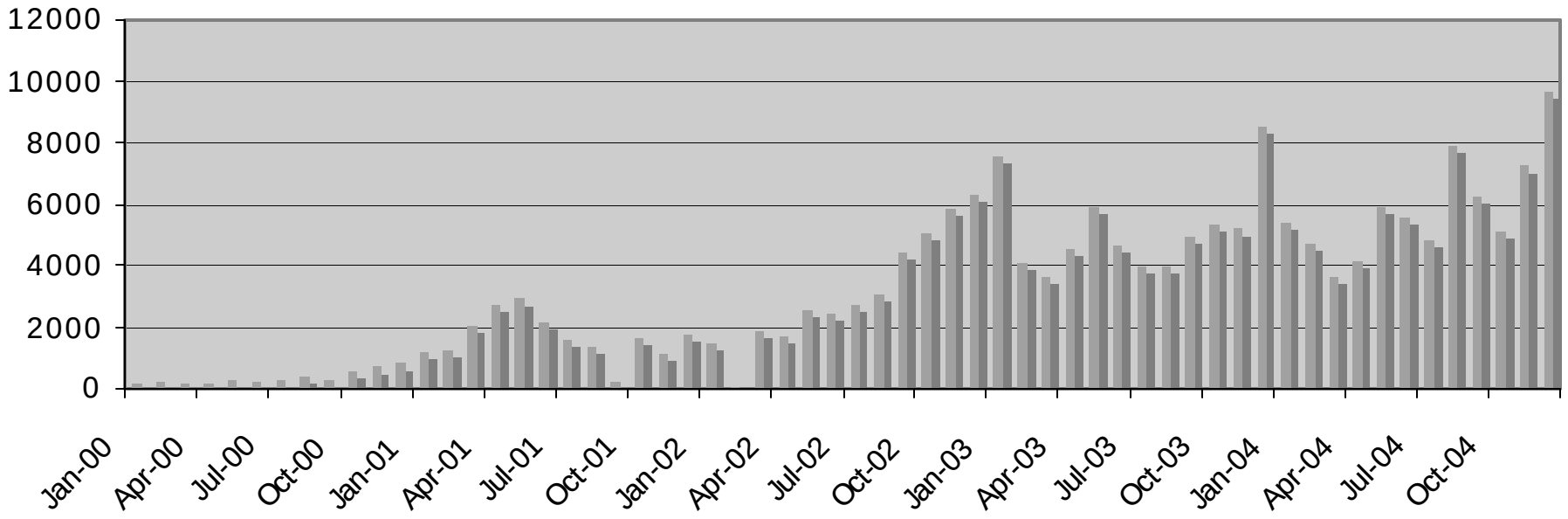
THE LECTURERS

Fabio Ghioni - Roberto Preatoni

INDEX

1) Introduction: old and new threats
2) Industrial Espionage and State-sponsored espionage
3) Cyber defense methodology: from digital identification of attacker to counterattack strategy
4) Cyber counterattacks: information leakage, Injected Interception

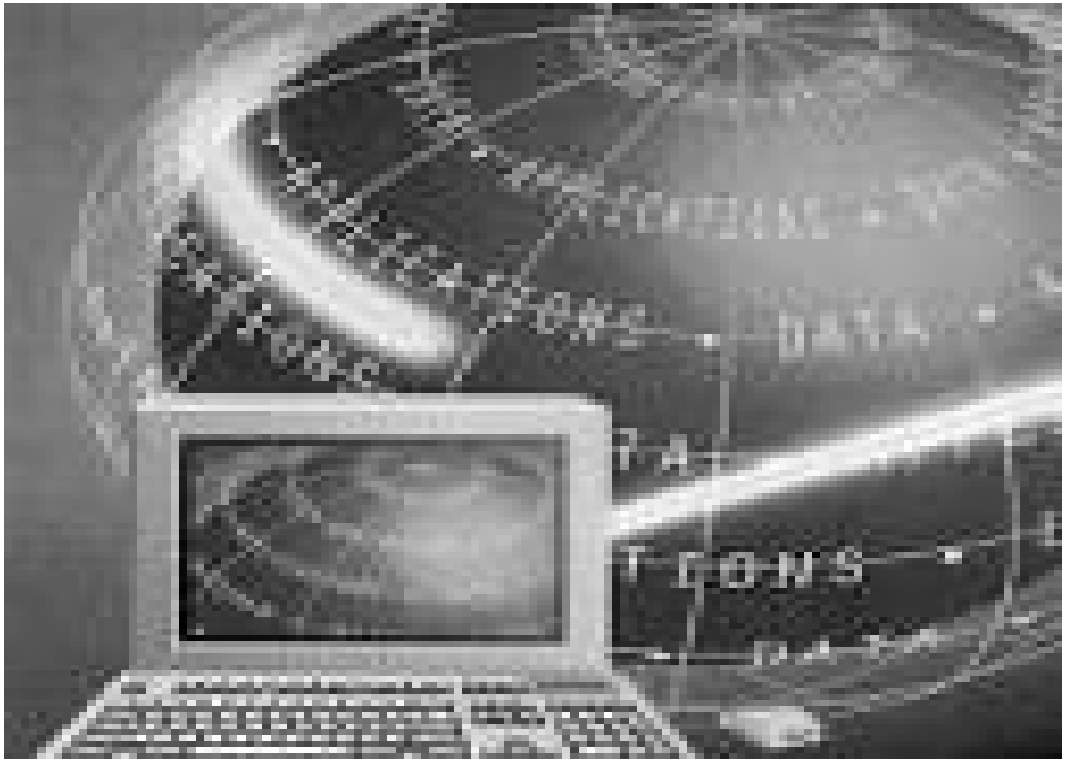
WEB SERVER INTRUSIONS 2000-2004



In the aftermath of September 11th, security issues came into the limelight... everybody focalized their attention on increasing anti-terrorist measures and countering the increasing number of hacker attacks to business and government networks...

... but hardly anyone has ever mentioned a more insidious and widespread criminal activity: INDUSTRIAL ESPIONAGE

WHY ?



