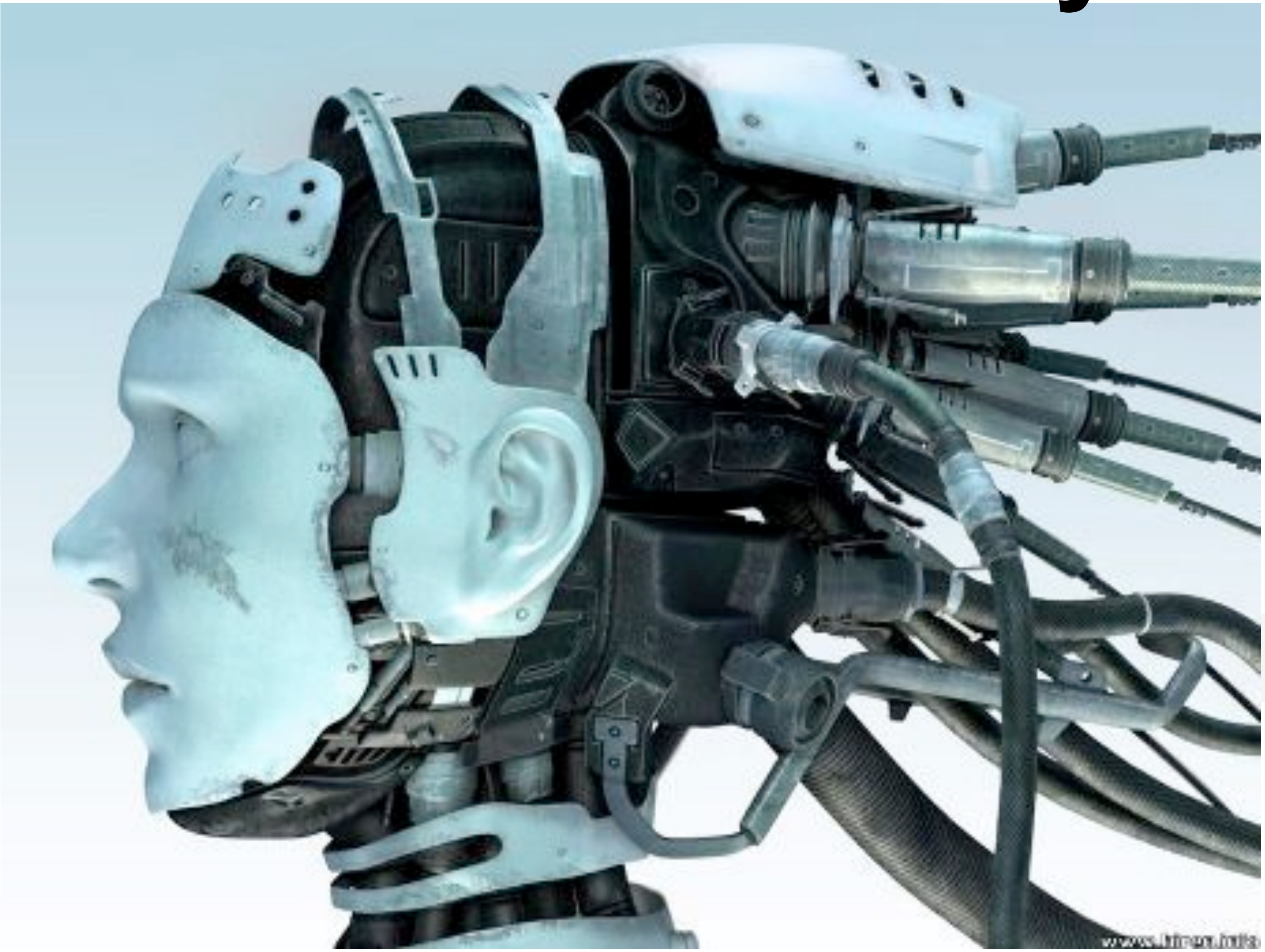
Roberto Preatoni

zone-h
unrestricted information

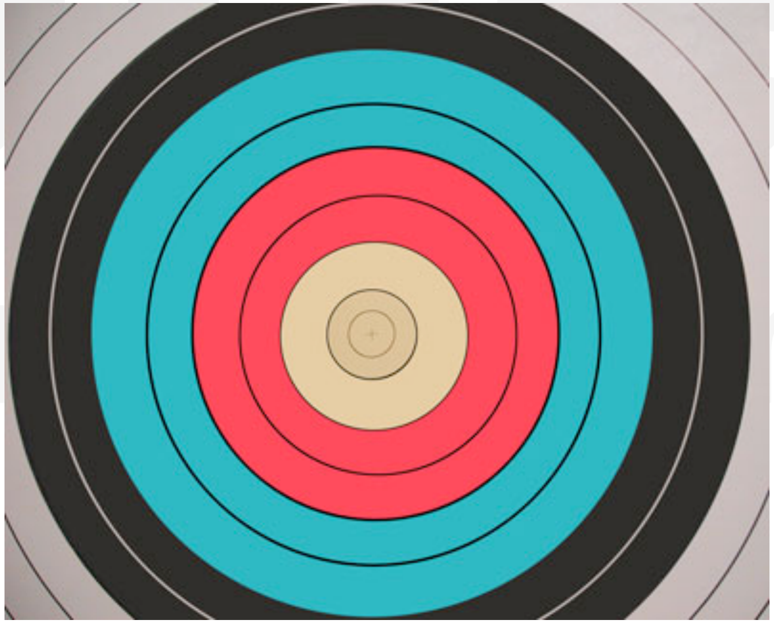
Modern Threats and Cyber War Lessons Learned? Maybe Not



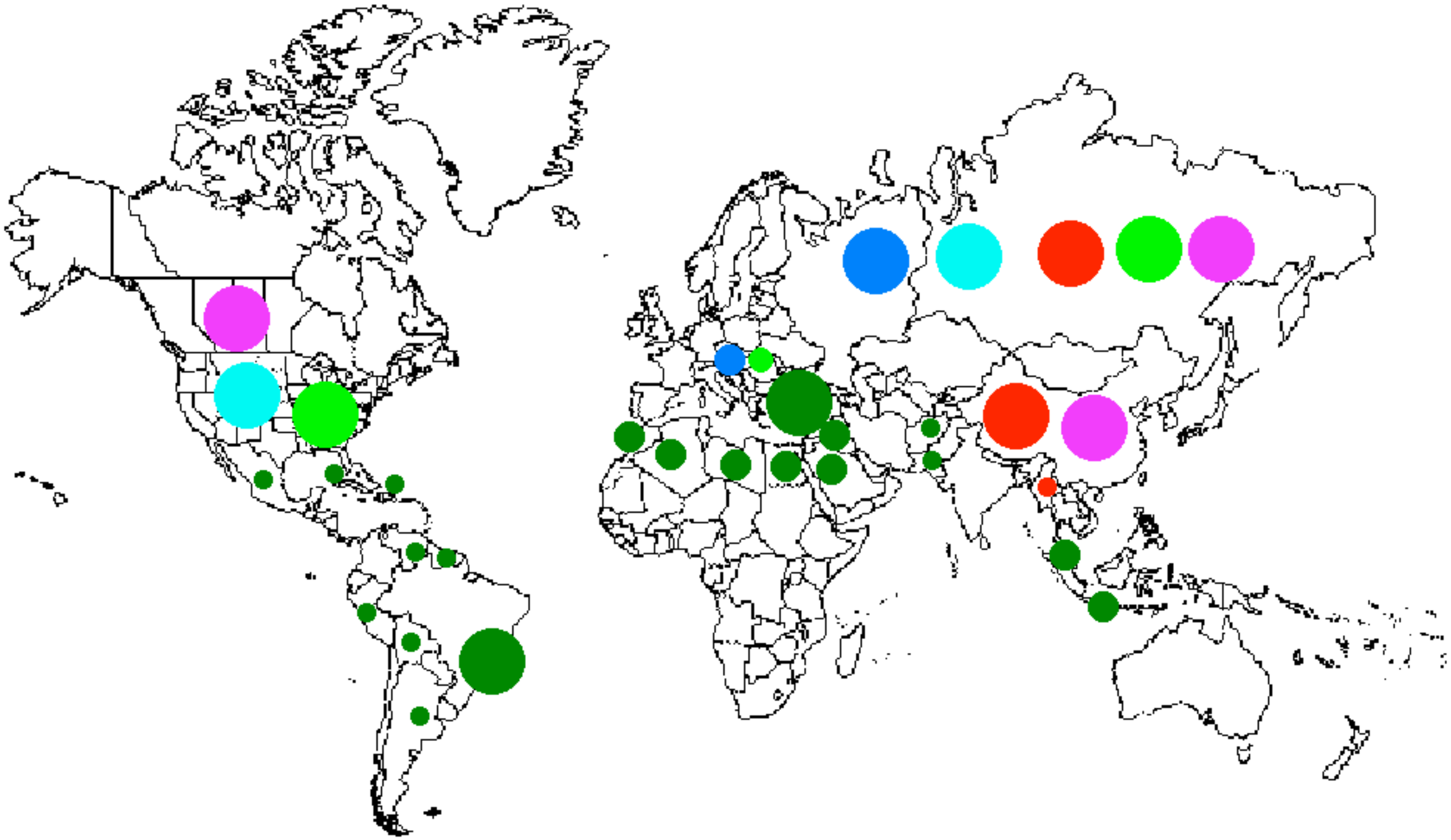
www.hiren.info

Am I a target? Is my company a target? Is my government a target?

