Laboratoire de virologie et de cryptologie opérationnelles (V+ C)^{o}

How to plan, launch and conduct cyberattacks

Intelligence, planning, conduct

Ltc (ret) FILIOL Eric

filiol@esiea.fr

How to plan, launch and conduct cyberattacks

These slides and data exposed hereafter are freely reusable provided that their origin and their author are explicitely mentionned.

Introduction

- Which concept of cyberwarfare?
  - Cyberwar or cyberattacks?
- Are ``cyberattacks’’ restricted to a hypothetical ``cyberspace’’ only?
- Is there such thing as a cybernetic reality which would be independent from the real, physical world?
  - Are our systems and networks an ``independent’’ territory?
  - Would cyberattacks concern virtual worlds only (e.g. *Second Life*)?

Introduction (2)

- How to conduct a cyberattacks?
- What is the difference with conventional conduc of maneuver?
- Is is necessary to create a new army branch (digital infantry, digital corps of engineer…)?
  - What about planning and conduct of maneuver aspects?
- What is a critical infrastructure?
  - Is the concept of "bunker" still a valid one?
- What are the cybertattacks' targets?
- Does the concept of cyberwar law make senses?
- What about the cyberwarrior's ethics?

Introduction (3)

- Different views exist but what about their relevance?
- The operational background (military, police) COMBINED to the scientific/computer science backgroung is essential.
- An intelligence background is useful as well.
- The talk will be put under that triple view.

Introduction (4)

- Aim of the talk:
  - To explain what an attacker can really do.
    - Get rid of what you call Ethics! Think like the attacker does!
  - To generalize the concept of cyberattack.
    - There exist far more critical approaches than website defacing or DoS/DDoS attacks.
    - Let your imagination play!
  - To generalize the concept of critical infrastructure
    - Organizing your systems and networks as bunkers becomes inefficient and futile.

Introduction (5)

- This talk is based on different feedbacks and experience:
  - Analyses of real cases and military experience.
  - NATO InfoOps Course.
  - Forensics analysis (technical court-ordered appraisial).
  - Analyses of existing doctrines.
  - RESEARCH: from theory to (and for) the operational stuff!

Summary

- For a definition of the cyberattack concept.
- Critical infrastructure concept.
- Interdependencies between systems.
- The different phases of a cyberattack.
  - Key role of intelligence.
  - Planning.
  - Conduct of manoeuver.
- A few exemples of « bricks of attacks ».
- Conclusion

For a definition of the cyberattack concept

Founding doctrine

- Colonels Qiao & Wang

  « *Unrestricted warfare* » *(1999)*

- « The first rule of **unrestricted warfare** is that there are no rules, with nothing forbidden.»

« Today there is nothing in the world that cannot be considered as a potential weapon. »

Concept of « building the weapon to fit the fight. »

Founding doctrine (2)

(…) if attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. (…)

Concept of war

- Extreme form of communication between two or more groups to protect or increase its wealth, its interests or its influence through action on
  - resources (physical component),
  - populations (human component),
  - minds (intellectual and cultural component),
  - territory (space),
  - information.
- War ultimate action tagets the real, physical world!

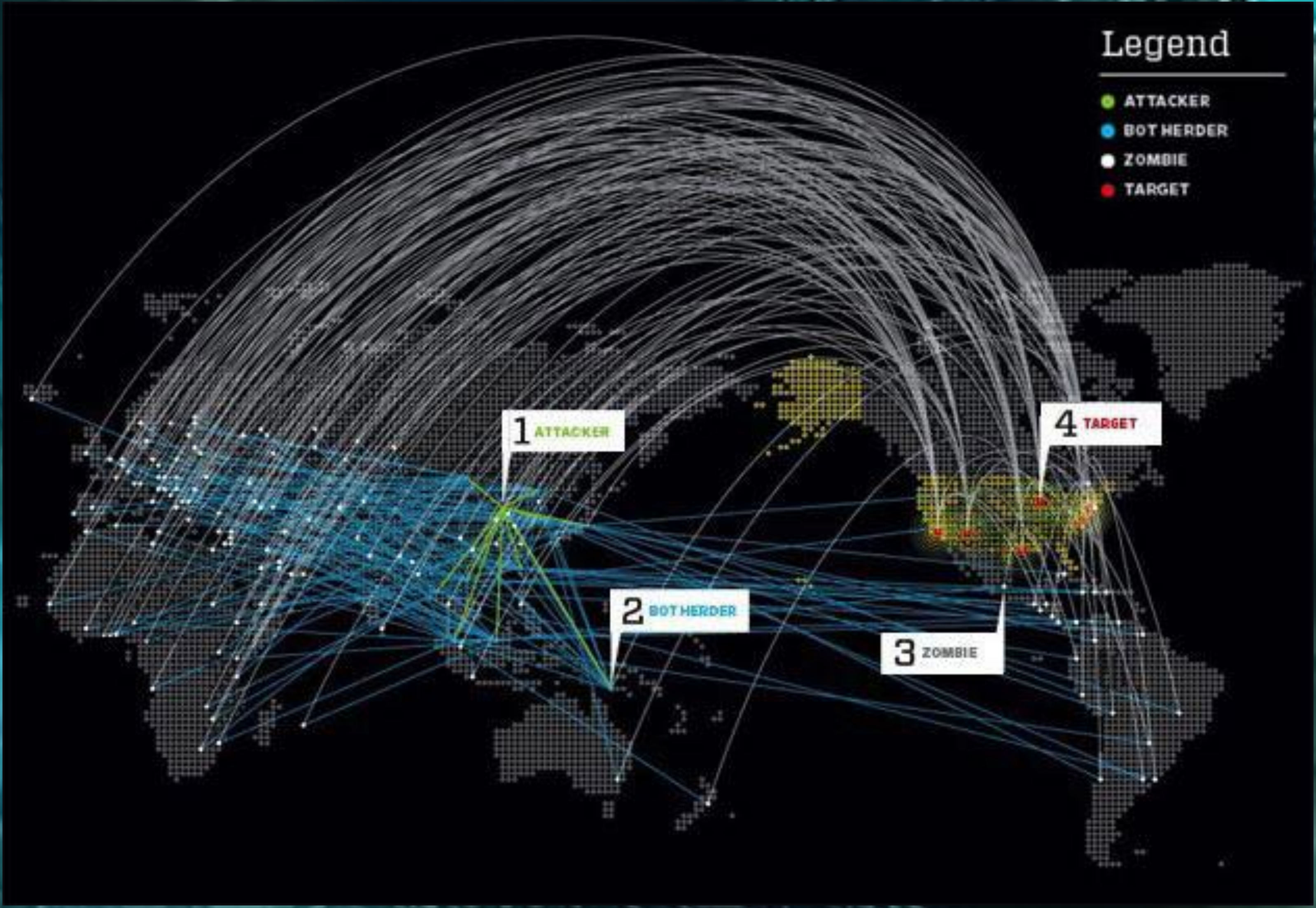
Concept of cyberattack

- Attack targeting the real sphere (world).
  - Either directly through an Information and Communication System (ICS).
    - E.g. : attack against people.
  - Or indirectly by attacking a ICS, one or more components in the real world are depending on.
    - E.g. : attack against the ATM networks.

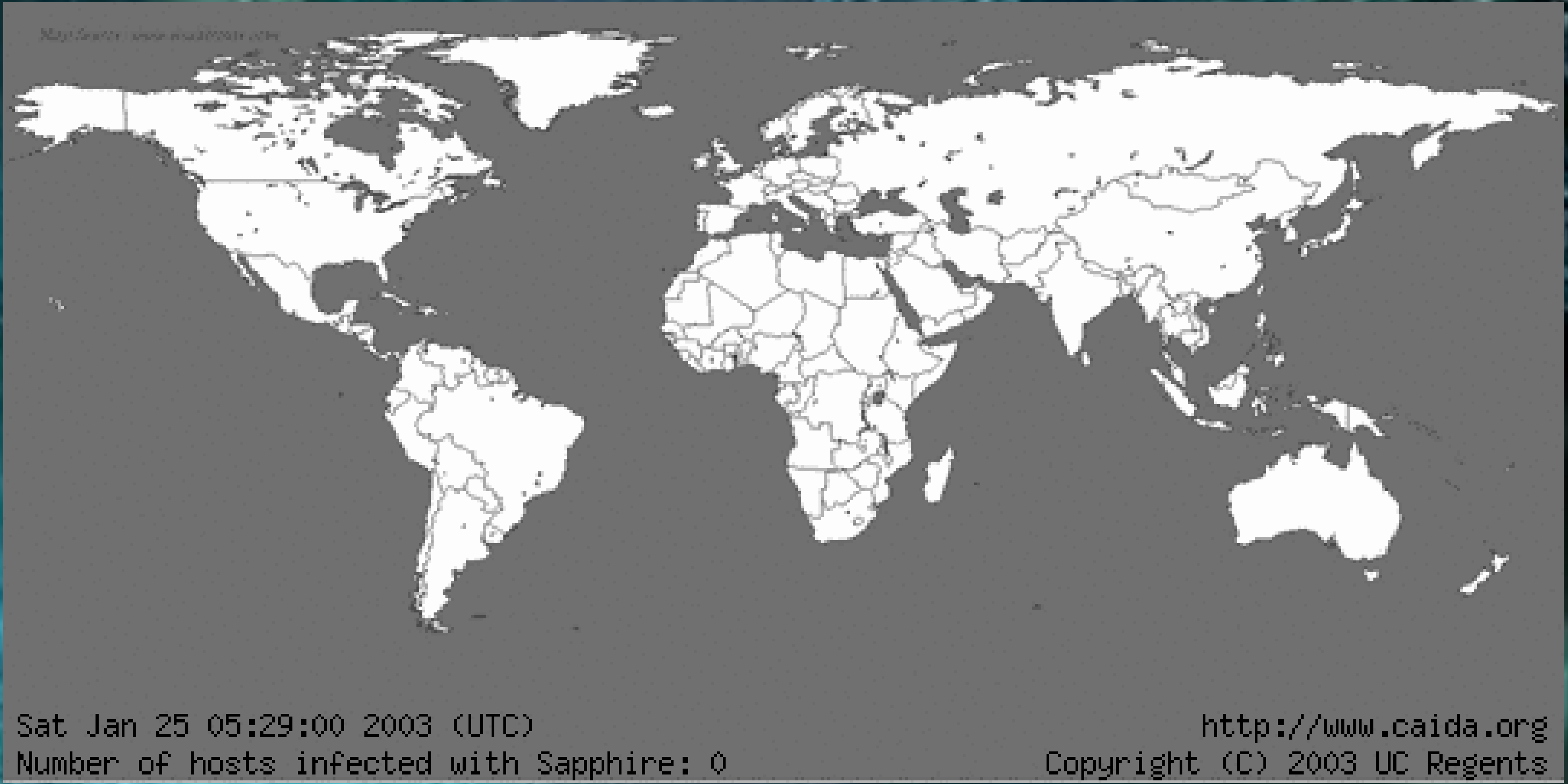
Concept of cyberattack (2)

- Three intrinsic characteristics:
  - *Obliteration of the space concept.*
  - *Obliteration of the time concept.*
  - *Obliteration of the concept ofproof.*
- Those are three fundamental differences with classical (conventional) war techniques.

Obliteration of space



Obliteration of space (2)



Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0

http://www.caida.org
Copyright (C) 2003 UC Regents

Obliteration of time

- This primarily concerns the victim:
  - Any attack is perceived as sudden and immediate.
- The victim can no longer:
  - Perform intelligence operation.
  - Conduct any maneuver.
- Very limited *a posteriori* analysis (debriefing and forensics).

Obliteration of time (2)

- As for the attacker, ability to go back in time (*backward time*) before the actual attack time.
  - Immediacy in the conduct of maneuver.
  - Delay in planning and intelligence phases.
- The attacks can be prepared months ahead!

