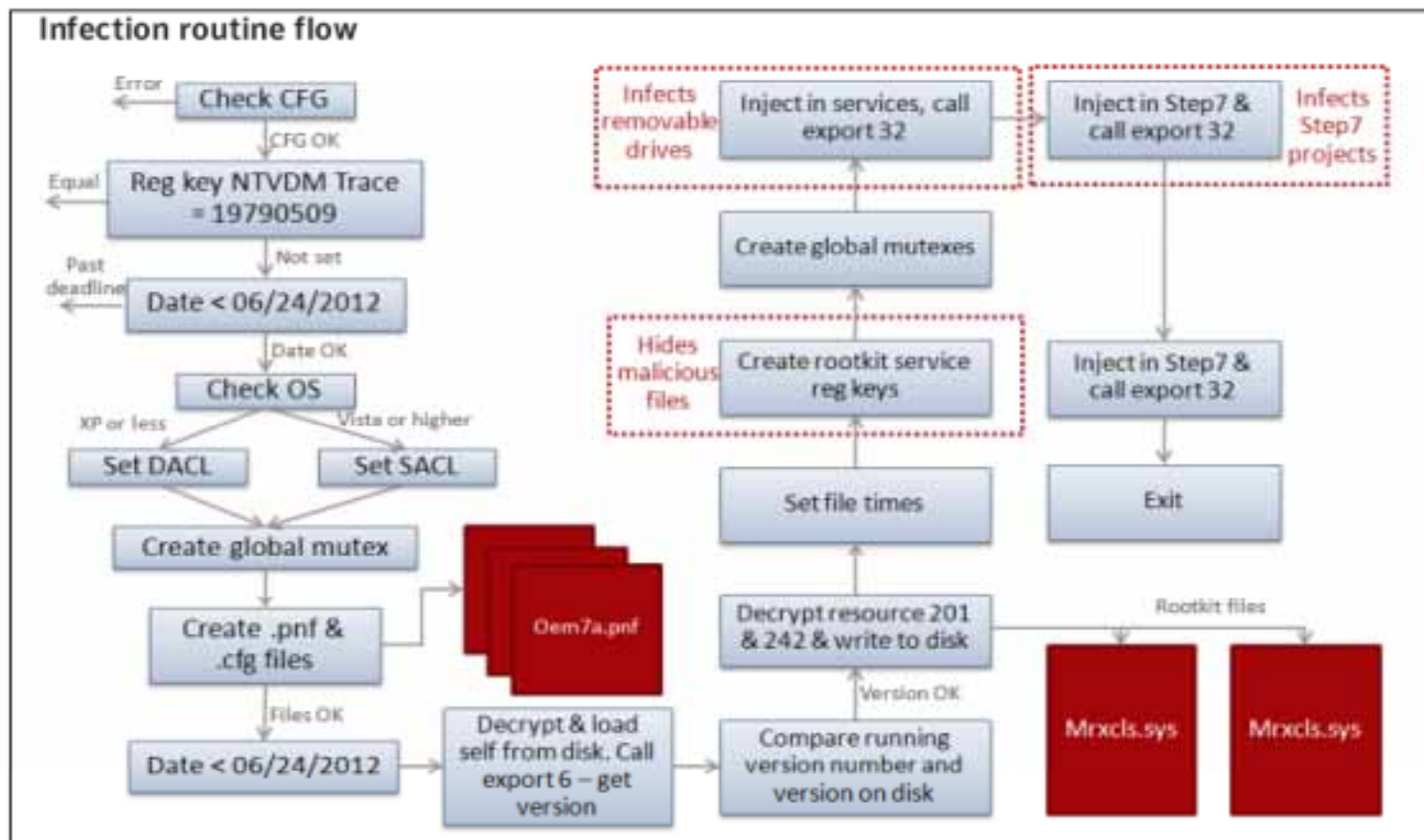
* Stuxnet - Attacked System MITM - Pass Thru Mode

Export #	Function
1	Infect connected removable drives, starts RPC server
2	Hooks APIs for Step 7 project file infections
4	Calls the removal routine (export 18)
5	Verifies if the threat is installed correctly
6	Verifies version information
7	Calls Export 6
9	Updates itself from infected Step 7 projects
10	Updates itself from infected Step 7 projects
14	Step 7 project file infection routine
15	Initial entry point
16	Main installation
17	Replaces Step 7 DLL
18	Uninstalls Stuxnet
19	Infects removable drives
22	Network propagation routines
24	Check Internet connection
27	RPC Server
28	Command and control routine
29	Command and control routine
31	Updates itself from infected Step 7 routines
32	Same as 1