Companies are often reluctant to publicly admit that they have been victims of industrial espionage for two main reasons:

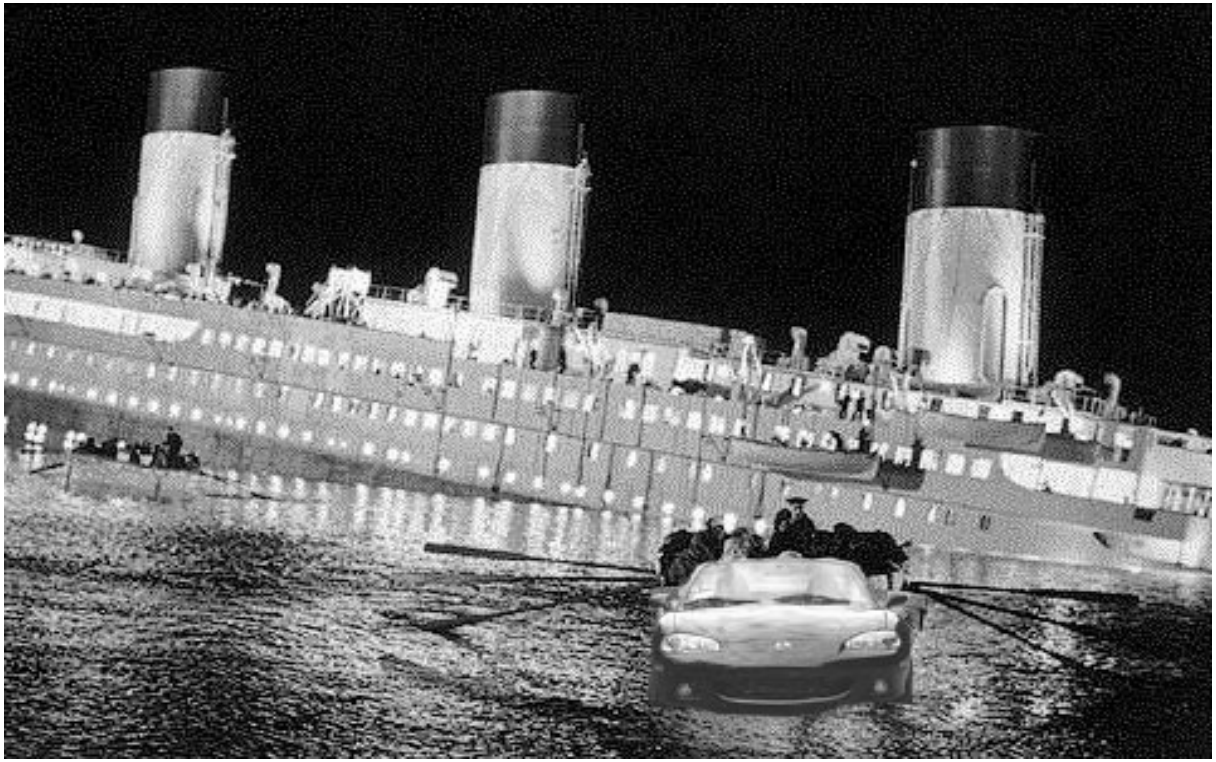
- it implicitly means that THERE WAS SOME KIND OF VULNERABILITY to be exploited
- it implies the unveiling of MORE CONFIDENTIAL lines of business

REAL CASES

-CC companies

-T-mobile

-K



WHAT exactly is INDUSTRIAL ESPIONAGE?

The illegal acquisition of intellectual property and trade secrets, in other words THEFT!

The techniques to steal information from outside a company range from the traditional eavesdropping to social engineering tactics...

Since the 1990s Western Intelligence Agencies appear to have focused most of their time and resources on industrial espionage

In most countries corporations rely on Government Agencies to carry out investigations whose results can be used to boost the National economy...

France, the United States and Israeli have often been accused to spying on competitors' industrial secrets through scanning systems such as Echelon or the Helios 1A satellite up until the more recent Carnivore software and Magic Lantern used officially for lawful interception (now outdated by more sophisticated solutions)

Conversely, the INDUSTRIAL/BUSINESS INTELLIGENCE process consists of researching information on public source documents in order to draw inferences about what competitors might be going to do and provide the basis for possible counteraction

Situational Awareness is the key word...

". . . attaining one hundred victories in one hundred battles is not the pinnacle of excellence.

Subjugating the enemy's army without fighting is the true pinnacle of excellence."

Sun Tzu, The Art of War

"There are but two powers in the world, the sword and the mind. In the long run the sword is always beaten by the mind."

Napoleon Bonaparte

Nevertheless, there is sometimes a fine line between the legitimate tactics of competitive intelligence gathering and the illegitimate practice of industrial espionage...

THE ATTACKS

AUTONOMOUS AGENTS / BOTNETS

Set up of botnets or drones instructed to perform searches within the traffic or within the PC content

SOCIAL ENGINEERING

Exploitation of human vulnerabilities

Big mouths

INFORMATION LEAKAGE AND DATA MANIPULATION

- Intranet access due to loose access policies
- Weak corporate applications
- Exploitation of insiders