Obliteration of proof

- In the digital world
  - Everything can be falsified.
  - The concept of proof does no longer make sense.
- It is possible to usurp or forge any kind of data:
  - IP or MAC address.
  - Email address.
  - Any document.
- The complexity depends on the security tools in place on the target system.
- The concept of digital retaliations or legitime defense has no validity.
  - Bénichou/Lefranc *Introduction to Network Self-defense: technical and judicial issues*. Journal in Computer Virology, 1-(1-2), 2005.

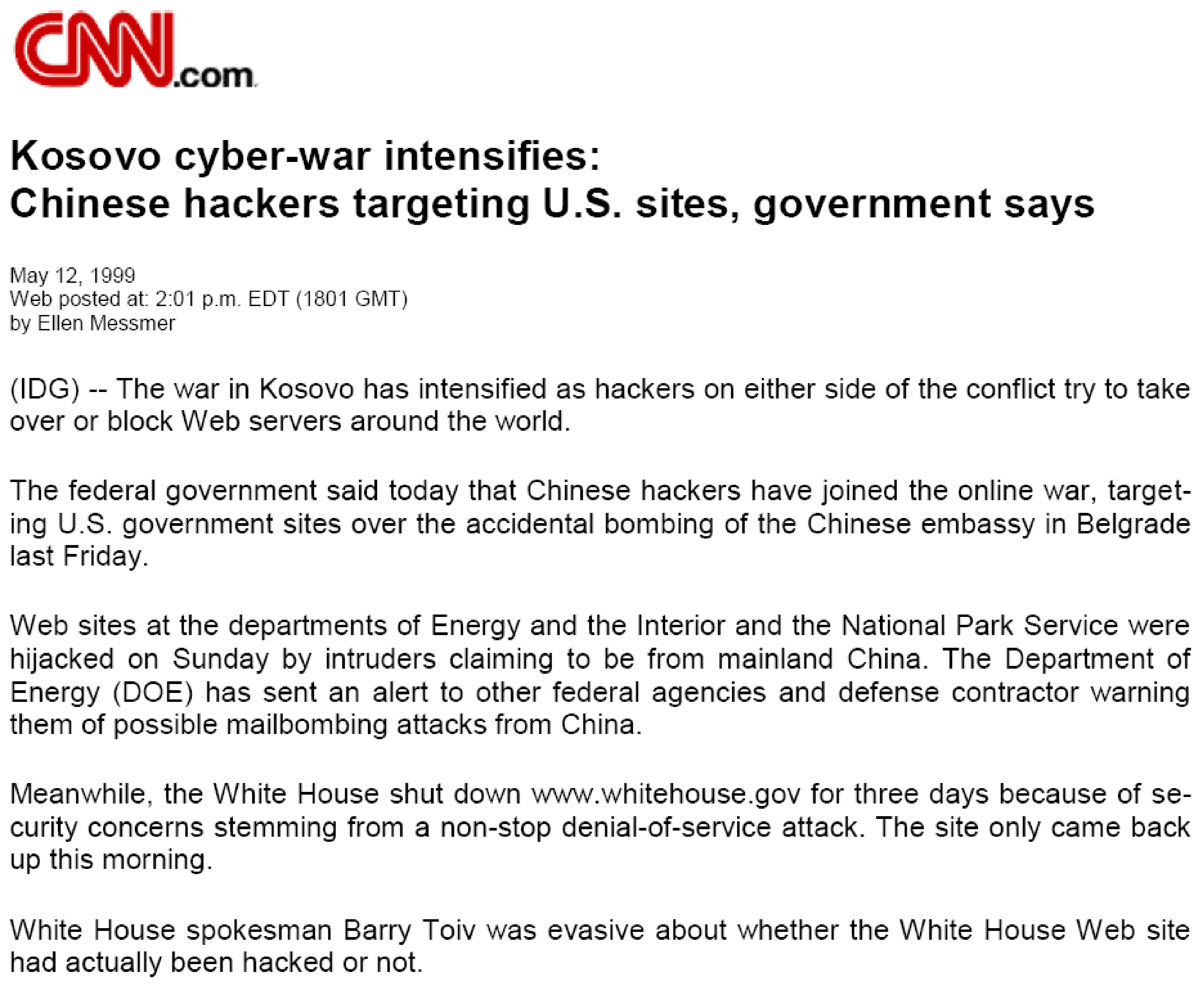
Total dematerialisation

- Cybertattackers exploit that dematerialisation as musch as possible:
  - Stop to be naive!
  - Ethics does no longer make sense…
  - … and any control attempt as well!
    - what about UNO observers?
    - what about international courts?

In the cyberspace EVERYTHING is allowed *(« Unrestricted warfare ! »)*

Who are cyberwarriors?

- Any individual skilled in ICS
  - *nearly any student in computer science/computer security (graduate and undergraduate).*
  - *critical problem of knowledge transfer in western university curriculum.*
- However having a logistic support for the planning and the conduct of maneuver is mandatory:
  - Mafias', terrorist groups' and (rogue) state support.



CNN.com

Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says

May 12, 1999
Web posted at: 2:01 p.m. EDT (1801 GMT)
by Ellen Messmer

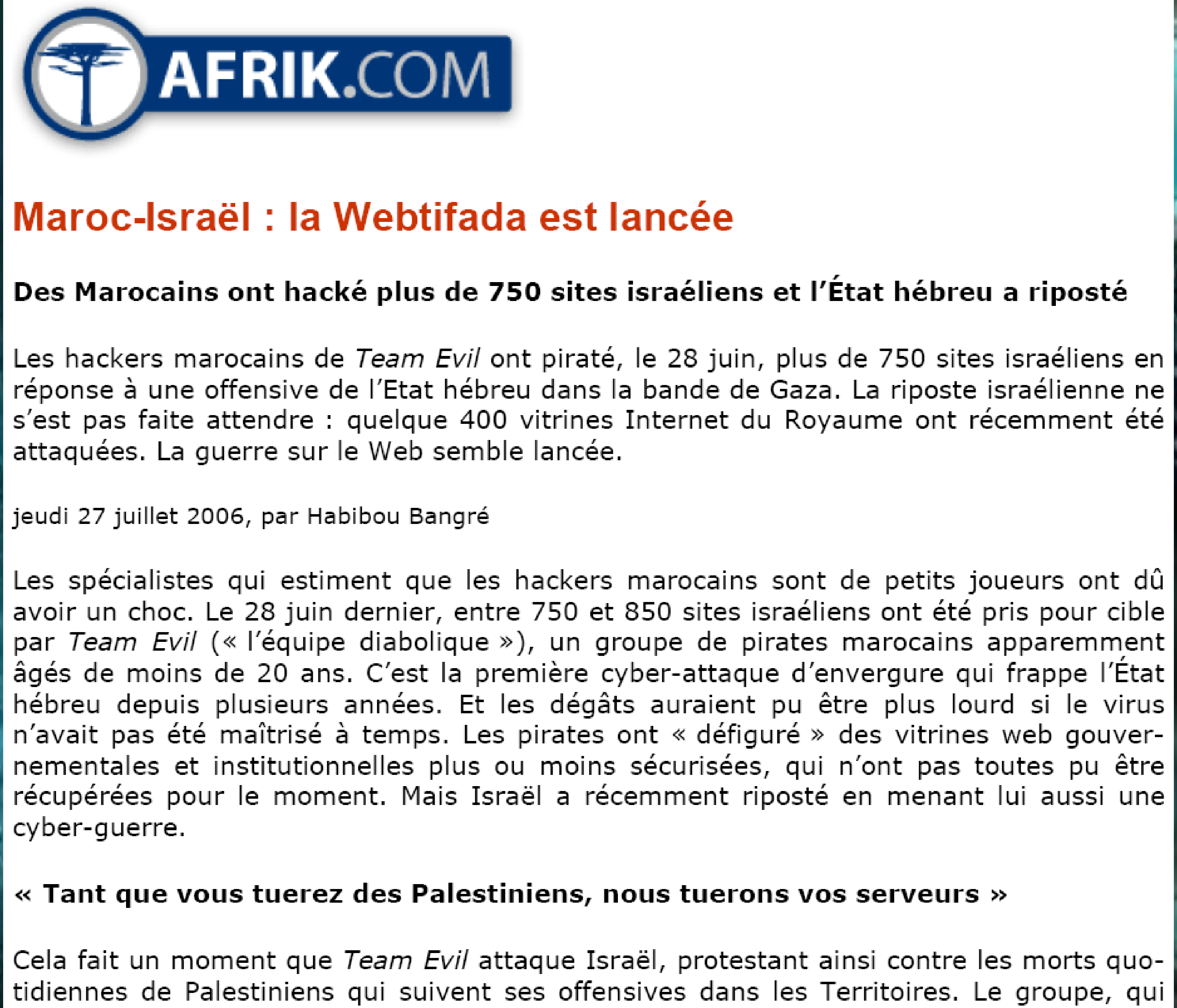
(IDG) -- The war in Kosovo has intensified as hackers on either side of the conflict try to take over or block Web servers around the world.

The federal government said today that Chinese hackers have joined the online war, targeting U.S. government sites over the accidental bombing of the Chinese embassy in Belgrade last Friday.

Web sites at the departments of Energy and the Interior and the National Park Service were hijacked on Sunday by intruders claiming to be from mainland China. The Department of Energy (DOE) has sent an alert to other federal agencies and defense contractor warning them of possible mailbombing attacks from China.

Meanwhile, the White House shut down www.whitehouse.gov for three days because of security concerns stemming from a non-stop denial-of-service attack. The site only came back up this morning.

White House spokesman Barry Toiv was evasive about whether the White House Web site had actually been hacked or not.



Maroc-Israël : la Webtifada est lancée

Des Marocains ont hacké plus de 750 sites israéliens et l'État hébreu a riposté

Les hackers marocains de *Team Evil* ont piraté, le 28 juin, plus de 750 sites israéliens en réponse à une offensive de l'Etat hébreu dans la bande de Gaza. La riposte israélienne ne s'est pas faite attendre : quelque 400 vitrines Internet du Royaume ont récemment été attaquées. La guerre sur le Web semble lancée.

jeudi 27 juillet 2006, par Habibou Bangré

Les spécialistes qui estiment que les hackers marocains sont de petits joueurs ont dû avoir un choc. Le 28 juin dernier, entre 750 et 850 sites israéliens ont été pris pour cible par *Team Evil* (« l'équipe diabolique »), un groupe de pirates marocains apparemment âgés de moins de 20 ans. C'est la première cyber-attaque d'envergure qui frappe l'État hébreu depuis plusieurs années. Et les dégâts auraient pu être plus lourd si le virus n'avait pas été maîtrisé à temps. Les pirates ont « défiguré » des vitrines web gouvernementales et institutionnelles plus ou moins sécurisées, qui n'ont pas toutes pu être récupérées pour le moment. Mais Israël a récemment riposté en menant lui aussi une cyber-guerre.

« Tant que vous tuerez des Palestiniens, nous tuerons vos serveurs »

Cela fait un moment que *Team Evil* attaque Israël, protestant ainsi contre les morts quotidiennes de Palestiniens qui suivent ses offensives dans les Territoires. Le groupe, qui

Islamic Jihad's cyber-war brigades

By OLA AL-MADHOUN
Posted June 17th, 2008

The Palestinian Islamist movement, Islamic Jihad, says it has a new division of its armed Al-Quds Brigades - a cyberwar unit that claims it has hacked into the websites of several Israeli media outlets.

Hassan Shakoura, former head of the Al-Quds Brigades' cyberwar unit before his death in March 2007. © Ola Al-Madhoun

GAZA CITY, June 17, 2008 (MENASSAT) – The Palestinian Islamist movement, Islamic Jihad, has added a cyber-war division to its armed Al-Quds Brigades.

It was a response to years of attacks by Israeli hackers, and according to the Brigades spokesman, Abu Hamza, it equals the playing field in cyberspace.