Are the countermeasures put in place causing me more harm than good?



World Cybercrime Map

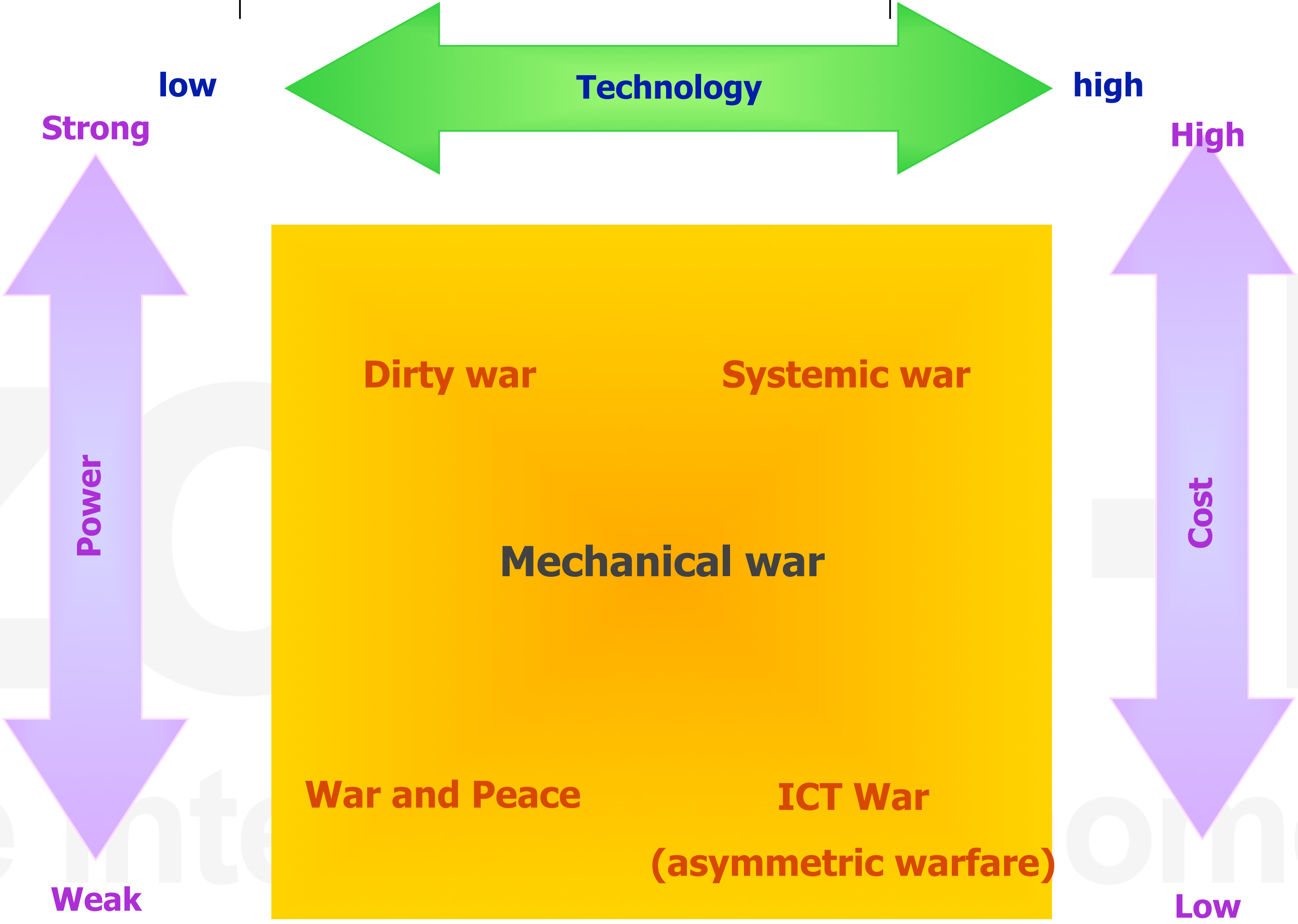


- ● carding
- ● spamming
- ● phishing
- ● political/industrial espionage
- ● Ddos/virus extortion
- ● Cyber Politics

OK, I KNOW’EM ALL, BUT…

WHAT’S NEXT?

Future conflicts dimensions



“It’s the best strategy in an asymmetric conflict”

- Distributed attacks, high anonimity
- Possibility to use the same enemy’s infrastructures
- Low cost of technology implementation and R&D
- Wide range of critical infrastructures to be attacked
- Possibility to carry out unconventional activities
- Direct contact with the enemy’s command and control center at the highest ranks

INTERNET + ASYMMETRIC CONFLICT MEANS:

In the traditional wars to fight a country it takes a country

In asymmetric Internet based conflicts, to fight a country it can take just a few or just **one** motivated and even **not so much** skilled hacker.

New Cyber Crime Fields

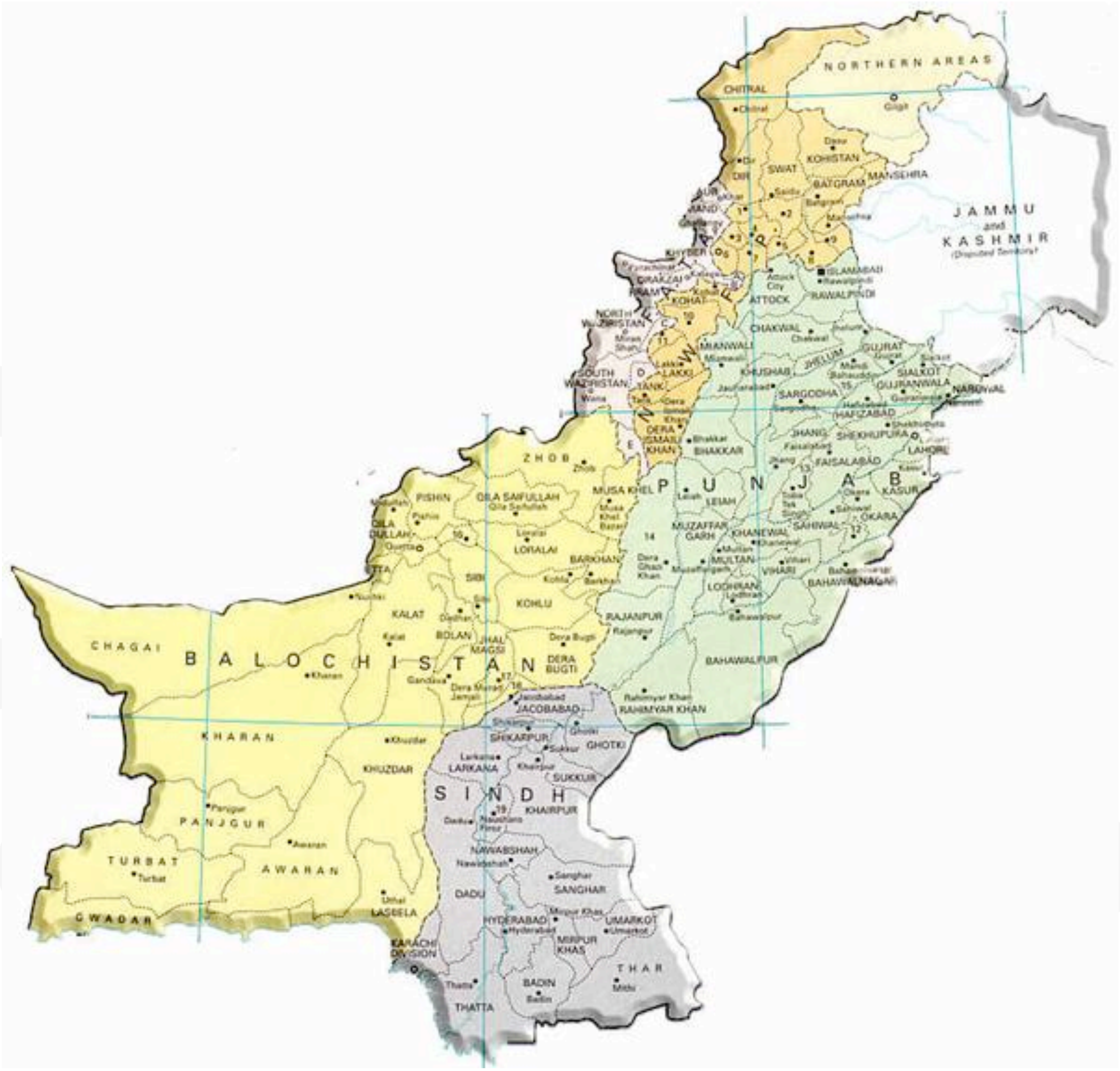
- Cyber Politics
- Cyber industrial and private espionage

CYBER Politics

- 2001 Pakistan vs West
- 2002 USA vs China
- 2004 South America vs USA
- 2007 Arab countries vs Denmark
- 2007 Russia vs Estonia
- 2008 Russia vs Georgia

2001 Pakistan vs West

zone-h
unrestricted information



2002 United States vs China

2004 South America Vs United States

In year 2004, a large number of Brasilian hacker crews united their efforts with other South American hackers in launching hacking campaigns against USA in protest to the Bushist imperialistic regime.