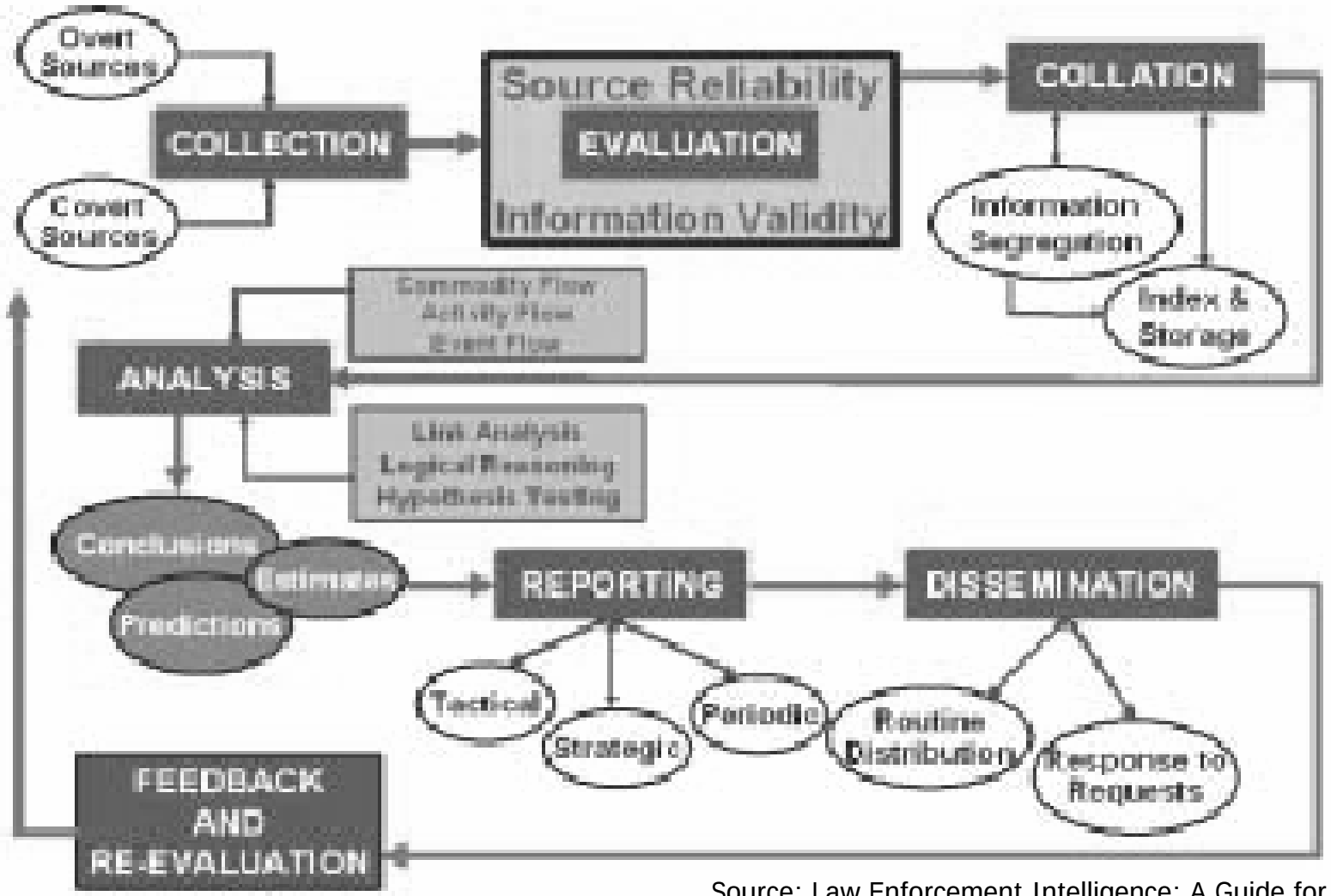
OPEN SOURCES GATHERING

- Old pal google
- Company pubblications

EMPLOYEES EXPLOITATION

- Home pc compromission
- Mailbox hijacking

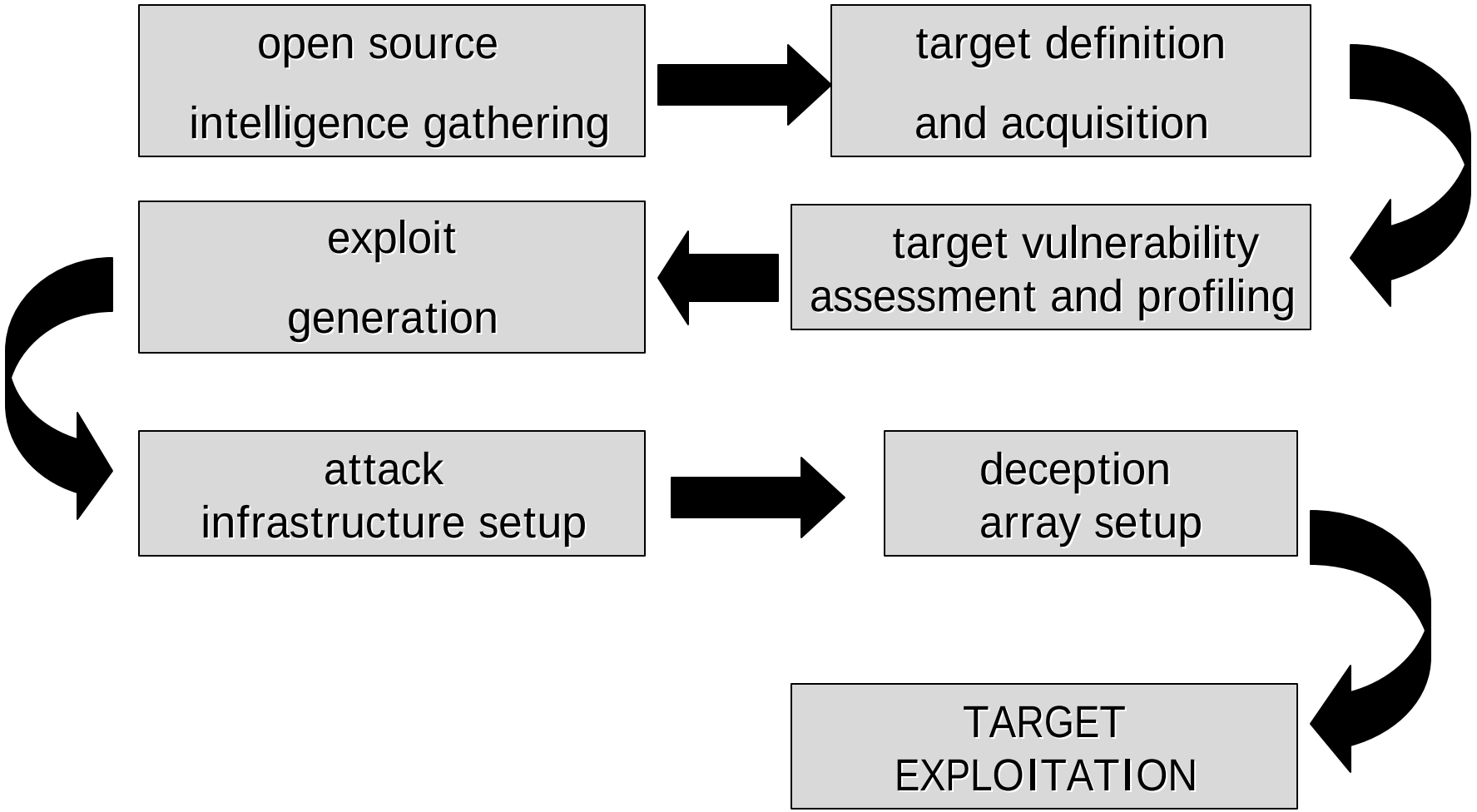
The classic Intelligence Cycle



Source: Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies

http://www.cops.usdoj.gov/mime/open.pdf?Item=1396

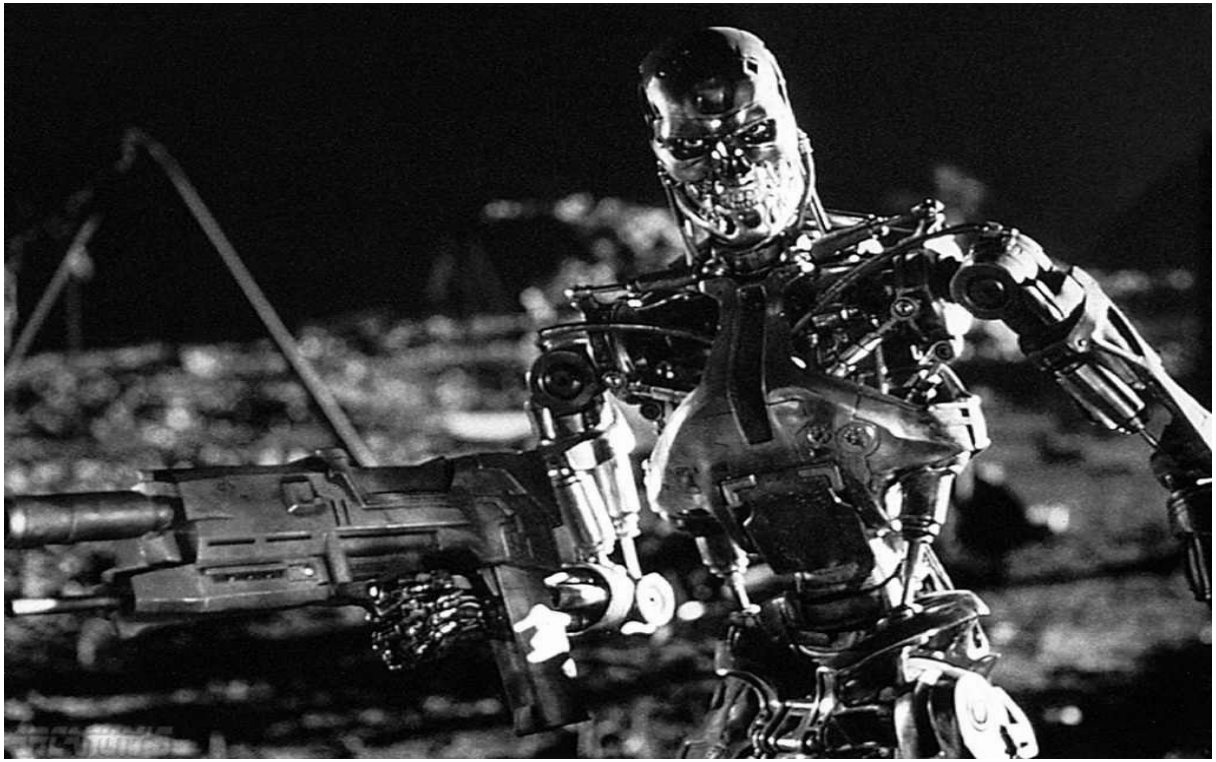
Modern espionage process flow



CASE STUDIES 1/5

Skynet 1.0

- A new application of Artificial Intelligence
- Set up of intelligent networked agents
- Underground work is in progress



CASE STUDIES 2/5

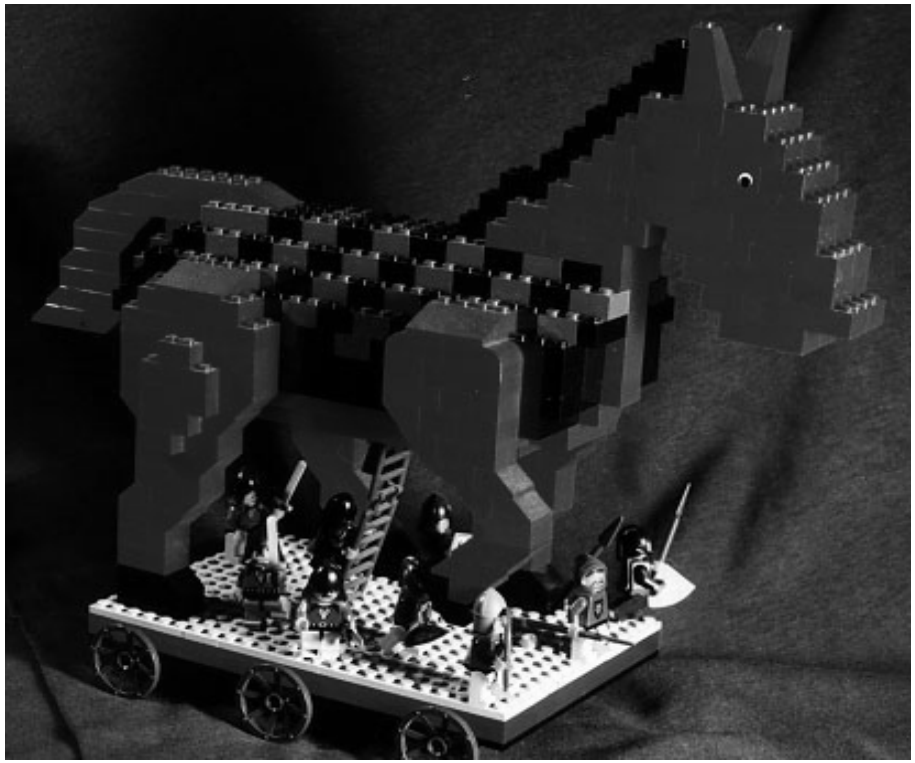
T-Mobile

- At the end of 2003 a hacker got access to the T-mobile users' accounts and stole private material from jet-set users as well as a C.I.A. document located on a T-Mobile transit e-mail account belonging to a C.I.A. agent. The hacker exploited a Bea Weblogic interface flaw.
- Even though it was not a case of corporate sponsored espionage, the T-mobile subcribers data were posted on-sale on the Internet.

CASE STUDIES 3/5

Israel Trojan Horse

- In 2005 Israel was put in a difficult situation by an industrial espionage scandal involving several corporation and dozens of people.
- Once again data were stolen using a trojan and social engineering.
- Trojan-based attacks are growing rapidly and are considered as among the most important security risks for today's corporations.



CASE STUDIES 4/5

Chinese Trojan Attacks

- Several American corporations got compromised in the last year by trojan attacks perpetrated by chinese citizens, according to the attacks' logs.