"The Israeli's have worked very hard the past few years on monitoring all the Palestinian websites, especially

Concept of critical infrastructure

Classical definition

« *Critical infrastructures are the physical facilities and information technology, networks, services and assets which, in the event of disruption or destruction, may have serious impacts on health, safety or welfare of citizens or the work of governments. Critical infrastructures are in many sectors of the economy, including banking and financial sectors, transport and distribution, energy, utilities, health, food supply and communications, and some government services (EC 12/12/2006)* »

- Only the target is taken into account! Not its environment!

Generalized definition

- To take into account human part of a system is essential:
  - Decision-making level (always target the head!)
    - « *The fish always rots from the head* » (Chinese saying)
  - Technical staff.
  - Staff with strong media impact (journalists, union leaders…).
  - ... any human component on which the infrastructure relies to function properly.
- Those components are prioritary targets with respect to the system interdependencies.

Generalized definition (2)

- Take external components which are (seemingly) not critical:
  - Subcontractors
  - Suppliers.
- Take the political and public (media) dimension:
  - Strong asymmetry between what the attacker can do and what the public power can do.
  - Managing the public opinion is a sensitive matter!
- There is a strong need for a precise mapping of all interpendencies between those components.

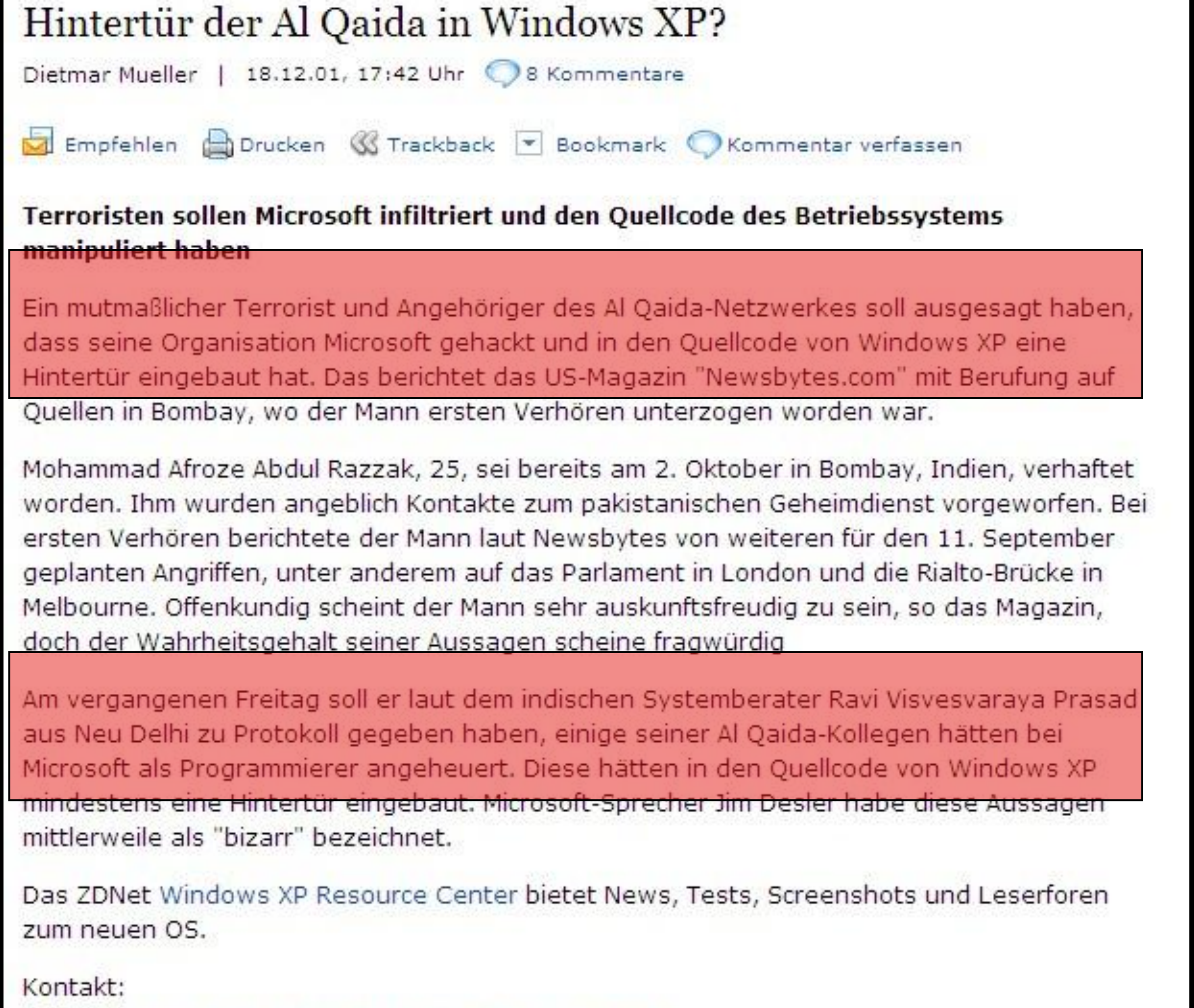
Generalized definition (3)

- Take external and relocated components into account:
  - *Data centers*
  - Oversight and supervision services (e.g. Tel. operators)
  - Foreign suppliers
  - Subcontractors.
  - Foreign subcontractors…
- For those components, to establish
  - their exact number,
  - their reel impact on the interpendencies,

  is very complex not to say impossible.
- No control of their security is actually possible!

Example: Windows XP

- December 2001 – Arrest of Afroze Abdul Razzak, in Bombay.
- Al-Qaida member hired in the Windows XP development teams in India.
- At that time, strongly suspected of having introduced one of the first critical Windows XP vulnerabilities .
- This case has never been really clarified.



Hintertür der Al Qaida in Windows XP?

Dietmar Mueller | 18.12.01, 17:42 Uhr 8 Kommentare

Terroristen sollen Microsoft infiltriert und den Quellcode des Betriebssystems manipuliert haben

Ein mutmaßlicher Terrorist und Angehöriger des Al Qaida-Netzwerkes soll ausgesagt haben, dass seine Organisation Microsoft gehackt und in den Quellcode von Windows XP eine Hintertür eingebaut hat. Das berichtet das US-Magazin "Newsbytes.com" mit Berufung auf Quellen in Bombay, wo der Mann ersten Verhören unterzogen worden war.

Mohammad Afroze Abdul Razzak, 25, sei bereits am 2. Oktober in Bombay, Indien, verhaftet worden. Ihm wurden angeblich Kontakte zum pakistanischen Geheimdienst vorgeworfen. Bei ersten Verhören berichtete der Mann laut Newsbytes von weiteren für den 11. September geplanten Angriffen, unter anderem auf das Parlament in London und die Rialto-Brücke in Melbourne. Offenkundig scheint der Mann sehr auskunftsfreudig zu sein, so das Magazin, doch der Wahrheitsgehalt seiner Aussagen scheine fragwürdig

Am vergangenen Freitag soll er laut dem indischen Systemberater Ravi Visvesvaraya Prasad aus Neu Delhi zu Protokoll gegeben haben, einige seiner Al Qaida-Kollegen hätten bei Microsoft als Programmierer angeheuert. Diese hätten in den Quellcode von Windows XP mindestens eine Hintertür eingebaut. Microsoft-Sprecher Jim Desler habe diese Aussagen mittlerweile als "bizarr" bezeichnet.

Das ZDNet Windows XP Resource Center bietet News, Tests, Screenshots und Leserforen zum neuen OS.

Kontakt:

Example: Windows XP (2)

- Example of critical vulnerability:

Modify the code

```
If(VarCritique == fonction (arguments))
  {
    ….
  }
```

into the following one

```
If(VarCritique = fonction(arguments))
  {
    ….
  }
```

Interdependencies of systems

Definition

- All direct and indirect dependencies between a target (*final goal*) and one or more components (*primary objectives*) on which this target depends.
- Managed through the dependencies matrix.
- This matrix is built during the intelligence phase.
- Enable to identify the non visible or non obvious dependencies.
- Strong support of graph theory concepts/tools.
- Application: optimized dynamic management of botnets (Filiol et al. – 2007).
- Development of Gorgias tool.

Dependencies matrix

- Let C_0 be a target and c_1, c_2, c_3, c_4, c_i a given number of components…
- Those components are physical, human parts, services…
- Any matrix entry is defined by

$$c_{ij} = \begin{cases} 1 & \text{if component } i \text{ depends on component } j \\ 0 & \text{otherwise} \end{cases}$$

- It is possible to generalize to matrices with integer (non binary) entries.

Dependencies matrix (2)

Trivial but didactic case (sparse dependencies)

$$\begin{array}{cc}
C_0 \rightarrow & \left[\begin{matrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{matrix}\right.
\end{array}$$

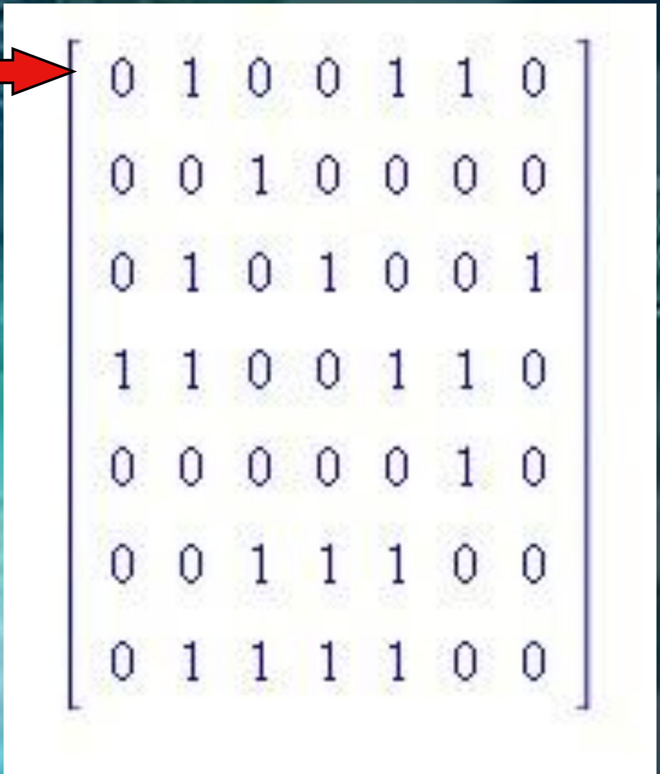
Initial matrix

$$\left[\begin{matrix} 0 & 0 & 0 & 0 & 0 & \boxed{1} & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{matrix}\right]$$

Dependency of depth 5 between C_0 and C_5

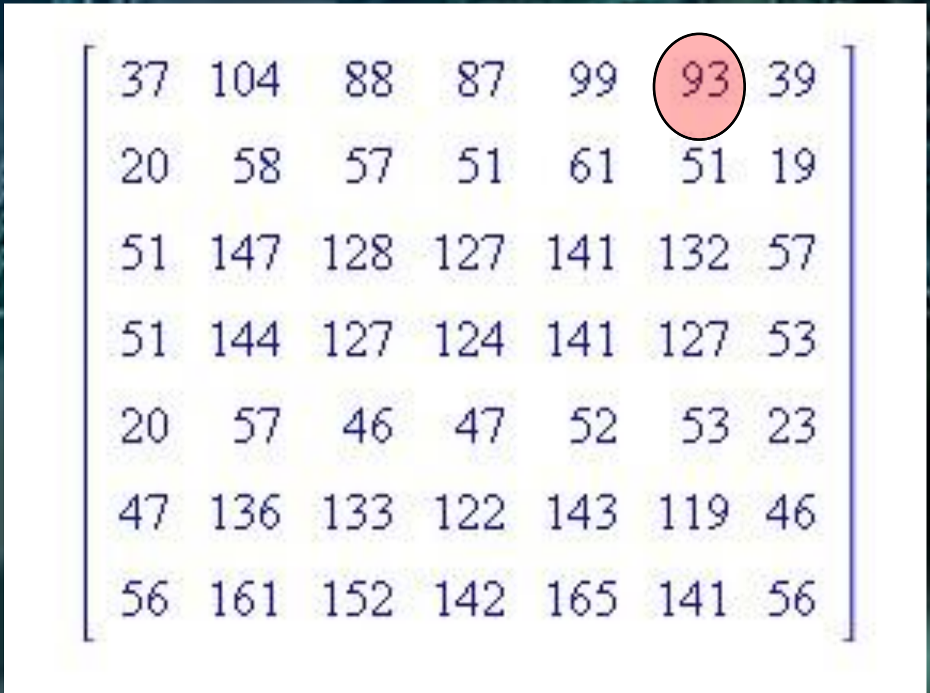
Dependencies matrix (3)