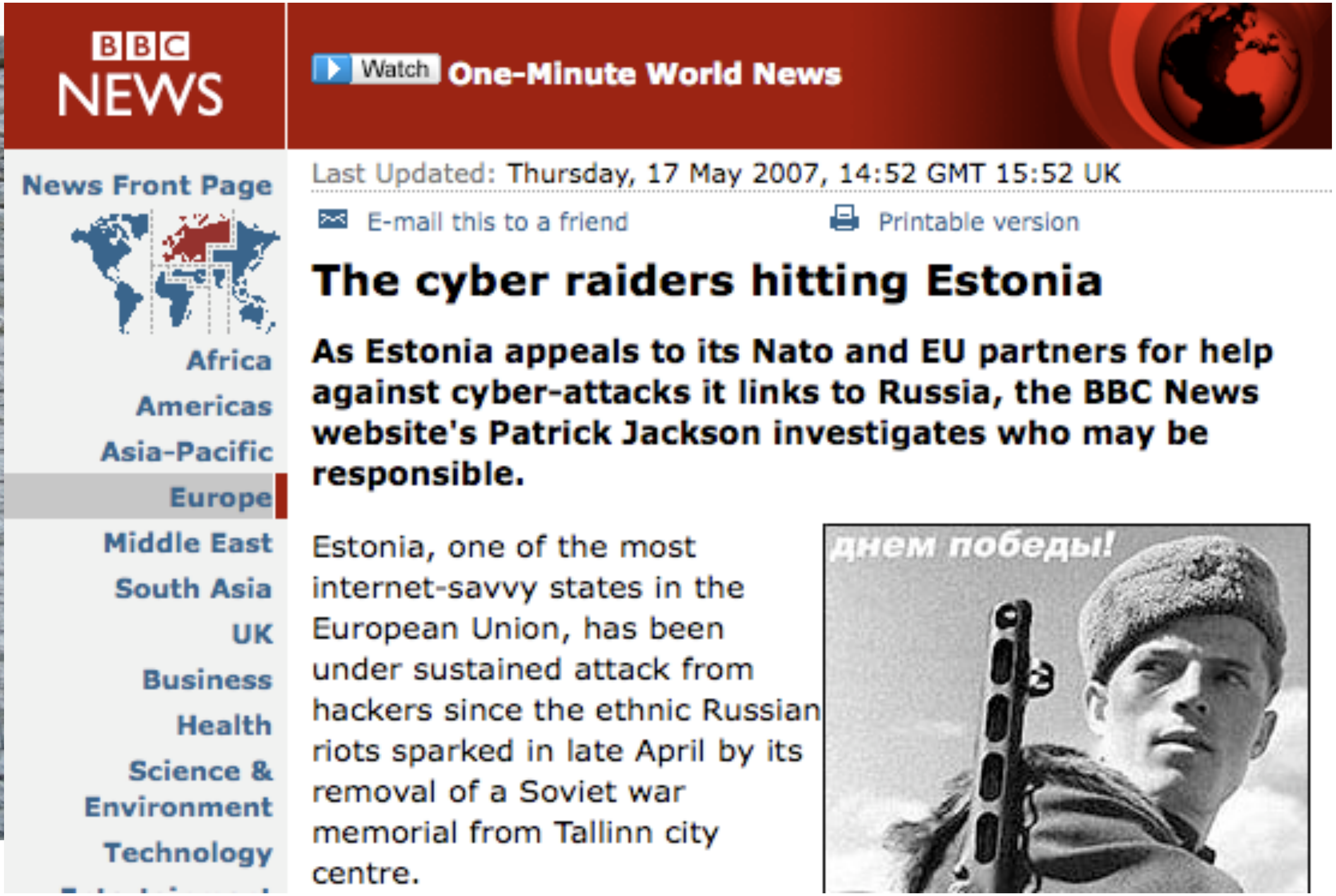
For the first time ever, hackers from Chile, Venezuela and even Cuba, participated in a joint cyber-war against one of the major political player of the planet, gaining factual support even from Pakistani hackers.

2007 Arab countries vs Denmark

In year 2007 several hackers from Arab countries launched coordinated defacing and Ddos attacks against Nordic countries particularly against Denmark in protest to the publication of some cartoons portraying Prophet Mohamed.

The Danish economy suffered some losses and it took a couple of weeks to re-gain the normal Internet operability.

2007 Russia vs Estonia



Last Updated: Thursday, 17 May 2007, 14:52 GMT 15:52 UK

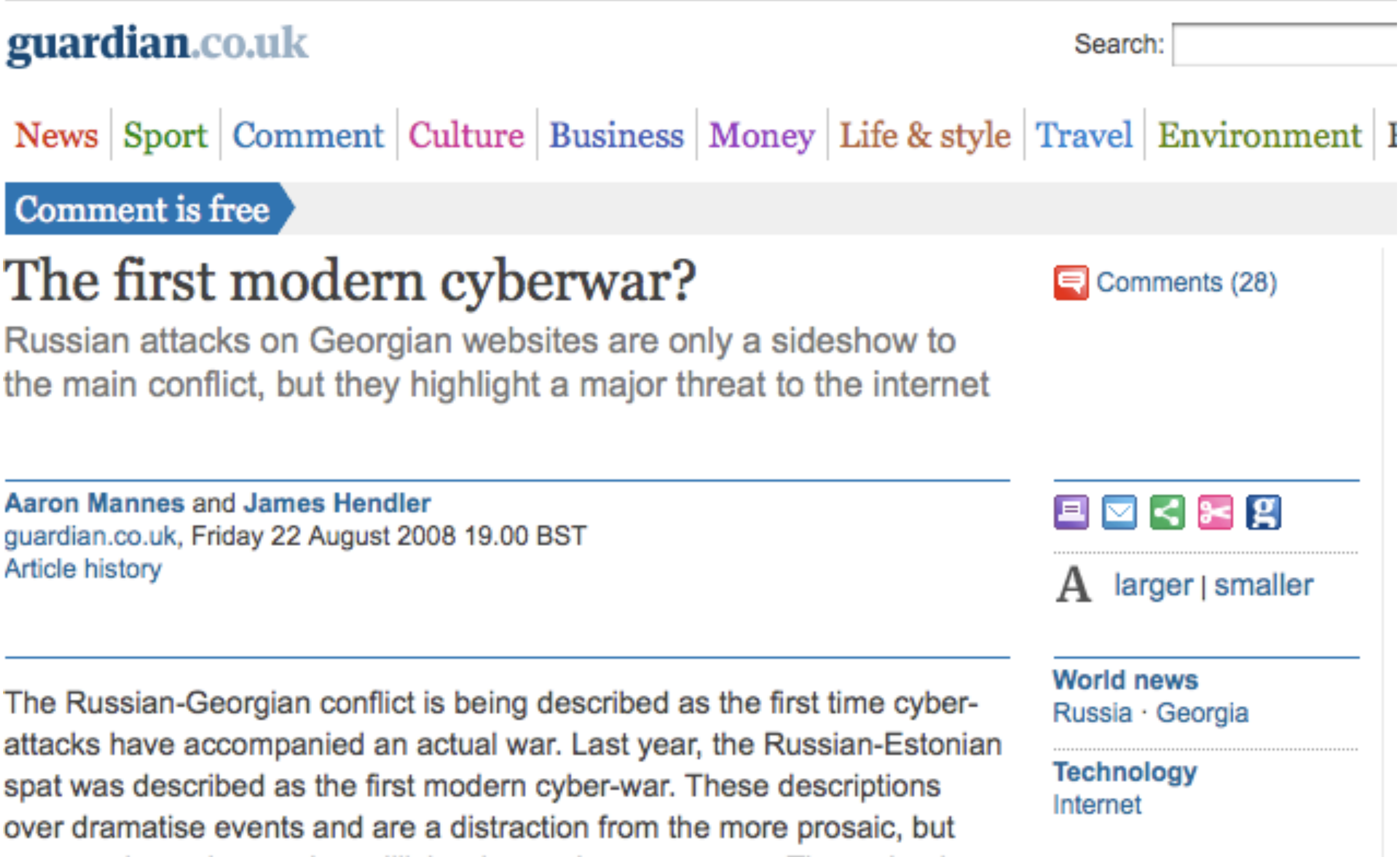
The cyber raiders hitting Estonia

As Estonia appeals to its Nato and EU partners for help against cyber-attacks it links to Russia, the BBC News website's Patrick Jackson investigates who may be responsible.

Estonia, one of the most internet-savvy states in the European Union, has been under sustained attack from hackers since the ethnic Russian riots sparked in late April by its removal of a Soviet war memorial from Tallinn city centre.

2008 Russia vs Georgia

zone-h
unrestricted information


guardian.co.uk
Search:
News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment
Comment is free
Comments (28)
A larger | smaller

The first modern cyberwar?