- Myfip, the trojan used for most of the attacks appeared to be one of the most sophisticated ever and one of its peculiarity was that it tried to steal also CAD/CAM files usually related to engineering design works.
- In Italy shoes factories identified successful intrusions in servers having the blueprints of new shoes models stolen even before they hit the production lines. North-West Italian shoe industry is now suffering a staggering 60% sales reduction
- According to an IBM report, in the first half of 2005, 'customized' attacks against governments, corporations and financial institutions jumped to 50 per cent.

CASE STUDIES 5/5

MILITARY INDUSTRY

THE SECOND GULF WAR

"The difference between the first Gulf War and the second one is that in the second one the US troops enjoied 42 times the bandwidth than in the first one thanks to the US Command Centers uplinks in Qatar and Kuwait"

Lt.Col.Ernest "Rock" Marcone

www.zone-h.org

the Internet thermometer

Customer: U.S. Army

Definitized Value: $14.8B (*21.2B)

Period of Performance:

May 2003 thru Dec 2011 (*2014)

***Result of recent Program restructuring**

FUTURE COMBAT SYSTEMS

FCS

One Team-The Army/Defense/Industry

OLD WAR CONCEPT

-Heavy war equipment

-Massive firepower

-Large battlefronts

-Low-tech infantry

-Manned vehicles

NEW WAR CONCEPT

-Light war equipment

-Minimal firepower

-Small battlefronts

-High-Tech infantry (jargon: families)

-Large use of intelligence

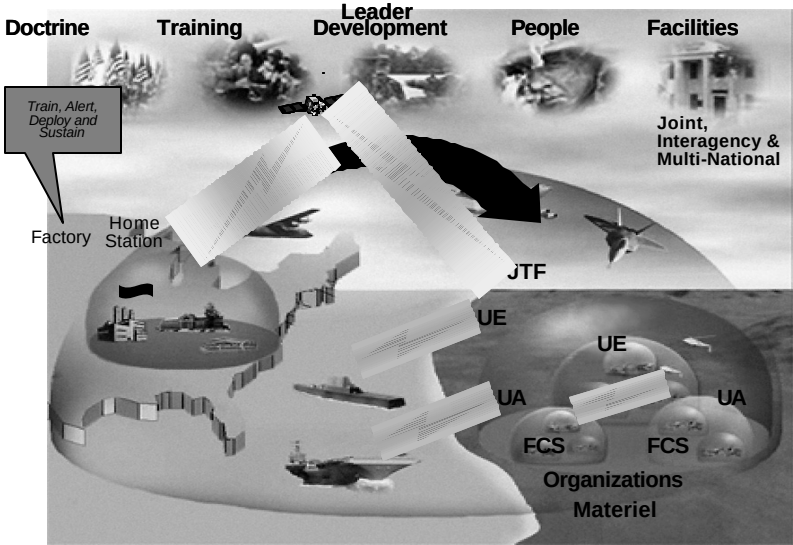
-Unmanned vehicles

The M.O.S.A.I.C. network

Warfighter Information Network-Tactical (WIN-T)