Real case (dense dependencies)



$$\begin{array}{cc}
C_0 \rightarrow & \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}
\end{array}$$

Initial matrix



$$\begin{bmatrix} 37 & 104 & 88 & 87 & 99 & 93 & 39 \\ 20 & 58 & 57 & 51 & 61 & 51 & 19 \\ 51 & 147 & 128 & 127 & 141 & 132 & 57 \\ 51 & 144 & 127 & 124 & 141 & 127 & 53 \\ 20 & 57 & 46 & 47 & 52 & 53 & 23 \\ 47 & 136 & 133 & 122 & 143 & 119 & 46 \\ 56 & 161 & 152 & 142 & 165 & 141 & 56 \end{bmatrix}$$

93 dependencies of depth 5 between C_0 and C_5

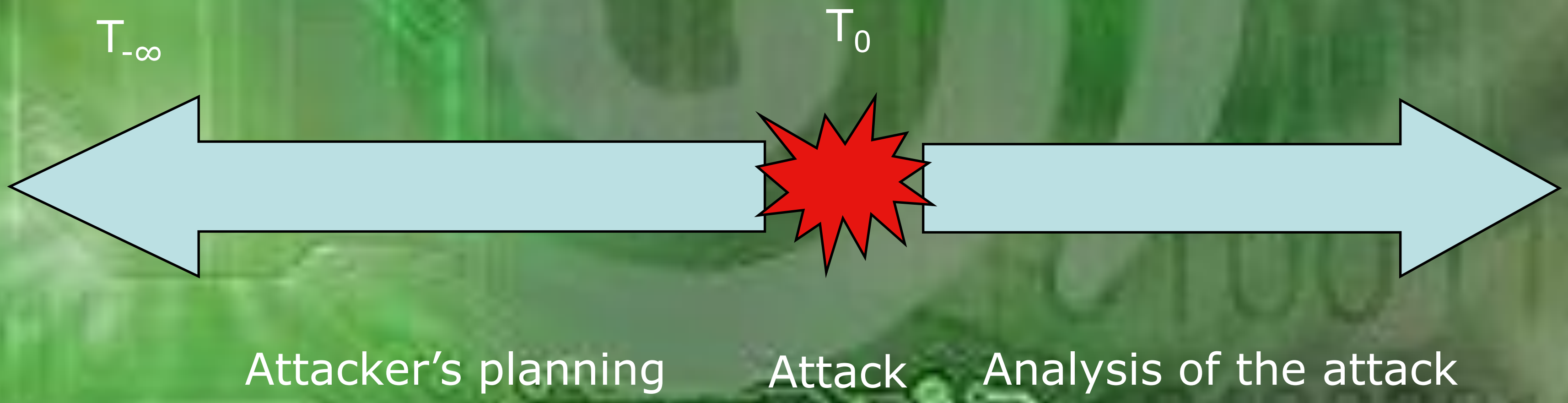
Dependencies matrix (4)

- In both cases, there exist a dependency chain between the target C_0 and the C_5 component.
- Component C_5 is not protected enough against cyberattacks.
- By attacking C_5, the attacker tries to obtain a « domino effect » by exploiting the existing dependencies.
- In the real case (dense dependencies), the number of possibilities is such
  - that their exist a large number « variants » for the attacker (planning and conduct of maneuver phases).
  - The mapping is far too complex to analyse, to provide a strong enough defense of target C_0.

The different phases of a cyberattack

Backward time

- The attacker plans his attack with an inversed time vision.
  - How to plan in time in order to achieve the desired final effect?
  - Think as chess player!
- For the victim, the attack must appear sudden and unaccountable.

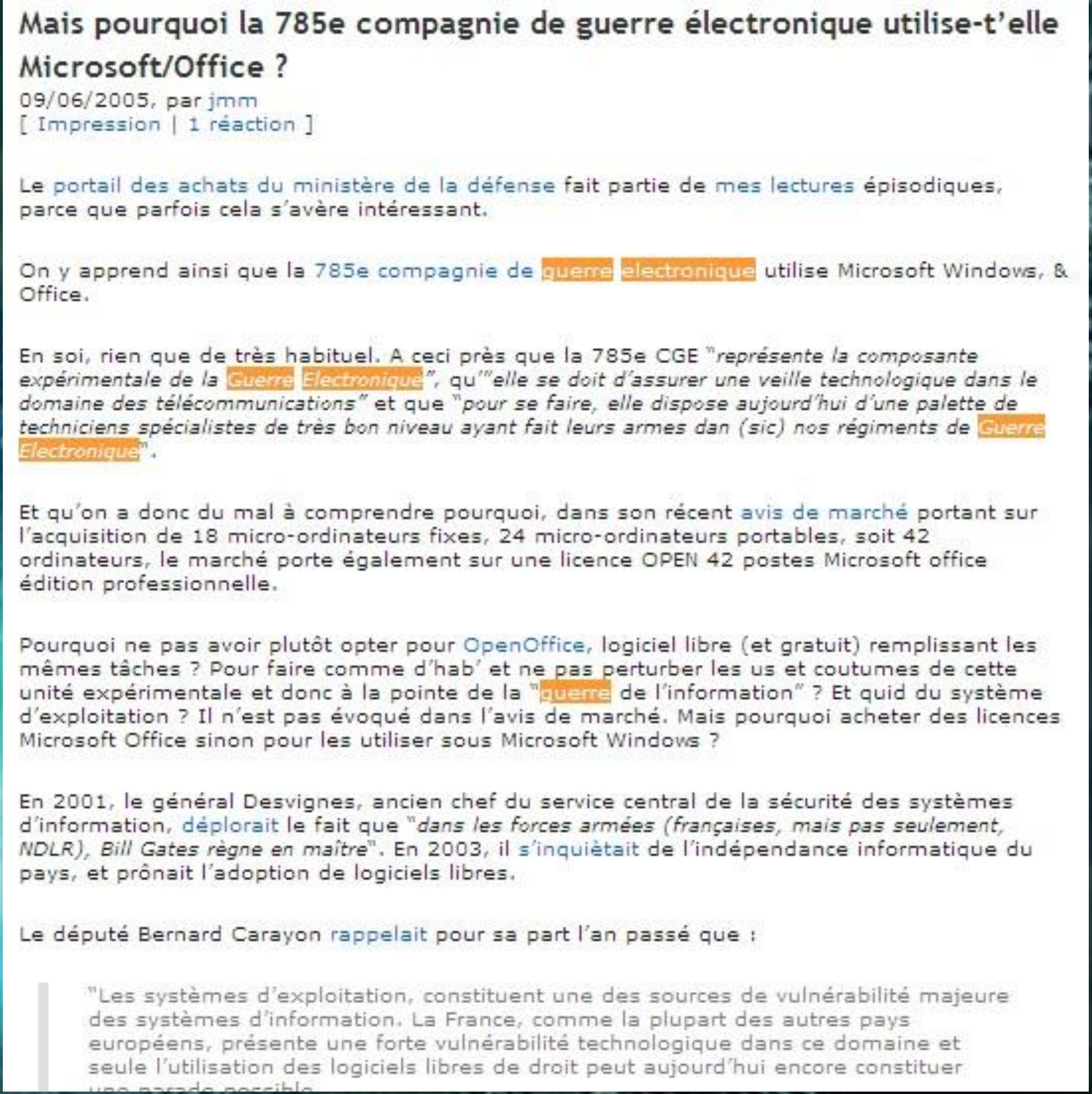


Intelligence phase

- It is an essential one since it enables to
  - identify critical components,
  - build the dependencies matrix,
  - to provide information for the planning and the conduct phases.
- Strategic upstream intelligence.
- Tactical intelligence (current action).

Intelligence phase (2)

- Nature of intelligence:
  - Technical intelligence.
  - Human (blogs, social networks, public places…)
    - Just exploit the lack of professional discretion and of security backgroung (culture).
  - Open documents (e.g: public market offer)
  - « Ambient » intelligence.
- Goal: to gain a precise image of the intended target whatever the aspect is.
  - Static image
  - Dynamical



Mais pourquoi la 785e compagnie de guerre électronique utilise-t'elle Microsoft/Office ?

09/06/2005, par jmm
[Impression | 1 réaction]

Le portail des achats du ministère de la défense fait partie de mes lectures épisodiques, parce que parfois cela s'avère intéressant.

On y apprend ainsi que la 785e compagnie de guerre electronique utilise Microsoft Windows, & Office.

En soi, rien que de très habituel. A ceci près que la 785e CGE "*représente la composante expérimentale de la Guerre Electronique*", qu'"*elle se doit d'assurer une veille technologique dans le domaine des télécommunications*" et que "*pour se faire, elle dispose aujourd'hui d'une palette de techniciens spécialistes de très bon niveau ayant fait leurs armes dan (sic) nos régiments de Guerre Electronique*".

Et qu'on a donc du mal à comprendre pourquoi, dans son récent avis de marché portant sur l'acquisition de 18 micro-ordinateurs fixes, 24 micro-ordinateurs portables, soit 42 ordinateurs, le marché porte également sur une licence OPEN 42 postes Microsoft office édition professionnelle.

Pourquoi ne pas avoir plutôt opter pour OpenOffice, logiciel libre (et gratuit) remplissant les mêmes tâches ? Pour faire comme d'hab' et ne pas perturber les us et coutumes de cette unité expérimentale et donc à la pointe de la "guerre de l'information" ? Et quid du système d'exploitation ? Il n'est pas évoqué dans l'avis de marché. Mais pourquoi acheter des licences Microsoft Office sinon pour les utiliser sous Microsoft Windows ?