* Stuxnet - The DLL export paths



* Stuxnet - checking the correct target

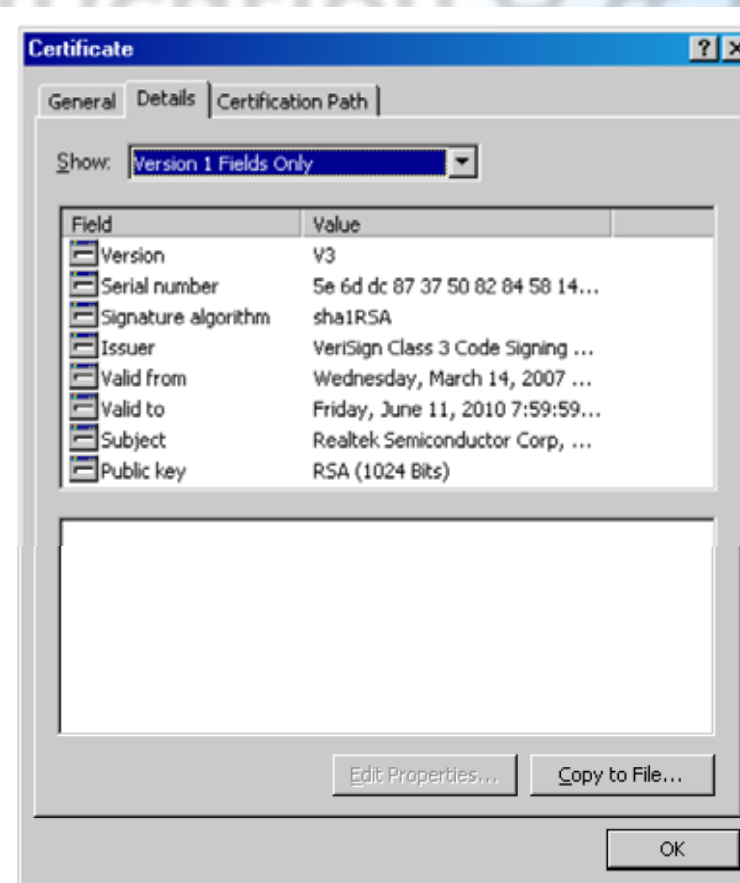
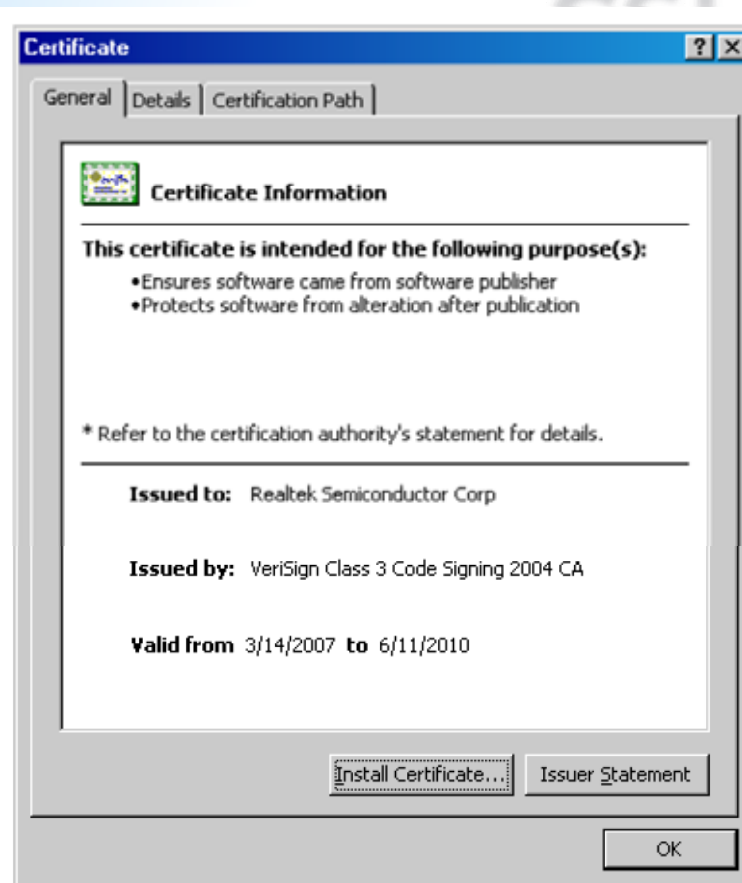


* Stuxnet - main injection process

Ref: Joel Langill

* Stuxnet - Stolen Certification A & B

SYSTEM32\MRXCLS.SYS



- * VirusBlokAda – Belarus
- * Symantec - Exploring Stuxnet's PLC Infection Process
- * Pierre-Marc Bureau : ESET - Stuxnet Under the Microscope, an analysis of Stuxnet
- * F-Secure - Stuxnet Questions and Answers
- * Joel Langill of ENGglobal, CSFI - Stuxnet Infection Video, Tofinosecurity
- * Ralph Langner's - Stuxnet is a directed attack -- 'hack of the century'
- * VB Conference in Vancouver
- * Ruben Santamarta, March 2011, RootedCon (Madrid, Spain)

* Stuxnet - Community Resources