"*The WIN-T network provides command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) support capabilities that are mobile, secure, survivable, seamless, and capable of supporting multimedia tactical information systems within the warfighters' battlespace.*"

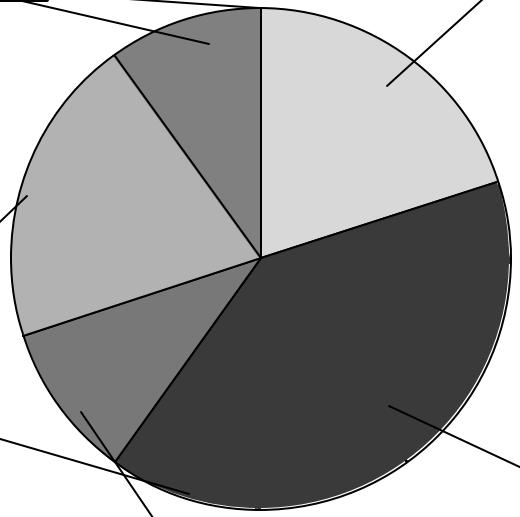
MOSAIC: Working with CECOM-RDEC, Rockwell Collins has developed IP, mobility and Quality of Service (QoS) networking capabilities as part of the MOSAIC program. MOSAIC is an ad hoc, self-routing network, with key elements being migrated into WIN-T, FCS and JTRS/WNW.



The M.O.S.A.I.C. network

- The Army Multifunctional On-the-Move Secure Adaptive Integrated Communications (MOSAIC) program addresses some of these hurdles. By 2004, it is expected to demonstrate a self-organized wireless cluster consisting of 15 to 20 nodes. The network is expected to have a 2-minute installation time and 5-minute recovery. Data transmission is between 56 Kbps and 15 Mbps, dependent upon the range between nodes, which at the extremes are from 100 kilometers (km) to 100 meters (m). However, a wireless network with the capacity for 100 Mbps transmission will not be ready until at least 2010.

F.C.S.: 31 millions lines of unaudited code



Direct/procured Information Leakage 20%

SW System Intergration 10%

Data transmission protocol 20%

Application layer exploitability 40%

HW System Integration 10%

F.C.S. main contractors

The Boeing Co., Phantom Works, Seattle, Wash.

Science Applications International Corp., McLean, Va.

TEAM FoCuS Vision CONSORTIUM, led by General Dynamics Land Systems Inc., Sterling Heights, Mich., and Raytheon Company, Plano, Texas

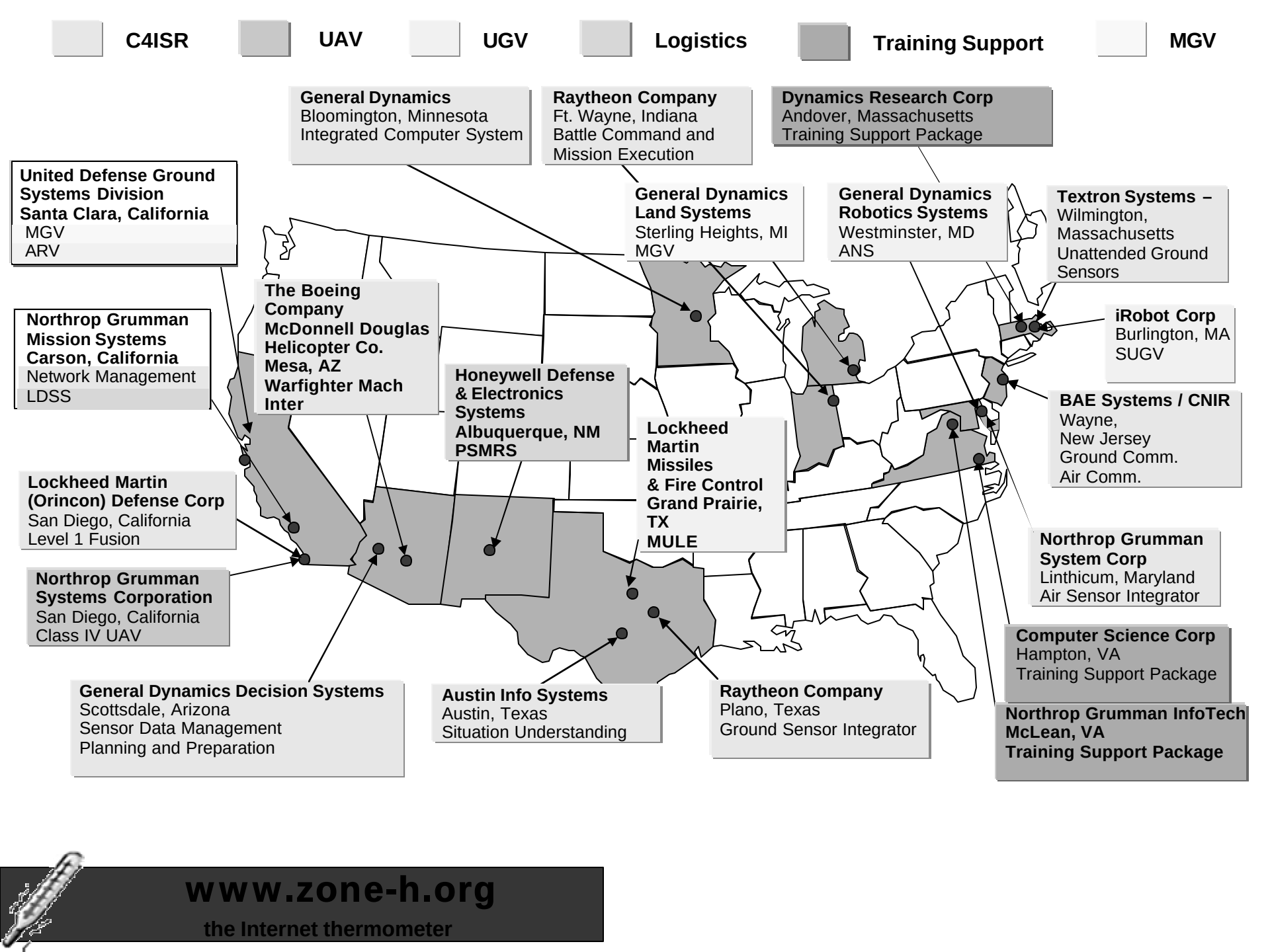
Team Gladiator (TRW Inc., Carson, Calif.; Lockheed Martin Inc., Lockheed Martin Vought Systems, Dallas, Texas; CSC/Nichols Research, Huntsville, Ala.; Carnegie Mellon Research Institute, Pittsburgh, Penn.; Battelle Memorial Institute, Columbus, Ohio; IITRI/AB Tech Group, Alexandria, Va.)