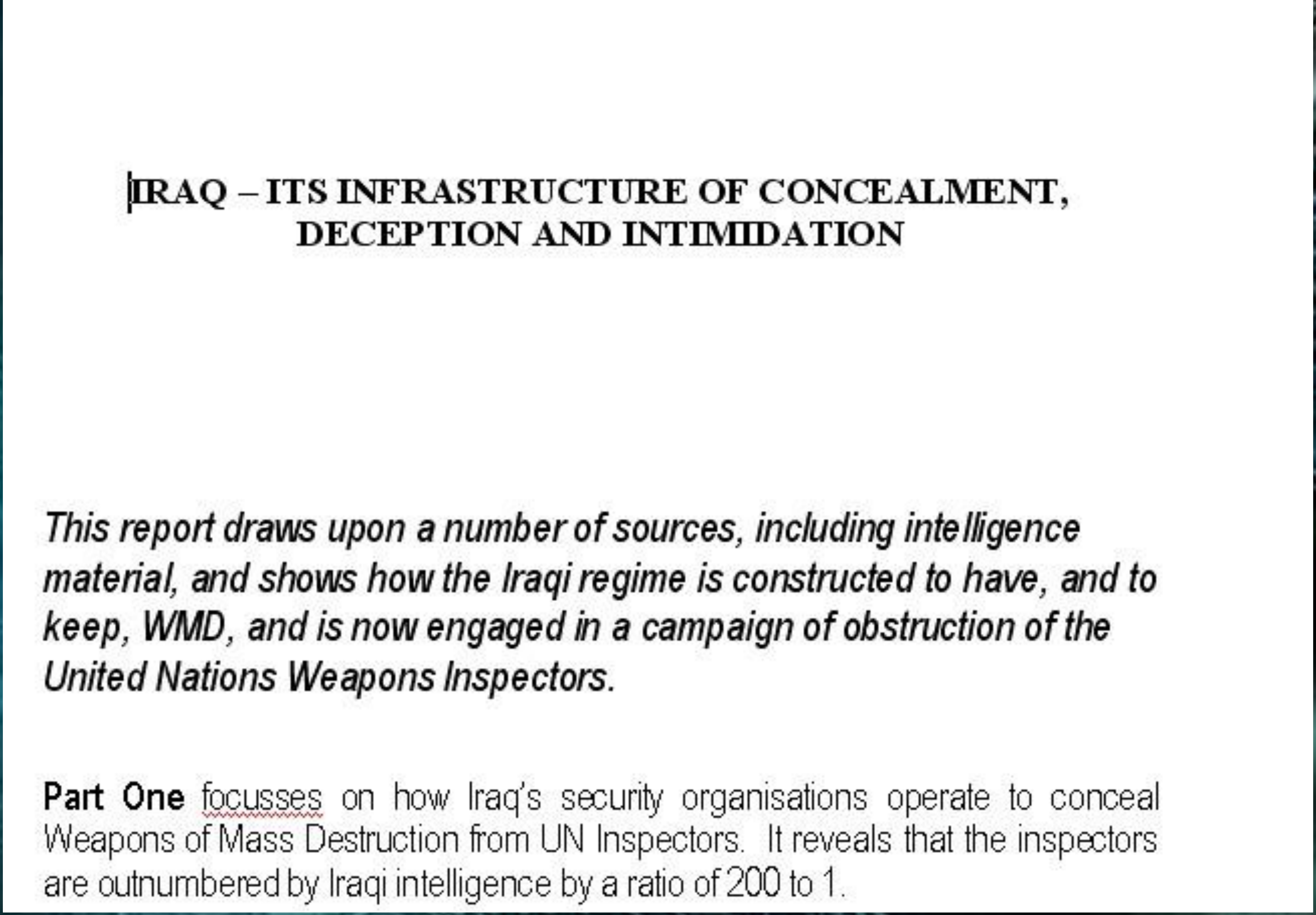
En 2001, le général Desvignes, ancien chef du service central de la sécurité des systèmes d'information, déplorait le fait que "*dans les forces armées (françaises, mais pas seulement, NDLR), Bill Gates règne en maître*". En 2003, il s'inquiètait de l'indépendance informatique du pays, et prônait l'adoption de logiciels libres.

Le député Bernard Carayon rappelait pour sa part l'an passé que :

> "Les systèmes d'exploitation, constituent une des sources de vulnérabilité majeure des systèmes d'information. La France, comme la plupart des autres pays européens, présente une forte vulnérabilité technologique dans ce domaine et seule l'utilisation des logiciels libres de droit peut aujourd'hui encore constituer une parade possible

Intelligence phase (3)

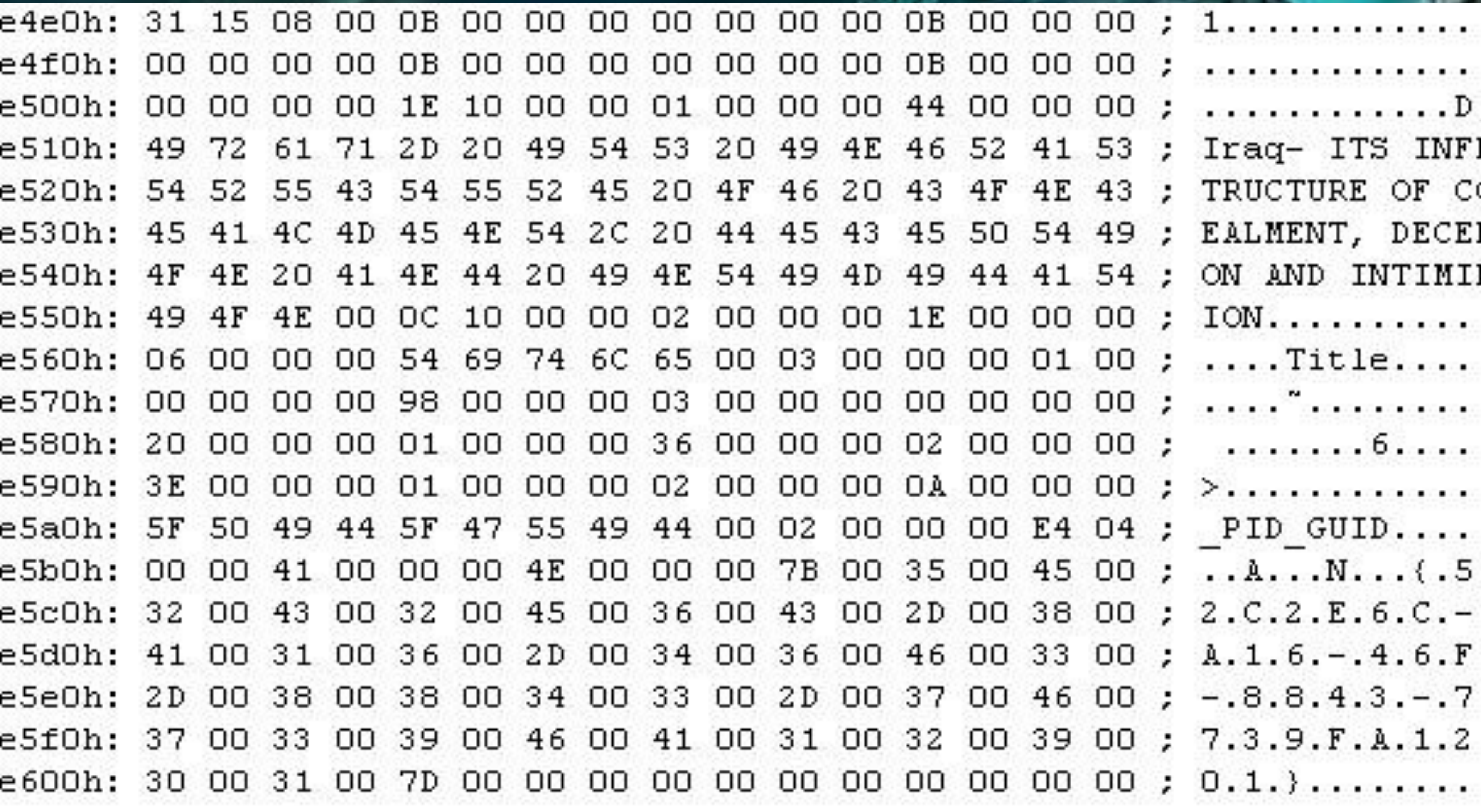
- Gather technical intelligence:
  - Very easy when you where to look!
  - Used hard drives.
  - Innocent looking file.
  - …
- Example: MAC address MAC at the 10th Downing Street (CICR22).
- A large number of real cases.
- Facilitated by most of the Operating systems or so-called « security » software.



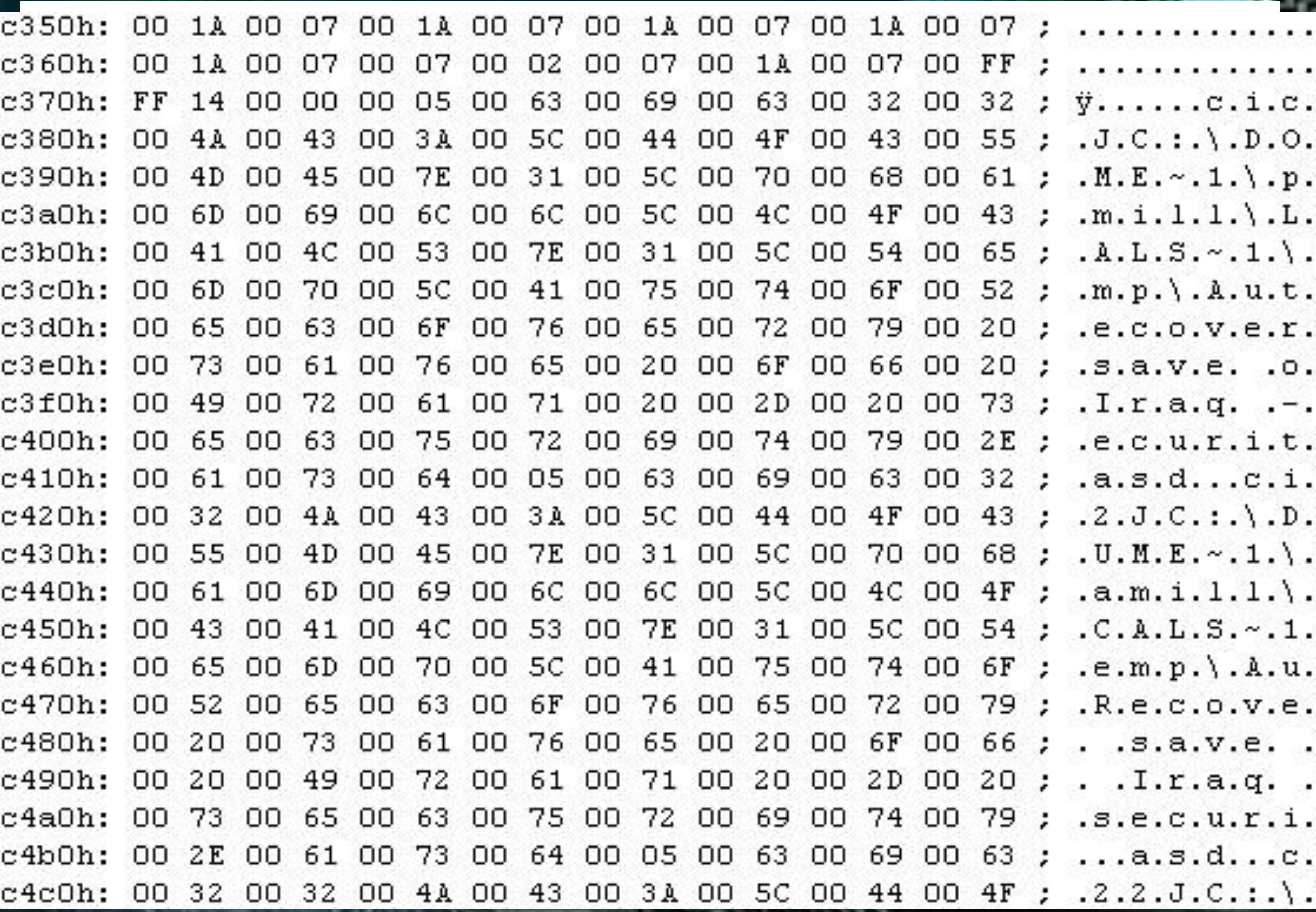
IRAQ – ITS INFRASTRUCTURE OF CONCEALMENT, DECEPTION AND INTIMIDATION

This report draws upon a number of sources, including intelligence material, and shows how the Iraqi regime is constructed to have, and to keep, WMD, and is now engaged in a campaign of obstruction of the United Nations Weapons Inspectors.