Russian attacks on Georgian websites are only a sideshow to the main conflict, but they highlight a major threat to the internet

Aaron Mannes and James Hendler
guardian.co.uk, Friday 22 August 2008 19.00 BST
Article history

World news
Russia · Georgia

Technology
Internet

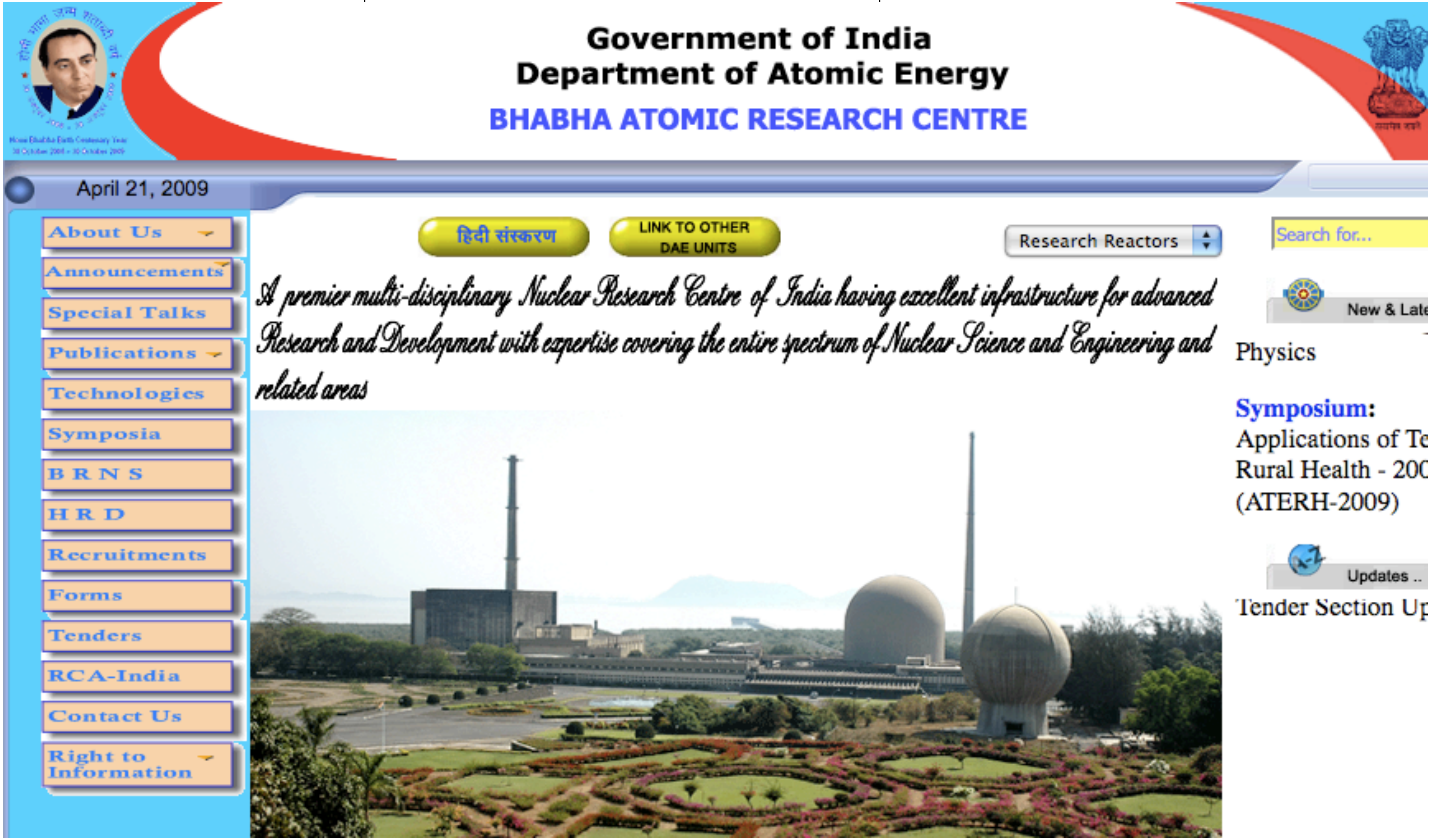
The Russian-Georgian conflict is being described as the first time cyber-attacks have accompanied an actual war. Last year, the Russian-Estonian spat was described as the first modern cyber-war. These descriptions over dramatise events and are a distraction from the more prosaic, but

CYBER Espionage

- 2001 Pakistan vs India
- 2005 China vs EU (political)
- 2005 China vs Italy (industrial)
- 2006 Russia vs USA (militar)
- 2008 China vs rest of the world
- 2009 China vs USA (preemptive war?)

2001 Pakistan vs India

zone-h
unrestricted information



Government of India
Department of Atomic Energy
BHABHA ATOMIC RESEARCH CENTRE

April 21, 2009

A premier multi-disciplinary Nuclear Research Centre of India having excellent infrastructure for advanced Research and Development with expertise covering the entire spectrum of Nuclear Science and Engineering and related areas

Physics

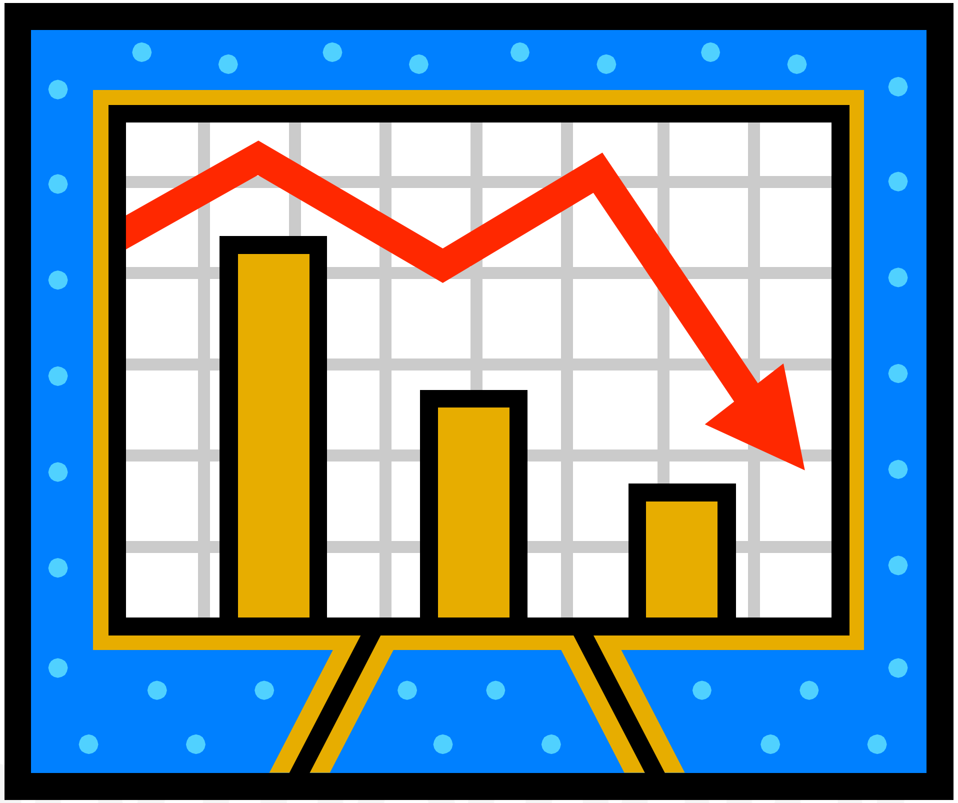
Symposium: Applications of Te
Rural Health - 200
(ATERH-2009)

Tender Section Up

2005 China vs European Union

2005 China vs Italy

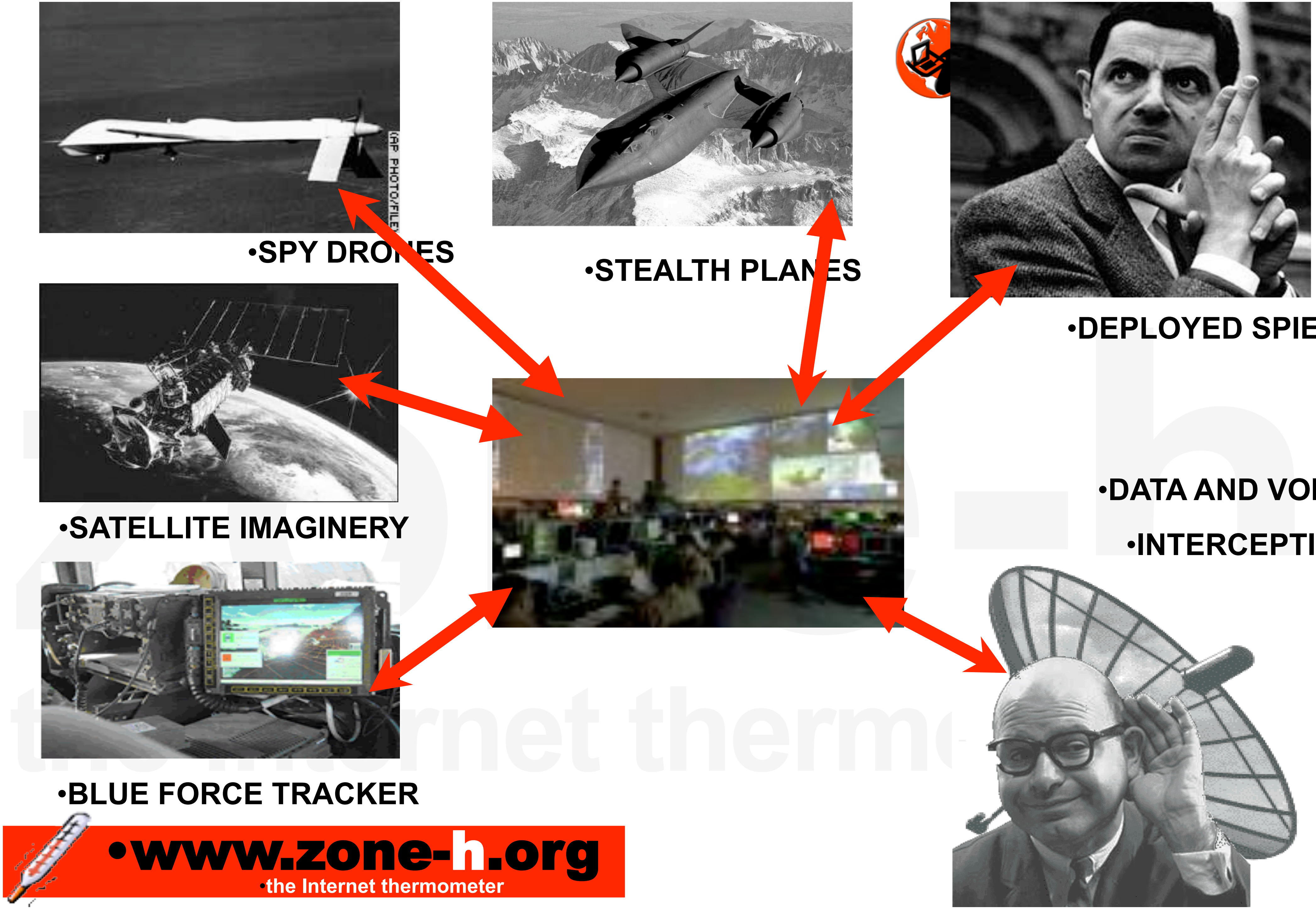
In year 2005 China launched an extensive cyber espionage campaign against Italian shoe factories and fashion houses causing a dramatic loss to the industry income.