The Boeing Company - NID, WB& B, VRI, Signature Research, Rockwell Science Center, NIST, Krauss- Maffei Wegmann (KMW)

Full Spectrum Team - SAIC, United Defense, SPL, VRI, Omnitech Robotics, LMI, SRI International, ITT Industries, CEM, Northrop Grumman

Focus Vision Consortium - General Dynamics Land Systems, SRI International, Halliburton Company, Coates & Jarratt, Inc., Raytheon, Honeywell, Electrical & Computer Engineering, Maxwell Technologies, Carnegie Mellon, WB& B, Sensis Corporation, BAE Systems, Aurora, Sensor.com

Gladiator Consortium - IITRI AB Tech Group, Carnegie Mellon, Lockheed Martin, CSC, Battelle, TRW



Legal Company Name	City	State
Defense Service	Sterling Heights	MI
Defense Systems Integration	Highland Park	IL
Foster-Miller, Inc.	Waltham	MA
General Dynamics	Bloomington	MN
General Dynamics	Mountain View	CA
General Dynamics	Taunton	MA
General Dynamics Decision Systems Inc.	Scottsdale	AZ
General Dynamics Land Systems Inc.	Sterling Heights	MI
General Dynamics Robotic Systems	Westminster	MD
General Motors Defense	Goleta	CA
Goodrich EO	Danbury	CT
GS Engineering, Inc.	Handcock	MI
Hamilton Sundstrand Corporation	Windsor Locks	CT
Harris	Melbourne	FL
Honeywell	Clearwater	FL
Honeywell International	Torrance	CA
Honeywell International, Inc.	Albuquerque	NM
Honeywell International, Inc.	Minneapolis	MN
IAC	Poway	CA
IBM	Bethesda	MD
Impact	Rochester	NY
Innovative Survivability Technologies	Goleta	CA
Intelligent Automation, Inc.	Rockville	MD
iRobot Corporation	Somerville	MA
Isothermal Systems Research	Clarkston	WA
ITT	FT Wayne	IN
ITTRI	Annapolis	MD
Kaman	Hudson	MA
Krauss-Maffei Wegmann GmbH & Co. KG	Munich	Bavaria
LexCarb LLC	Lexington	KY
Mathworks	Natick	MA
Mesa Associates, Inc.	Madison	AL
Metadapt	San Francisco	CA
NAI Labs	Glenwood	MD
NATC	Carson City	NV

Legal Company Name	City	State
National Institute of Standards and Technology	Gaithersburg	MD
Natural Selection, Inc.	La Jolla	CA
Navigator Development	Enterprise	AL
NDI	Tacoma	WA
Northrop Grumman Electronic Systems	Linthicum Heights	MD
Northrop Grumman PRB Systems, Inc.	Hollywood	MD
Northrop Grumman Systems Corporation	San Diego	CA
Northrop-Grumman	Woodland Hills	CA
Orincon Corporation	San Diego	CA
Parametric Technology Corporation	Belllevue	WA
Pathfinder Systems, Inc.	Lakewood	CO
PEI Electronics	Huntsville	AL
Physics Math & Computers Inc	Socorro	NM
PreMag	Albany	NY
Rational	Redmond	WA
Raytheon Company	Plano	TX
Redzone Robotics	West Homested	PA
Remotec, Inc.	Oak Ridge	TN
Ricardo	Belleville	MI
Robotic Technologies	Potomac	MD
Rockwell Collins, Inc.	Cedar Rapids	IA
Rockwell Scientific	Thousand Oaks	CA
Science Applications International Corporation	Mclean	VA
Science Applications International Corporation	San Diego	CA
Scientific Monitoring	Tempe	AZ

Legal Company Name	City	State
SeQual	San Diego	CA
Signature	Calumet	MI
Smiths Aerospace, Inc.	Grand Rapids	MI
SRI International	Menlo Park	CA
The Charles Stark Draper Laboratory, Inc.	Cambridge	MA
Toyon	Goleta	CA
TRW Inc.	San Diego	CA
TRW Systems	Carson	CA
United Defense L.P.	Santa Clara	CA
Univ of Texas Austin	Austin	TX
Virginia Polytechnic Inst & St. Univ	Blackburg	VA
Virtual Technology Corporation	Alexandria	VA
Vista Controls	Santa Clarita	CA
VT Kinetics	Hunstville	AL

Legal Company Name	City	State
3D Research Corporation	Huntsville	AL
3-TEX	Cary	NC
AAI Corporation	Hunt Valley	MD
Agile	Rancho Cucamonga	CA
Allied Aerospace Industries Inc.	San Diego	CA
Applied Data Trends, Inc.	Huntsville	AL
Applied Systems Intelligence, Inc.	Roswell	GA
Architecture Technology Corporation	Eden Prairie	MN
Army - Aberdeen Test Center	Aberdeen	MD
Army - AMRDEC	Redstone Arsenal	AL
Army - CECOM	Ft Monmouth	NJ
Army - Research Center	Vicksburg	MS
Aspen - Systems	Marlborough	MA
ATAK	San Jose	CA
BAE	Nashua	NH
BAE SYSTEMS	Merrimack	NH
BAE Systems	Wayne	NJ
BAE Systems Information Systems Sector	Reston	VA
Ball Aerospace & Tecnologies Corp.	Fairborn	OH
Barrday	Cambridge	Canada
BBNT Solutions LLC	Cambridge	MA
BBNT Solutions LLC	Arlington	VA
Carnegie Mellon University	Pittsburgh	PA
CECOM CRADA	Ft Monmouth	NJ
CHI	Lower Gwynedd	PA
Construx	Bellevue	WA
Cougaar	Fairfax	VA
CSI	Ft. Wayne	IN
CyberNet	Ann Arbor	MI