Part One focusses on how Iraq's security organisations operate to conceal Weapons of Mass Destruction from UN Inspectors. It reveals that the inspectors are outnumbered by Iraqi intelligence by a ratio of 200 to 1.



```
e4e0h: 31 15 08 00 0B 00 00 00 00 00 00 00 0B 00 00 00 ; 1............
e4f0h: 00 00 00 00 0B 00 00 00 00 00 00 00 0B 00 00 00 ; .............
e500h: 00 00 00 00 1E 10 00 00 01 00 00 00 44 00 00 00 ; ............D
e510h: 49 72 61 71 2D 20 49 54 53 20 49 4E 46 52 41 53 ; Iraq- ITS INF
e520h: 54 52 55 43 54 55 52 45 20 4F 46 20 43 4F 4E 43 ; TRUCTURE OF C
e530h: 45 41 4C 4D 45 4E 54 2C 20 44 45 43 45 50 54 49 ; EALMENT, DECE
e540h: 4F 4E 20 41 4E 44 20 49 4E 54 49 4D 49 44 41 54 ; ON AND INTIMI
e550h: 49 4F 4E 00 0C 10 00 00 02 00 00 00 1E 00 00 00 ; ION..........
e560h: 06 00 00 00 54 69 74 6C 65 00 03 00 00 00 01 00 ; ....Title....
e570h: 00 00 00 00 98 00 00 00 03 00 00 00 00 00 00 00 ; ....˜........
e580h: 20 00 00 00 01 00 00 00 36 00 00 00 02 00 00 00 ;  .......6....
e590h: 3E 00 00 00 01 00 00 00 02 00 00 00 0A 00 00 00 ; >............
e5a0h: 5F 50 49 44 5F 47 55 49 44 00 02 00 00 00 E4 04 ; _PID_GUID....
e5b0h: 00 00 41 00 00 00 4E 00 00 00 7B 00 35 00 45 00 ; ..A...N...{.5
e5c0h: 32 00 43 00 32 00 45 00 36 00 43 00 2D 00 38 00 ; 2.C.2.E.6.C.-
e5d0h: 41 00 31 00 36 00 2D 00 34 00 36 00 46 00 33 00 ; A.1.6.-.4.6.F
e5e0h: 2D 00 38 00 38 00 34 00 33 00 2D 00 37 00 46 00 ; -.8.8.4.3.-.7
e5f0h: 37 00 33 00 39 00 46 00 41 00 31 00 32 00 39 00 ; 7.3.9.F.A.1.2
e600h: 30 00 31 00 7D 00 00 00 00 00 00 00 00 00 00 00 ; 0.1.}........
```



```
c350h: 00 1A 00 07 00 1A 00 07 00 1A 00 07 00 1A 00 07 ; ............
c360h: 00 1A 00 07 00 07 00 02 00 07 00 1A 00 07 00 FF ; ............
c370h: FF 14 00 00 00 05 00 63 00 69 00 63 00 32 00 32 ; ÿ.....c.i.c.
c380h: 00 4A 00 43 00 3A 00 5C 00 44 00 4F 00 43 00 55 ; .J.C.:.\.D.O.
c390h: 00 4D 00 45 00 7E 00 31 00 5C 00 70 00 68 00 61 ; .M.E.~.1.\.p.
c3a0h: 00 6D 00 69 00 6C 00 6C 00 5C 00 4C 00 4F 00 43 ; .m.i.l.l.\.L.
c3b0h: 00 41 00 4C 00 53 00 7E 00 31 00 5C 00 54 00 65 ; .A.L.S.~.1.\.
c3c0h: 00 6D 00 70 00 5C 00 41 00 75 00 74 00 6F 00 52 ; .m.p.\.A.u.t.
c3d0h: 00 65 00 63 00 6F 00 76 00 65 00 72 00 79 00 20 ; .e.c.o.v.e.r.
c3e0h: 00 73 00 61 00 76 00 65 00 20 00 6F 00 66 00 20 ; .s.a.v.e. .o.
c3f0h: 00 49 00 72 00 61 00 71 00 20 00 2D 00 20 00 73 ; .I.r.a.q. .-.
c400h: 00 65 00 63 00 75 00 72 00 69 00 74 00 79 00 2E ; .e.c.u.r.i.t.
c410h: 00 61 00 73 00 64 00 05 00 63 00 69 00 63 00 32 ; .a.s.d...c.i.
c420h: 00 32 00 4A 00 43 00 3A 00 5C 00 44 00 4F 00 43 ; .2.J.C.:.\.D.
c430h: 00 55 00 4D 00 45 00 7E 00 31 00 5C 00 70 00 68 ; .U.M.E.~.1.\.
c440h: 00 61 00 6D 00 69 00 6C 00 6C 00 5C 00 4C 00 4F ; .a.m.i.l.l.\.
c450h: 00 43 00 41 00 4C 00 53 00 7E 00 31 00 5C 00 54 ; .C.A.L.S.~.1.
c460h: 00 65 00 6D 00 70 00 5C 00 41 00 75 00 74 00 6F ; .e.m.p.\.A.u.
c470h: 00 52 00 65 00 63 00 6F 00 76 00 65 00 72 00 79 ; .R.e.c.o.v.e.
c480h: 00 20 00 73 00 61 00 76 00 65 00 20 00 6F 00 66 ; . .s.a.v.e. .
c490h: 00 20 00 49 00 72 00 61 00 71 00 20 00 2D 00 20 ; . .I.r.a.q. .
c4a0h: 00 73 00 65 00 63 00 75 00 72 00 69 00 74 00 79 ; .s.e.c.u.r.i.
c4b0h: 00 2E 00 61 00 73 00 64 00 05 00 63 00 69 00 63 ; ...a.s.d...c.
c4c0h: 00 32 00 32 00 4A 00 43 00 3A 00 5C 00 44 00 4F ; .2.2.J.C.:.\.
```
]

Planning phase

- Very essential phase too, its goal is
  - to plan the general structure of maneuver,
  - to generate the required forces,
  - to coordinate the different attacks bricks,
  - to coordinate with the conventional pieces of the attack,
  - to integrate the conduct of maneuver in the early phase:
    - Management of the unexpected.
    - Choice of variants.
- Actual work of a B5 HQ.
  - The part strictly devoted to the cyberattack is managed in the context of the global effect to achieve.
- NATO InfoOps Vision translated into *Black InfoOps.*

Conduct phase

- It is the proper operational part.
- It is NOT a separate part BUT it always support another part of the action course.
  - Improvising is forbidden!
- Take part to the intelligence gathering.

Conduct phase (2)

- In the context of cyberattack, apply the partionning approach.
  - Prevent any coherent and global view of the intended target.
  - Maintain the attacker's anonimity.
- Two kind of forces:
  - Supply or support forces.
  - Chock forces (≅ infantry/cavalry).
- Consider the same approach/techniques as in Infantry/Cavalry.
- Use spoofing techniques or incriminate third parties.

A few exemples of « bricks of attacks ».

Cases studies

- Eric Filiol – Frédéric Raynal (2009) « Cyberguerre : de l'attaque du bunker à l'attaque dans la profondeur ». Revue de Défense Nationale, mars 2009.
  - Example of cyberattacks against a military operation.

- Eric Filiol (2009) *Operational aspects of cyberwarfare or cyber-terrorist attacks; what a truly devastating attack could do?* ECIW 2009, 8th European Conference on Information Warfare and Security, Military Academy, Lisbon, Portugal, 6-7 July 2009.
  - Example of cyberattacks against civilian targets.

General Strategy

- A systematic attack against a state or its national infrastructures is generally performed in three main steps:
  - Step 1: desorganize or disrupt transportation networks.
    - Railway, air control, road light traffic, communication networks…
  - Step 2: attacks against the financial systems and against the communications networks.
    - Stock market exchange, telephone networks…
  - Step 3: attacks against resources and services distribution.
    - Water supply, gas distribution, nuclear plants, electricity…
- Basically target anything which is managed by or depends on one or more ICS.
  - In other word quite everything!
- Everything elese is collapsing (domino effect).
- Target all infrastructure components!

A few « bricks of attacks ».

- Attacks against people
  - Attack of the home computer of the union leader of big company (by putting sensitive data into his computer).
  - Denounciation, press is alerted (by attackers).
  - Strikes are triggered.
  - False proofs are put that show that the company staff is involved.
  - Strikes are becoming worse, demonstrations, blocking of the plant...

LE MONDE | 24.10.03 | 13h21

Comment deux pères de familles britanniques ont vu leurs vies brisées par l'intrusion de virus dissimulant des photos pédophiles dans leur ordinateur.

Jusqu'à l'automne 2000, Karl Schofield, 36 ans, originaire de Reading, près de Londres, se considérait comme un homme comblé. Consultant pour des grandes entreprises de télécoms, il gagnait beaucoup d'argent et dirigeait sa propre société. Il avait travaillé aux Pays-Bas, en Arabie saoudite, puis à Chypre, où il avait rencontré sa seconde épouse, une Russe de 23 ans. Depuis peu, le couple habitait Reading, dans une grande maison où vivaient également les parents de Karl : *"C'était la belle vie, parfois nous allions passer le week-end à New York... C'est bien fini tout ça."*

Un matin d'octobre 2000, alors qu'il vient d'arriver au bureau, sa femme l'appelle : des policiers sont chez eux et demandent à le voir. Karl Schofield rentre aussitôt, pour trouver sept enquêteurs dans son salon. *"Ils m'ont posé des tas de questions sur mon PC de bureau, mon portable, mes CD-ROM, mes mots de passe,* se souvient-il. *Je leur ai dit que j'avais peut-être des copies pirates de jeux vidéo, mais je ne voyais pas où ils voulaient en venir."* Ils lui annoncent alors qu'ils cherchent des images pédophiles : *"Je ne les ai pas crus, ça me semblait délirant. Ma femme a ri, pour elle c'était forcément une erreur. Elle me connaît bien de ce côté-là."* La perquisition ne donne rien, mais les policiers emportent les ordinateurs.

Quelques semaines plus tard, Karl Schofield est convoqué au commissariat. Là, il apprend que les experts de la police ont trouvé sur son portable quatorze photos pédophiles. *"J'ai nié*

A few « bricks of attacks » (2)

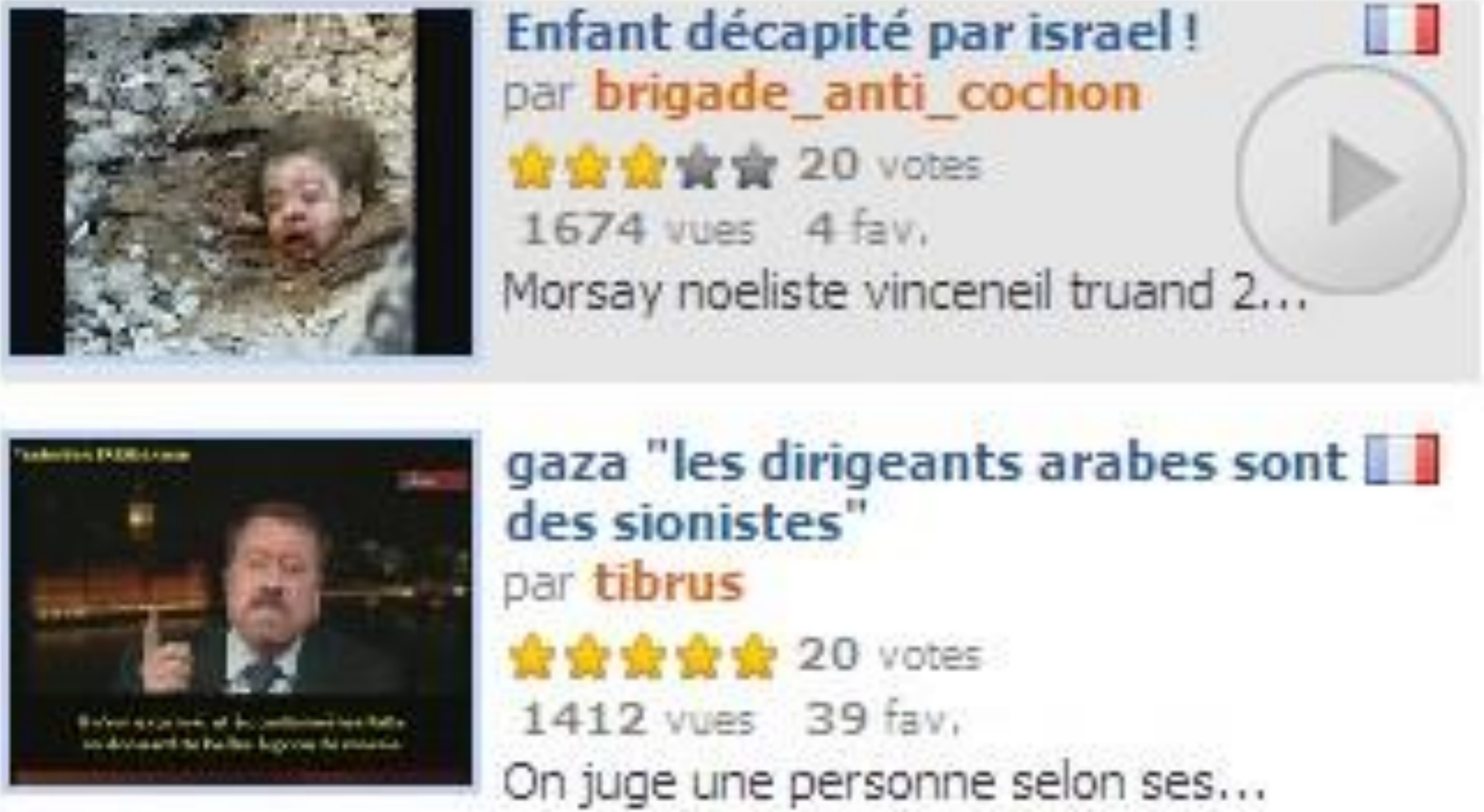
- Attack against a small high technology, innovative company (start up) in order to make it disappear or to buy it.
- Attack far ahead to the desired effect.
  - Attack of the company CEO and development engineers’s computers.
  - Deposit of data accrediting the use of sofware piracy and software counterfeiting.
  - Denounciation + alert the media/press.
  - Lawsuit with respect to the LCEN (Penal code + Intellectual property Code).
  - Prosecution.
  - Financial exhaustion of the target company by a lengthy legal process.
  - Bankruptcy or the target company!