•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

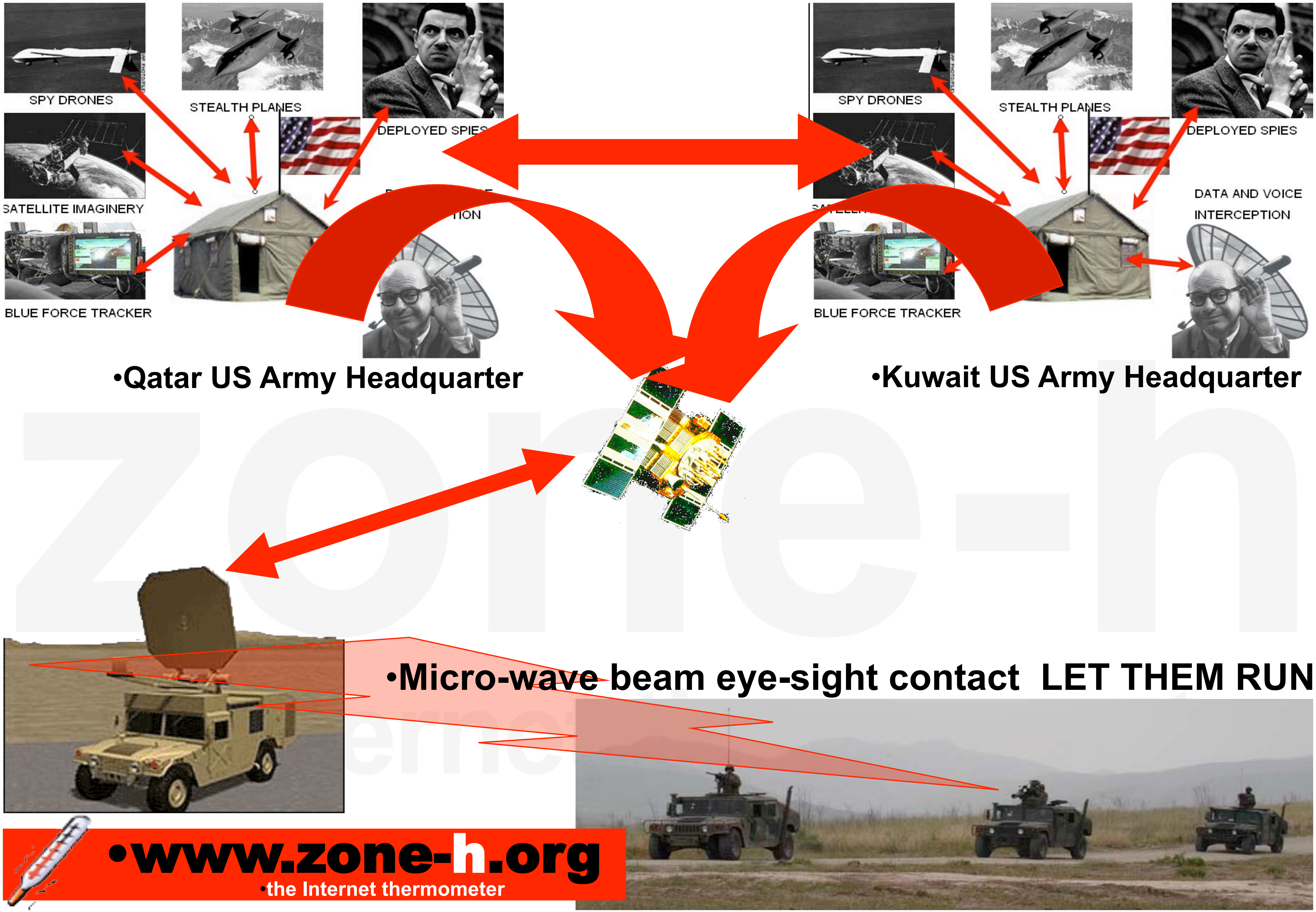


- SPY DRONES
- STEALTH PLANES
- DEPLOYED SPIES
- SATELLITE IMAGINERY
- DATA AND VOICE
- INTERCEPTION
- BLUE FORCE TRACKER

- WAS IT WORKING ?

"Hell, NO!"

"We had to stop the Humvees to re-gain connectivity and the tactical downloads took even up to 12 hours …"



- Qatar US Army Headquarter

- Kuwait US Army Headquarter

- Micro-wave beam eye-sight contact LET THEM RUN!

- www.zone-h.org

- the Internet thermometer

- *“The tactical systems were downloading nothing most of the time and when they were downloading they downloaded irrealistic data”*

- *“The system was so slow in distributing the intelligence that we knew about the enemy presence only when it was in front of us and shooting”*

- (too much of intelligence = no intelligence)

BFT + Email (!) tactical coordination

- usa@war

FUTURE COMBAT SYSTEMS • A DARPA/ARMY PROGRAM •

DARPA

FCS

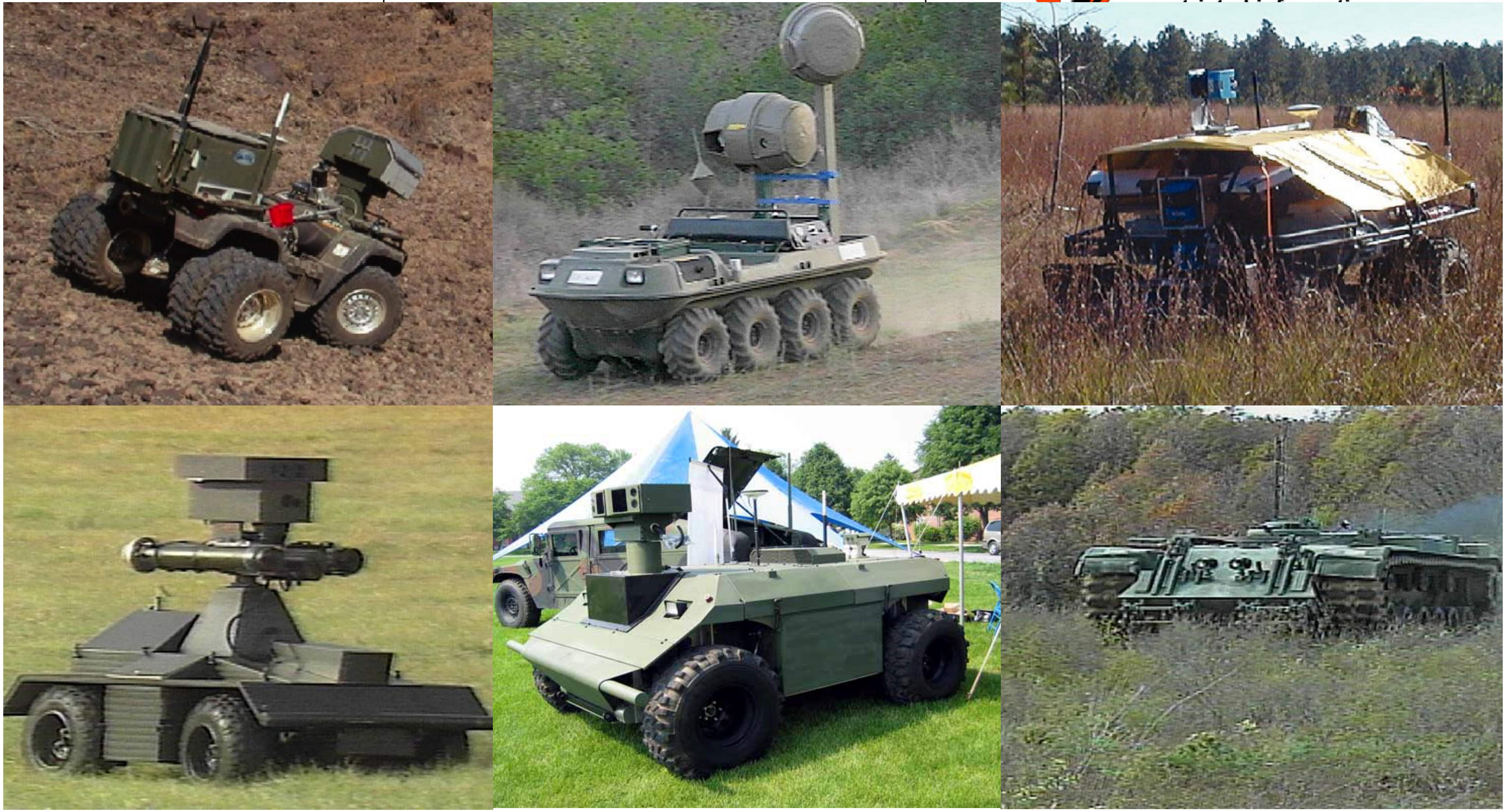
- **Customer:** U.S. Army
- **Definitized Value:** $14.8B (*21.2B)
- **Period of Performance:**
- May 2003 thru Dec 2011 (*2014)
- *Result of recent Program restructuring