BIA Number	BIA Description	Legal Company Name	City	State
14300.1	- Test & Evaluation Resources Requirements Development	3D Research Corporation	Huntsville	AL
15200	- High Altitude / Long Endurance (HALE) Unmanned Air Vehicle Platform Integration REV: 8/20/02	TRW Inc.	San Diego	CA
15250	- Organic Air Vehicle (OAV) Platform Integration REV: 8/20/02	Allied Aerospace Industries Inc.	San Diego	CA
15260	- Tactical Unmanned Air Vehicle (TUAV) Platform Integration REV: 8/20/02	Northrop Grumman Systems Corporation	San Diego	CA
15270	- Small Unmanned Air Vehicle (SUAV) Platform Integration REV: 8/20/02	Allied Aerospace Industries Inc.	San Diego	CA
15350.2	- Autonomous Navigation Subsystem	Carnegie Mellon University	Pittsburgh	PA
		National Institute of Standards and Technology	Gaithersburg	MD
		The Charles Stark Draper Laboratory, Inc.	Cambridge	MA
15360	- Soldier UGV	Foster-Miller, Inc.	Waltham	MA
		iRobot Corporation	Somerville	MA
		Mesa Associates, Inc.	Madison	AL
15370	- Mule UGV (1 Ton)	General Dynamics Robotic Systems	Westminster	MD
		iRobot Corporation	Somerville	MA
15711	- ECS/TMS/NBC Subsystem	Hamilton Sundstrand Corporation	Windsor Locks	CT
		Honeywell International	Torrance	CA
15712	- Survivability System	BAE SYSTEMS	Merrimack	NH
		General Motors Defense	Goleta	CA
		Innovative Survivability Technologies	Goleta	CA
15714	- Vehicle Electronics (Vetronics) REV: 8/23/02	Raytheon Company	Plano	TX
15716	- Warfighter Machine Interface -Common Crew Station & WMI Software Layer	General Dynamics Decision Systems Inc.	Scottsdale	AZ
		General Dynamics Robotic Systems	Westminster	MD
		Honeywell International, Inc.	Albuquerque	NM
16123	- Computer Systems, Networks and Data Storage	General Dynamics	Bloomington	MN
		Rockwell Collins, Inc.	Cedar Rapids	IA

BIA Number	BIA Description	Legal Company Name	City	State
16200.1	- Army Airspace Command and Control (A2C2) services	Northrop Grumman PRB Systems, Inc.	Hollywood	MD
16200.2	- Course of Action (COA) and Intelligence Preparation of the Battlefield (IPB) services	BBNT Solutions LLC	Cambridge	MA
16200.3	- Command and Control Mission Execution and Battle Management Subsystem	Raytheon Company	Plano	TX
		Applied Systems Intelligence, Inc.	Roswell	GA
		General Dynamics Decision Systems Inc.	Scottsdale	AZ
16200.4	- Command and Control Mission Planning and Preparation Subsystem	Honeywell International, Inc.	Minneapolis	MN
		General Dynamics Decision Systems Inc.	Scottsdale	AZ
16200.5	- Command and Control Situation Understanding Subsystem	Applied Data Trends, Inc.	Huntsville	AL
		BBNT Solutions LLC	Arlington	VA
16200.6	- Command and Control Sustainment Subsystem	Ball Aerospace & Tecnologies Corp. *	Fairborn	OH
		TRW Systems *	Carson	CA
16320	- Modeling & Simulation	Architecture Technology Corporation	Eden Prairie	MN
		BBNT Solutions LLC	Cambridge	MA
		Raytheon Company	Plano	TX
16500	- Battlefield Identification	Raytheon Company	Plano	TX
		Northrop Grumman Electronic Systems	Linthicum Heights	MD
17000.4	- Switchable Vision Block	Pathfinder Systems, Inc.	Lakewood	CO
17000.5	- Leader Training	General Dynamics Decision Systems Inc.	Scottsdale	AZ
		Virtual Technology Corporation	Alexandria	VA
18300	- Supportability	Natural Selection, Inc.	La Jolla	CA

"Best of Industry Team"

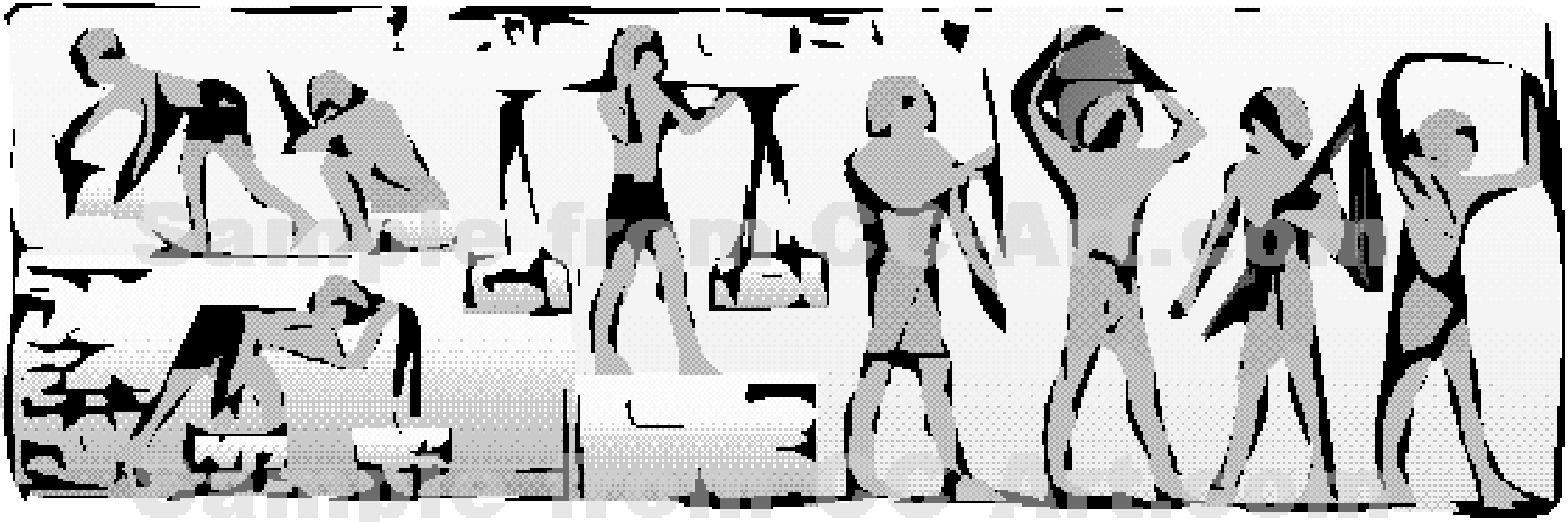
FUTURE COMBAT SYSTEMS
FCS
One Team – The Army/Defense/Industry

Company	Work Description	Contact	E-Mail Address	Phone Number
Honeywell Defense & Space Electronic Systems	Platform Soldier Mission Readiness System (PS-MRS)	Mike Cuff	mike.cuff@honeywell.com	(505) 828-5930
iRobot Corporation	Small Unmanned Ground Vehicle (SUGV)	Knob Moses	rmoses@irobot.com	(571) 331-4644
Lockheed Martin Missiles and Fire Control	Multifunction Utility/Logistics and Equipment Vehicle (MULE)	Don Nimblett	donald.nimblett@lmco.com	(972) 603-9219
Lockheed Martin, Orincon	ISR Sensor Fusion, Level 1	Kevin Stewart	kevin.stewart@lmco.com	(703) 351-4440
Northrop Grumman	Air Sensor Integrator, Class IV UAV Logistics Decision Support Systems, Network Management, Training Support	Kief Tackaberry	Kief.tackaberry@ngc.com	(703) 875-8342
Raytheon Network Centric Systems	Battle Command and Mission Execution, Ground Sensor Integrator	Darrell Gotcher	dgotcher@raytheon.com	(972) 344-1893
Textron Systems	Unattended Ground Sensors, Tactical and Urban Sensors	Dean Risseeuw	driseeuw@systems.textron.com	(978) 657-2324
United Defense, L.P., All Divisions	Armed Robotic Vehicle (ARV), Manned Ground Vehicles	David A. Napoliello	david.napoliello@udlp.com	(703) 312-6132