A few « bricks of attacks » (2bis)

- Attacks against persons seek to put off for a long period any person who has a critical role in the management of a critical infrastructure (particularly during crisis).
  - Target the home computer.
  - Target the mobile computers.
- The timing of these attacks must be carefully planned and coordinated.
- In this context, the concept of bunker remains illusory.

A few « bricks of attacks » (3)

- Triggering riots or clashes (blocking communication routes or areas).
- Deposit racist, violent, community video files on very visited websites.
- VinceNail vs Morsay case (since 2008 Q4).
  - Insulting/racist videos uploaded on *DailyMotion*
  - Morsay’s (violent) answer.
  - Vince’s (violent) counter attack.
  - …
  - Limited riots in sensitive suburb areas.
- Exploit the news.
- A large number of cases.



Enfant décapité par israel !
par **brigade_anti_cochon**
★★★☆☆ 20 votes
1674 vues 4 fav.
Morsay noeliste vinceneil truand 2...

gaza "les dirigeants arabes sont des sionistes"
par **tibrus**
★★★★★ 20 votes
1412 vues 39 fav.
On juge une personne selon ses...

FAA Confirms Hack Attack

Kevin Poulsen, SecurityFocus 2002-04-25

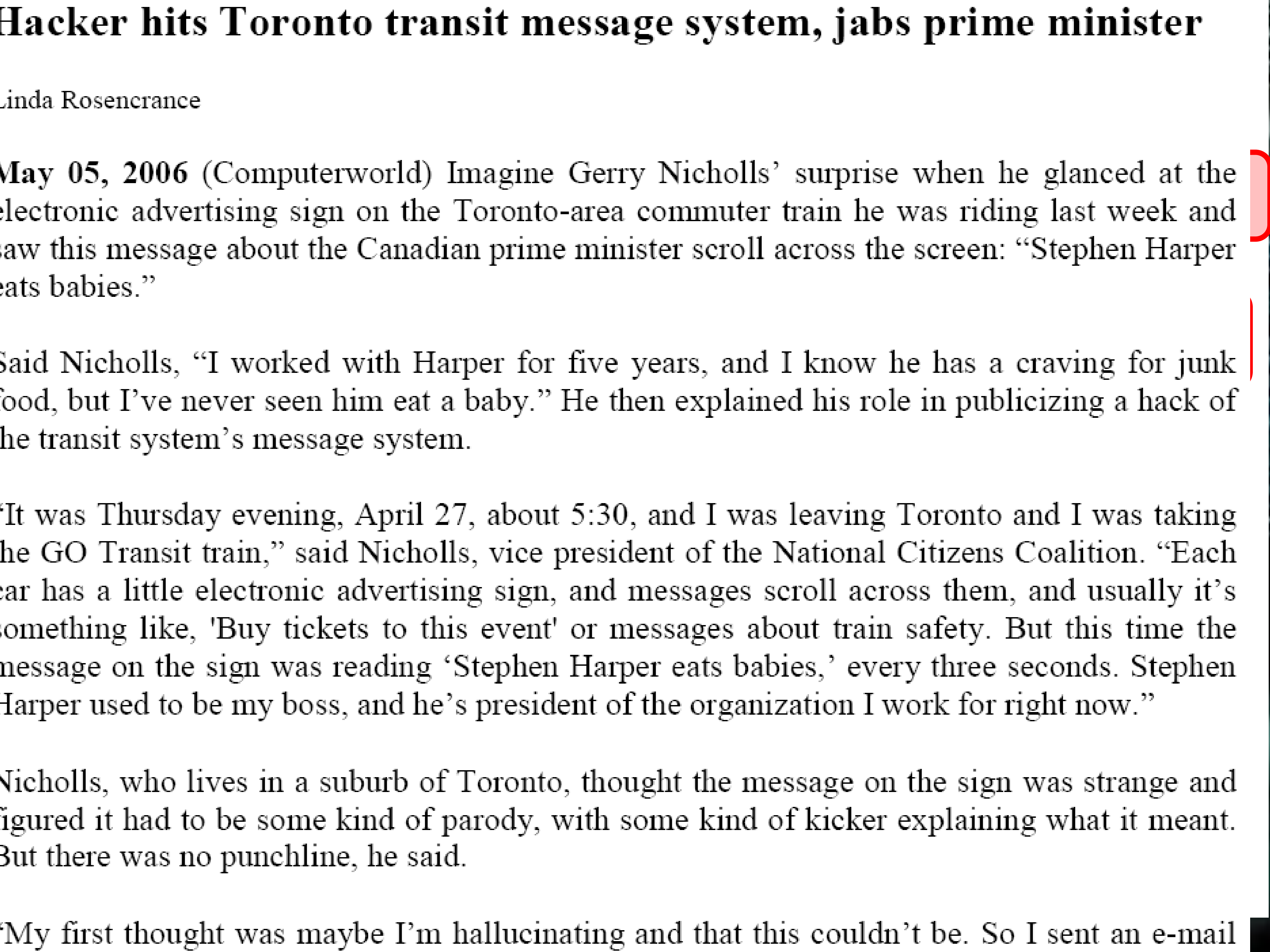
Self-styled patriotic intruders deface a government airline securit site and download a detailed screener database. Their proclaime mission: saving the U.S. from foreign cyber terrorists.

Hackers were able to penetrate a Federal Aviation Administration system earlie this week and download unpublished information on airport passenger screenin activities, federal officials confirmed Thursday.

Styling themselves "The Deceptive Duo," the hackers on Wednesday publicl defaced an FAA server used by what was the administration's Civil Aviatio Security organization, which until recently was responsible for supervisin passenger screening at U.S. airports. There, the intruders posted a missio statement vowing to expose America's poor state of cyber security for the goo of the nation.

"Tighten the security before a foreign attack forces you to," the Duo extolled. "A a time like this, we cannot risk the possibility of compromise by a foreig enemy."

At the bottom of the page, the defacers included a screen-shot showing a portio of a Microsoft Access database, with each row displaying the three-letter code fo



Hacker hits Toronto transit message system, jabs prime minister

inda Rosencrance

May 05, 2006 (Computerworld) Imagine Gerry Nicholls' surprise when he glanced at the lectronic advertising sign on the Toronto-area commuter train he was riding last week and aw this message about the Canadian prime minister scroll across the screen: "Stephen Harper ats babies."

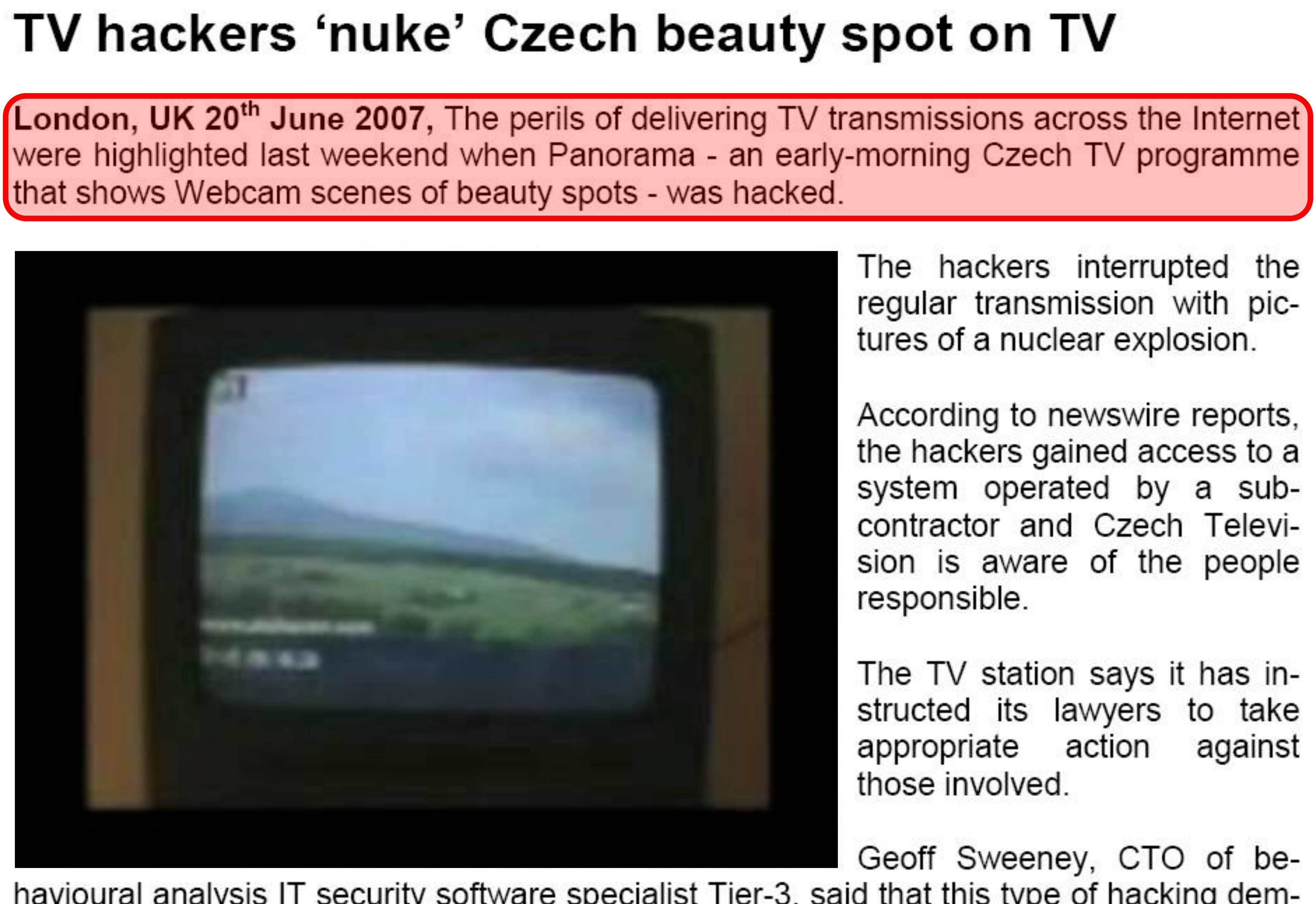
Said Nicholls, "I worked with Harper for five years, and I know he has a craving for junk ood, but I've never seen him eat a baby." He then explained his role in publicizing a hack of he transit system's message system.

'It was Thursday evening, April 27, about 5:30, and I was leaving Toronto and I was taking he GO Transit train," said Nicholls, vice president of the National Citizens Coalition. "Each ar has a little electronic advertising sign, and messages scroll across them, and usually it's omething like, 'Buy tickets to this event' or messages about train safety. But this time the nessage on the sign was reading 'Stephen Harper eats babies,' every three seconds. Stephen Harper used to be my boss, and he's president of the organization I work for right now."