FUTURE COMBAT SYSTEMS

FCS

One Team-The Army/Defense/Industry

F.C.S. unmanned vehicles

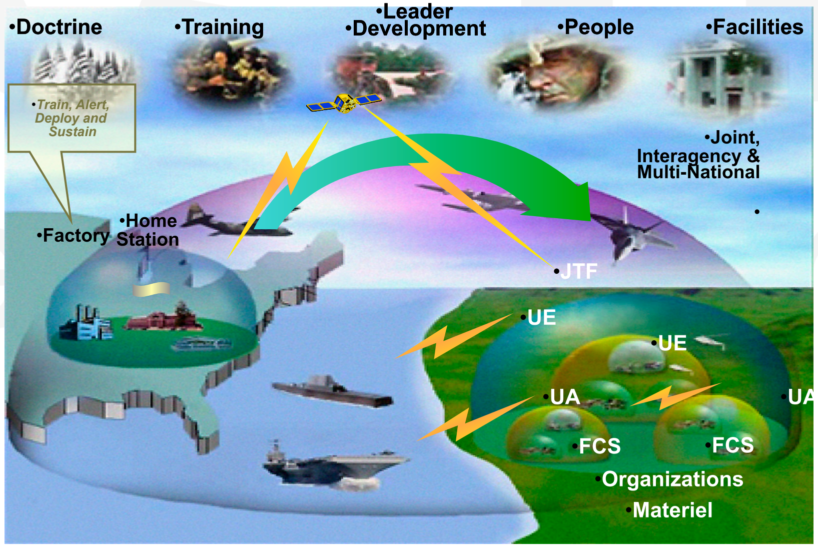


Warfighter Information Network-Tactical (WIN-T)

- *"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 Future Force

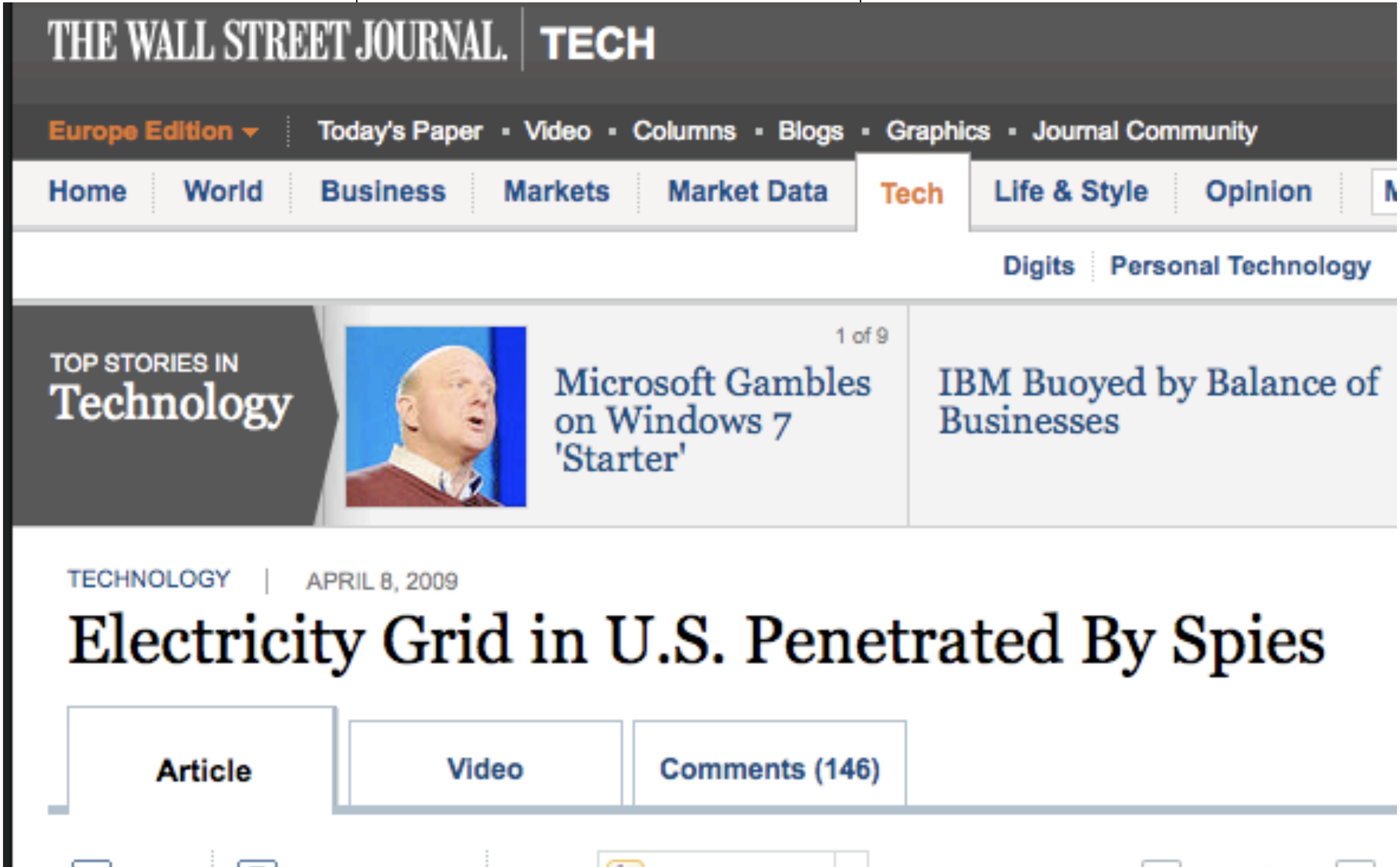


2008 China vs Rest of the world

In year 2008 most of the countries reportedly suffered from cyber-espionage attacks originating from within the Chinese territory.

Was it the demonstration that China was fearlessly attacking the rest of the world or just a convenient way to hide traditional western originated espionage activity behind Chinese proxies?

2009 China vs USA

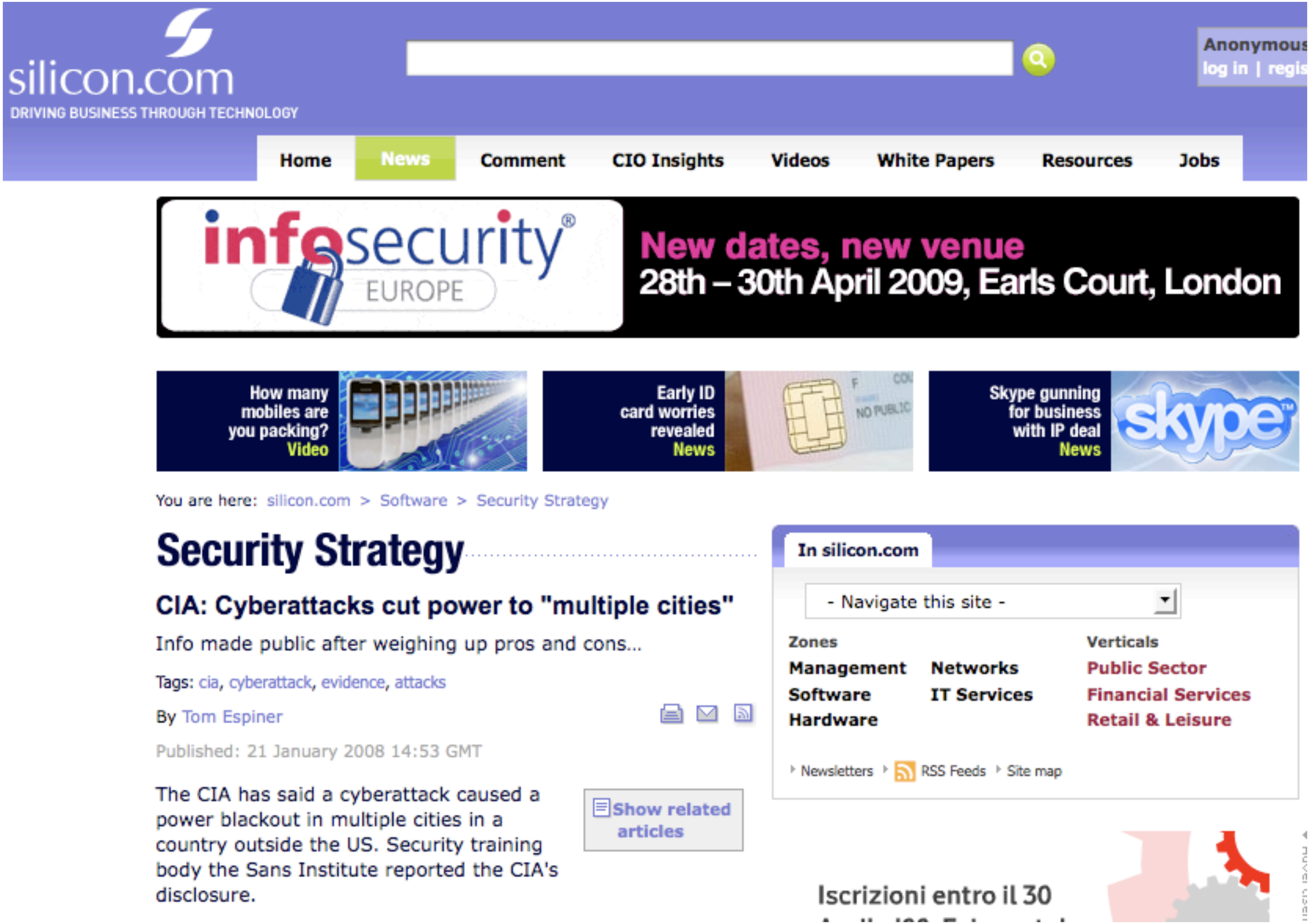


Microsoft Gambles on Windows 7 'Starter'

IBM Buoyed by Balance of Businesses

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies


silicon.com
DRIVING BUSINESS THROUGH TECHNOLOGY
Anonymous
log in | regis
Home
News
Comment
CIO Insights
Videos
White Papers
Resources
Jobs

How many mobiles are you packing? Video
Early ID card worries revealed News
Skype gunning for business with IP deal News

You are here: silicon.com > Software > Security Strategy

Security Strategy

CIA: Cyberattacks cut power to "multiple cities"

Info made public after weighing up pros and cons...