Honeywell Raytheon NORTHROP GRUMMAN TEXTRON LOCKHEED MARTIN

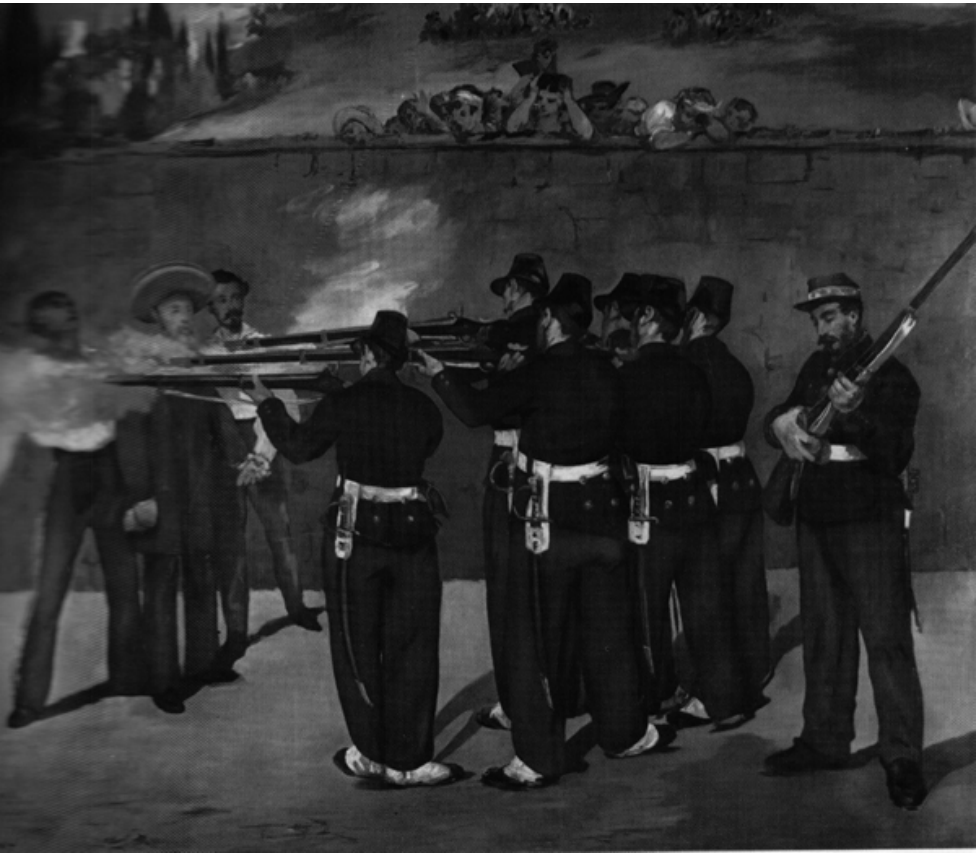
PREVENTION AND DEFENSE

PREVENTION AND DEFENSE



BEST PRACTICE

How to get rid of your IT staff



www.zone-h.org
the Internet thermometer

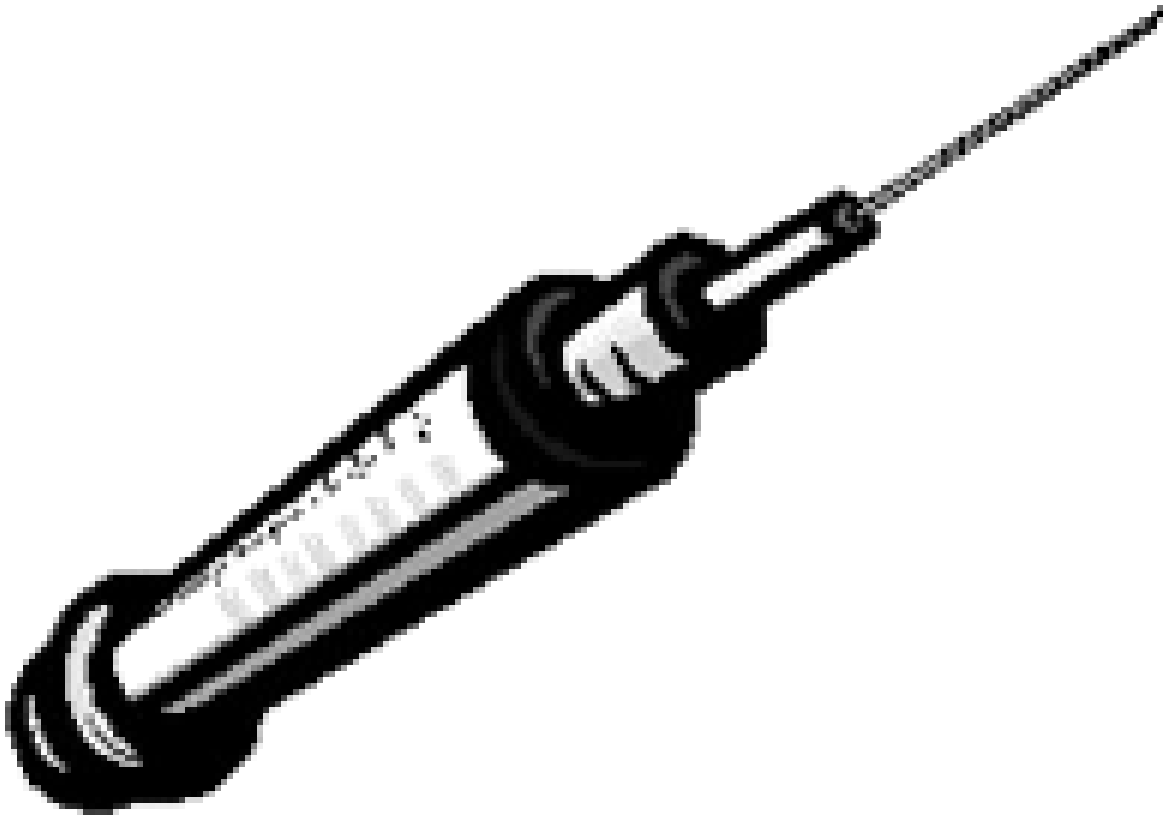
...but if you want to be sure...

www.zone-h.org

the Internet thermometer

INJECTED INTERCEPTION

•allows to trace the IP address of a target and gain direct access to all data contained on the computer no matter what is the means of data transport (i.e. physical or digital)



Tools

?

Questions?

English

¿Preguntas?

Spanish

?? ??

Arabic

Domande?

Italian

??????? ?

Russian

???t?se??

Greek

tupoQghachmey

Klingon

? ?

Japanese