Nicholls, who lives in a suburb of Toronto, thought the message on the sign was strange and igured it had to be some kind of parody, with some kind of kicker explaining what it meant. But there was no punchline, he said.

'My first thought was maybe I'm hallucinating and that this couldn't be. So I sent an e-mail

Other « attack bricks » (3)



TV hackers ‘nuke’ Czech beauty spot on TV

London, UK 20th June 2007, The perils of delivering TV transmissions across the Internet were highlighted last weekend when Panorama - an early-morning Czech TV programme that shows Webcam scenes of beauty spots - was hacked.

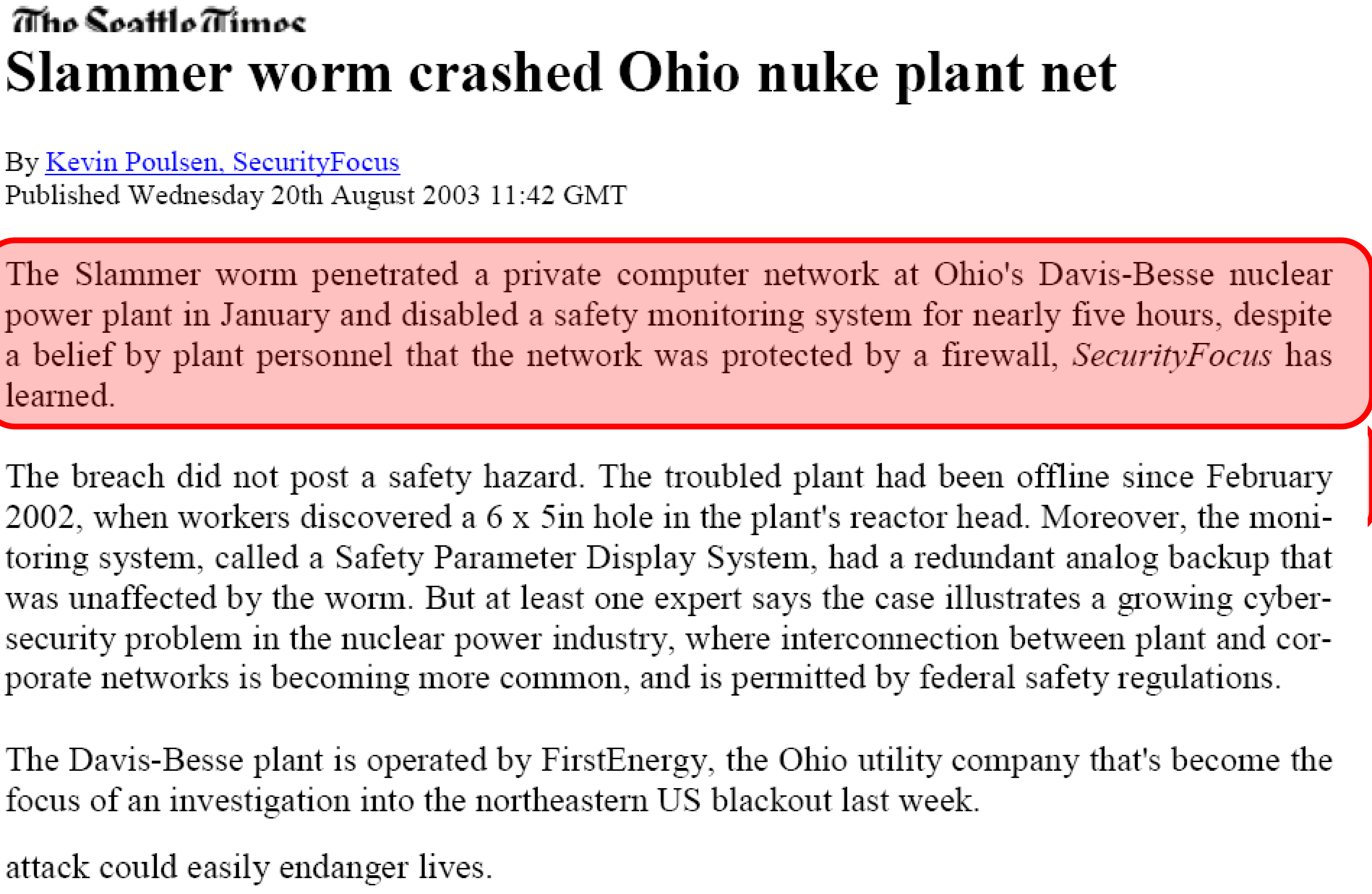
The hackers interrupted the regular transmission with pictures of a nuclear explosion.

According to newswire reports, the hackers gained access to a system operated by a sub-contractor and Czech Television is aware of the people responsible.

The TV station says it has instructed its lawyers to take appropriate action against those involved.

Geoff Sweeney, CTO of behavioural analysis IT security software specialist Tier-3, said that this type of hacking dem-

Autres « briques de base » (4)



The Seattle Times

Slammer worm crashed Ohio nuke plant net

By Kevin Poulsen, SecurityFocus
Published Wednesday 20th August 2003 11:42 GMT

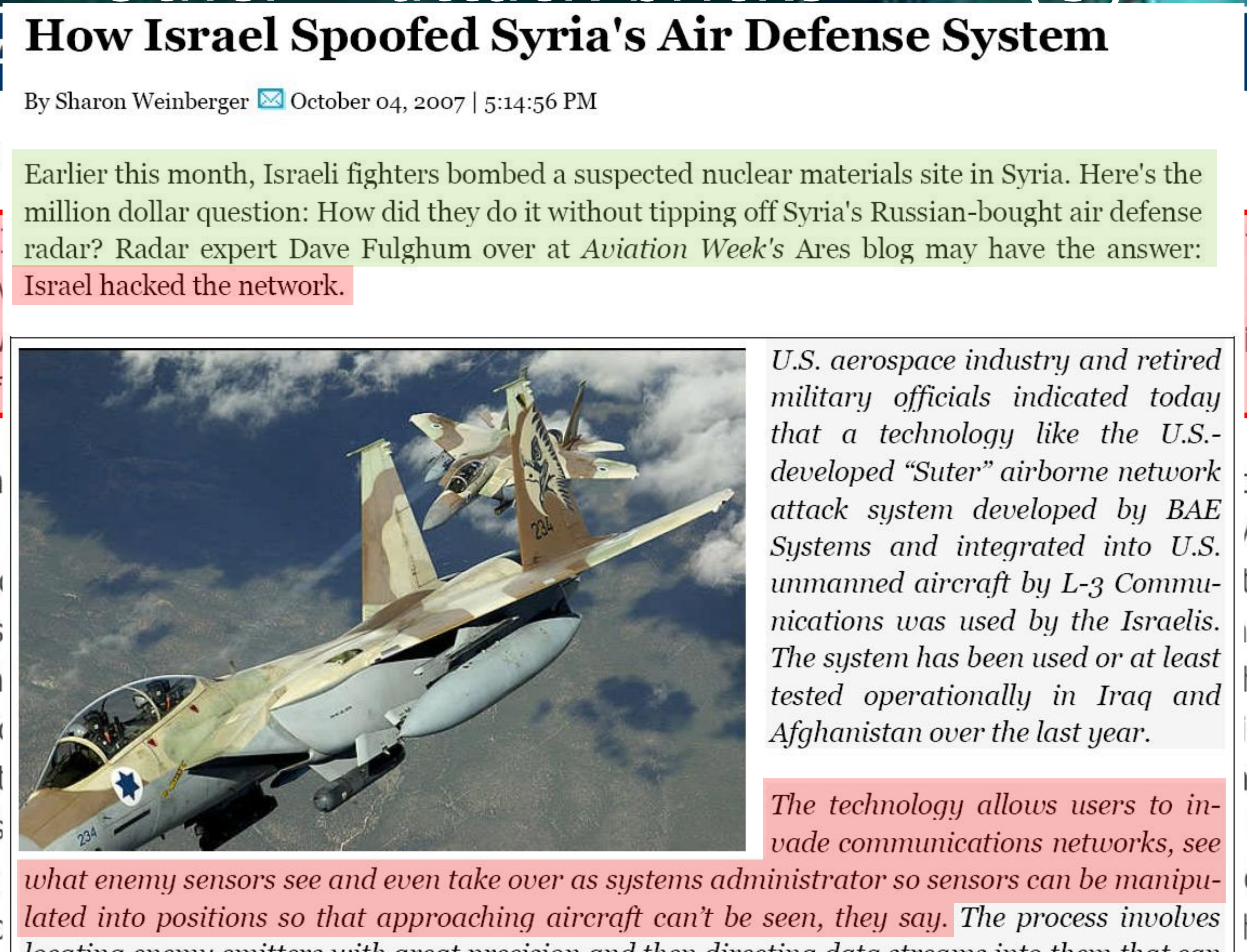
The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall, *SecurityFocus* has learned.

The breach did not post a safety hazard. The troubled plant had been offline since February 2002, when workers discovered a 6 x 5in hole in the plant's reactor head. Moreover, the monitoring system, called a Safety Parameter Display System, had a redundant analog backup that was unaffected by the worm. But at least one expert says the case illustrates a growing cybersecurity problem in the nuclear power industry, where interconnection between plant and corporate networks is becoming more common, and is permitted by federal safety regulations.

The Davis-Besse plant is operated by FirstEnergy, the Ohio utility company that's become the focus of an investigation into the northeastern US blackout last week.

attack could easily endanger lives.

Other « attack bricks » (5)



How Israel Spoofed Syria's Air Defense System

By Sharon Weinberger October 04, 2007 | 5:14:56 PM

Earlier this month, Israeli fighters bombed a suspected nuclear materials site in Syria. Here's the million dollar question: How did they do it without tipping off Syria's Russian-bought air defense radar? Radar expert Dave Fulghum over at *Aviation Week's* Ares blog may have the answer: Israel hacked the network.

U.S. aerospace industry and retired military officials indicated today that a technology like the U.S.-developed "Suter" airborne network attack system developed by BAE Systems and integrated into U.S. unmanned aircraft by L-3 Communications was used by the Israelis. The system has been used or at least tested operationally in Iraq and Afghanistan over the last year.

The technology allows users to invade communications networks, see what enemy sensors see and even take over as systems administrator so sensors can be manipulated into positions so that approaching aircraft can't be seen, they say. The process involves locating enemy emitters with great precision and then directing data streams into them that can

Other « attack bricks » (6)

- These cases can be systematized and coordinated for a devastating effect.
- Combination and coordination of these bricks at the planning stage.
  - Imagination and tactical richness have the power!
- Importance of the management of the unexpected and of the variants planning.
  - Ability to change/modify the mission in action.
- The technical vision alone (hackers, pirates) is insufficient.
  - Requires a real strategic and tactical thinking (doctrine).

Conclusion

How to protect ourself?

- First of all, is it possible to protect ourself easily?
  - No if we accept our dependence on ICS as inevitable.
  - That is where lies the actual difference between Estonia and Georgia !
- The key factor is to exploit the human component totally and without any rectriction!
- Exploit and generalize the InfoOps power as well as the classical Humint techniques.

How to protect ourself? (2)

- Waht about the ability to resist when using non controlled systems (hardware and software, standards…):
  - Operating systems.
  - Security software.
  - Cryptologic concepts…
- Protection is a matter of digital sovereignty first!
  - It is more a concepts/standards issue than a product issue.

« The power of a country lies in its ability to impose standards »

Bernard Carayon (MP) – SSTIC 2004

How to protect ourself? (3)

- Economic revolution. It is critical to
  - Make critical company come back to National soil as well as the national critical resources.
  - To forbid subcontracting with respect to the national scientific/technical critical resources:
    - Data centers
    - Oversight and supervision centers.
    - …
- Cultural revolution:
  - Create a culture of security and professional discretion, as a priority among policy-makers…
  - … as well as the notion of economic patriotrism!

Thanks for your attention!

Questions … and answers!