Tags: cia, cyberattack, evidence, attacks

By Tom Espiner

Published: 21 January 2008 14:53 GMT

The CIA has said a cyberattack caused a power blackout in multiple cities in a country outside the US. Security training body the Sans Institute reported the CIA's disclosure.

Lessons not learned

- Germany (parliament law against security tools)
- France (Sarkozy doctrine)
- Italy (Pisanu decree)
- Sweden (The Pirate Bay case)
- All countries (blindness toward multi layered threats)
- All countries (blindness toward excessive data retention)

Germany

Before year 2007, Germany was the only country in the world which parliament was successfully communicating with the hacker community, seeking for advices and help on general IT law matters.

In Year 2007 the German parliament issued a law to ban the possession of penetration testing tools, even though the whole German hacker community tried to explain that it was a useless counter-measure against cybercrime

2008 France

In year 2008, the French prime minister Sarkozy started to lobby a law toward the European Parliament under which each citizen committing a cyber-crime or even downloading music was to be forcefully disconnected from the Internet for a long period of time.

The ISP should be entitled to enforce such law.

2006 Italy

In year 2006, the Italian Ministry of Interior Pisanu issued an anti-terrorism decree under which, all the hot spot and wired Internet connections couldn’t be granted to unidentified subjects.

This never helped in reality to fight against criminality but disrupted the communications and services throughout all the country’s hotels and airports.

Sweden 2008-2009
The Pirate Bay case

The music and movie industries are blaming file sharing as the reason behind a reduction of their incomes. The industry lobbied the Swedish authorities in seizing the equipment of the Pirate Bay torrent tracker, whose managers were found guilty in April 2009 after a controversial trial.

THE WRONG SOLUTION

Being INCAPABLE even to understand the file sharing phenomenon from its bare social, motivational and technical foundations, authorities are moving from the concept of punishing the wrongdoers to the concept of punishing those who provides “per se” legitimate technical solutions.

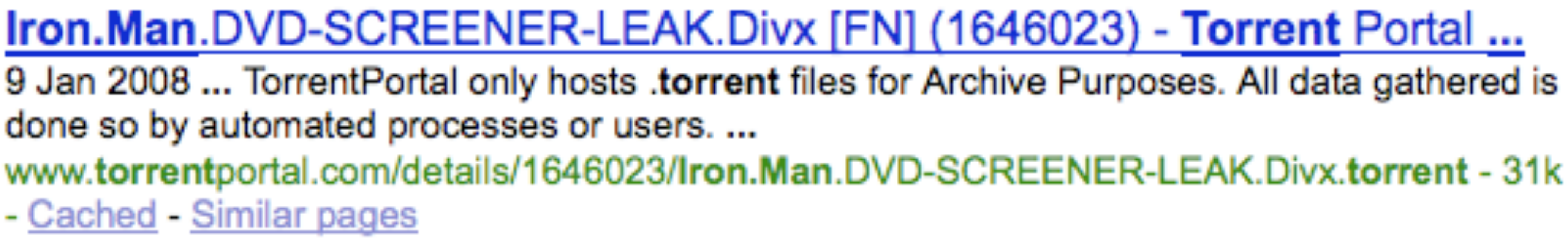
Under this point of view the ISPs, CERN, and all the search engines should be accounted as guilty

Modern threats to economy: file sharing

The Pirate Bay

http://torrents.thepiratebay.org/4856158/Iron_Man_%5BCz%5DDvDRip%5BbY_sOtY%5D.4856158.TPB.torrent

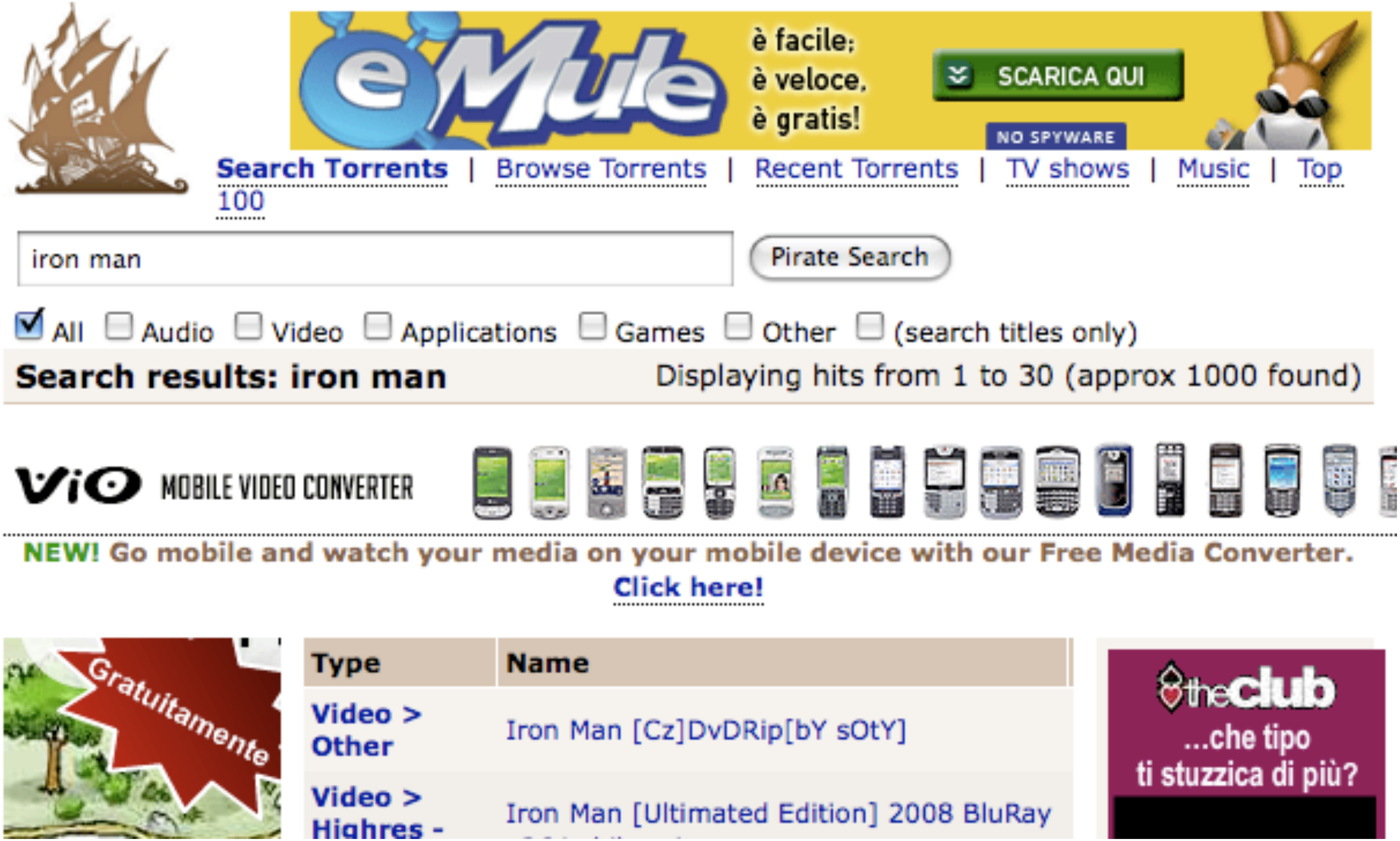
Google™



Iron.Man.DVD-SCREENER-LEAK.Divx [FN] (1646023) - **Torrent** Portal **...**

9 Jan 2008 ... TorrentPortal only hosts .**torrent** files for Archive Purposes. All data gathered is done so by automated processes or users. ...

www.**torrent**portal.com/details/1646023/**Iron.Man**.DVD-SCREENER-LEAK.Divx.**torrent** - 31k - Cached - Similar pages



Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100

iron man

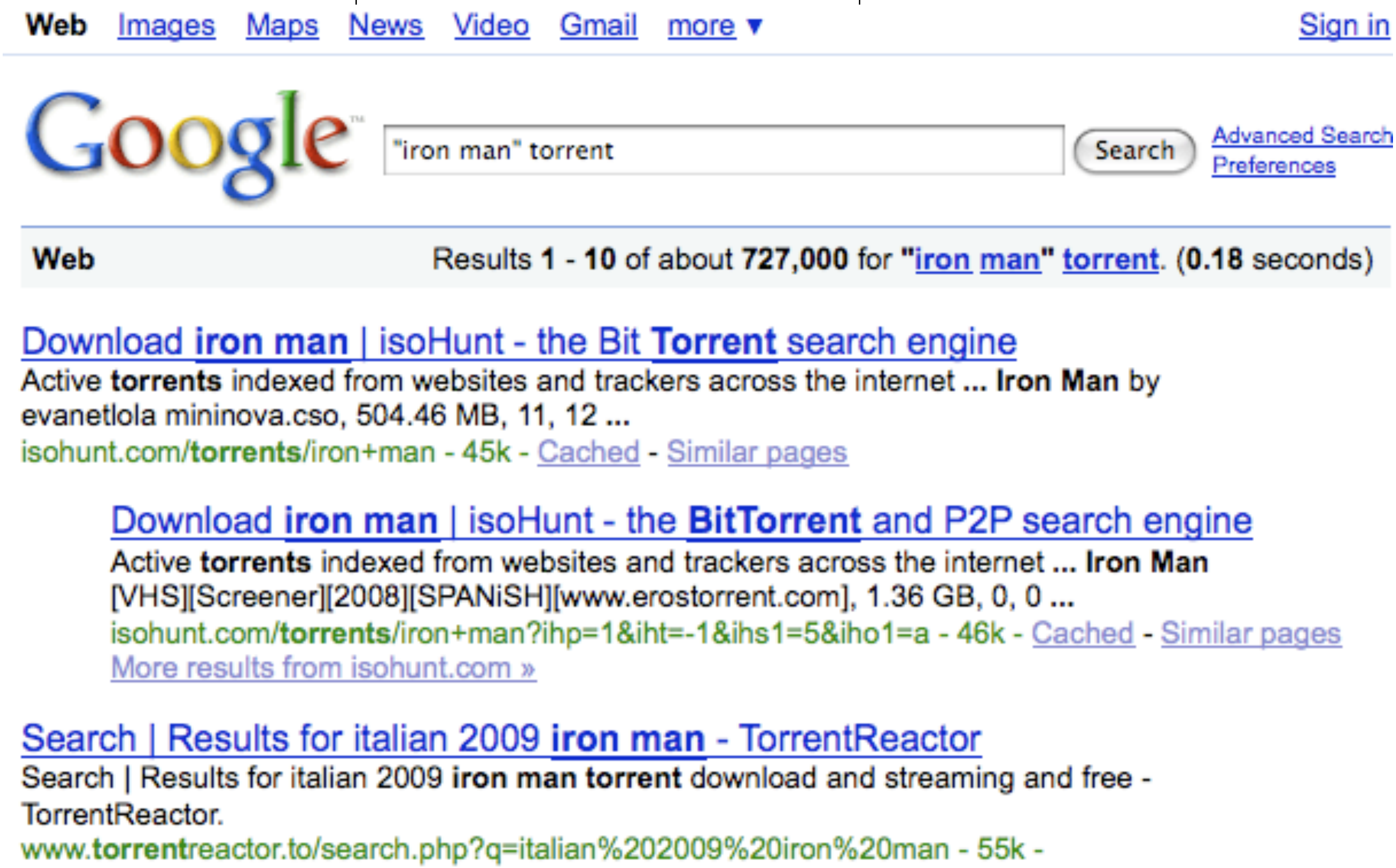
Pirate Search

☑ All □ Audio □ Video □ Applications □ Games □ Other □ (search titles only)

Search results: iron man Displaying hits from 1 to 30 (approx 1000 found)

NEW! Go mobile and watch your media on your mobile device with our Free Media Converter. Click here!

Type	Name
Video > Other	Iron Man [Cz]DvDRip[bY sOtY]
Video > Highres -	Iron Man [Ultimated Edition] 2008 BluRay



"iron man" torrent

Web Results **1** - **10** of about **727,000** for **"iron man" torrent**. (**0.18** seconds)

Download **iron man** | isoHunt - the Bit **Torrent** search engine
Active **torrents** indexed from websites and trackers across the internet ... **Iron Man** by evanetlola mininova.cso, 504.46 MB, 11, 12 ...
isohunt.com/**torrents**/iron+man - 45k - Cached - Similar pages

Download **iron man** | isoHunt - the **BitTorrent** and P2P search engine
Active **torrents** indexed from websites and trackers across the internet ... **Iron Man** [VHS][Screener][2008][SPANiSH][www.erostorrent.com], 1.36 GB, 0, 0 ...
isohunt.com/**torrents**/iron+man?ihp=1&iht=-1&ihs1=5&iho1=a - 46k - Cached - Similar pages
More results from isohunt.com »

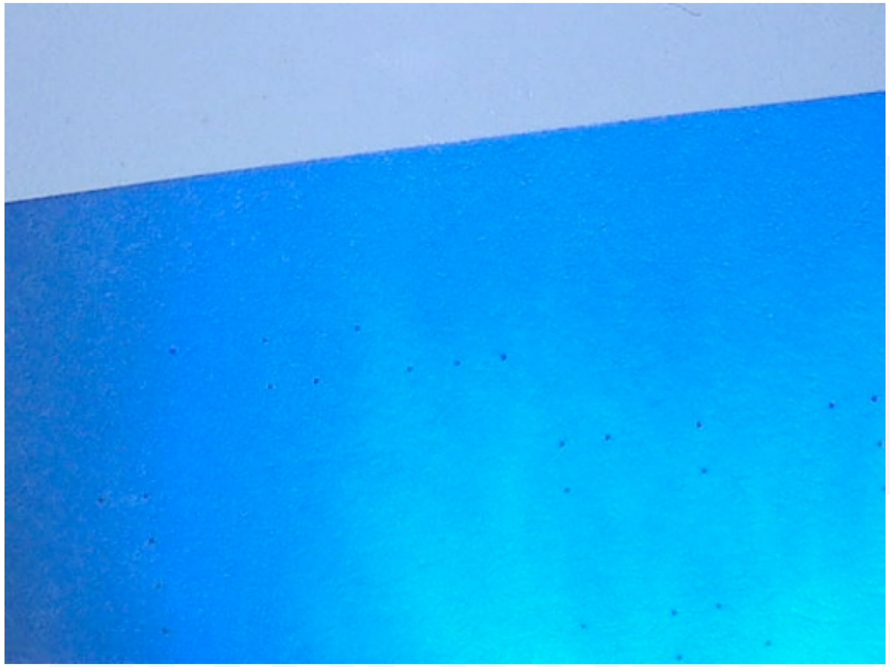
Search | Results for italian 2009 **iron man** - TorrentReactor
Search | Results for italian 2009 **iron man torrent** download and streaming and free - TorrentReactor.
www.**torrent**reactor.to/search.php?q=italian%202009%20iron%20man - 55k -

Multi layered threats

WHAT ELSE?

?

http://www.eff.org/Privacy/printers/



3G PHONES

- rtsp://media-1.datamerica.com/defcon/dc-11/video/2003_Defcon_V29-Roberto_Preatoni-Future_Frontiers_of_Hacking-video.rm

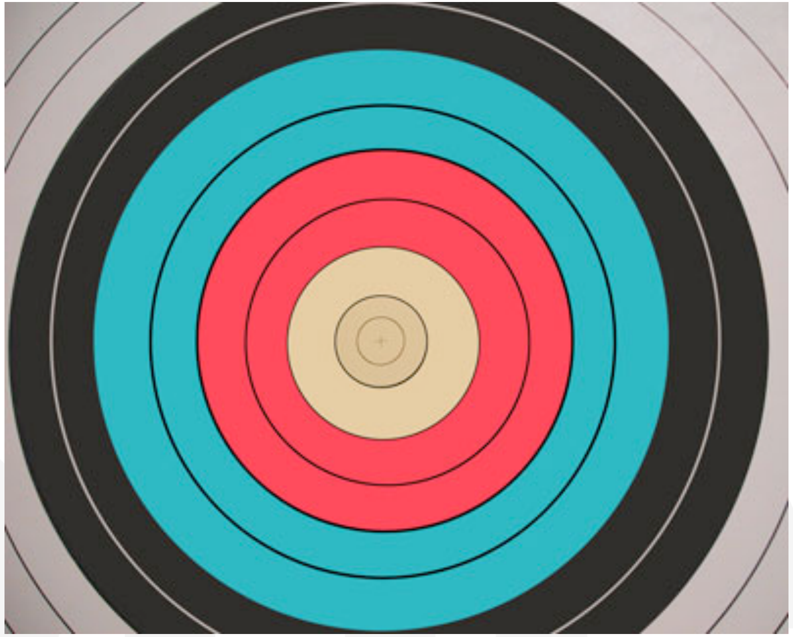
Lesson learned?

Use proprietary software and hardware when possible. And when not possible, use at least well reviewed open sourced software

Lesson learned?

Excessive data retention causes more troubles than benefits.

There is a hidden danger from the social point of view as once adopted and enforced a data retentive policy, it’ll take a revolution to take it down (remember the London airport case?)



ONCE AGAIN, AM I A TARGET OF CRIMINALS OR OF MY OWN GOVERNMENT?

Who were the best security aware managers in world’s history?

?

Questions?

English

¿Preguntas?

Spanish

Domande?

Italian

سئلة؟

Arabic

вопросы?

Russian

質問

Ερωτήσεις?

Greek

Japanese

tupoQghachmey

Klingon