# Cybercrime 2.0

## Addressing Security Issues in Cyberspace

International Conference on Technological Readiness for Innovation-based Competitiveness - Palais des Nations, Geneva - 30th June 2009

stéphane koch
internet & information strategy advisor
online reputation management



## Is cybercrime a threat for ecomomy...?

### 100,000 sites deleted in hack, software company boss commits suicide

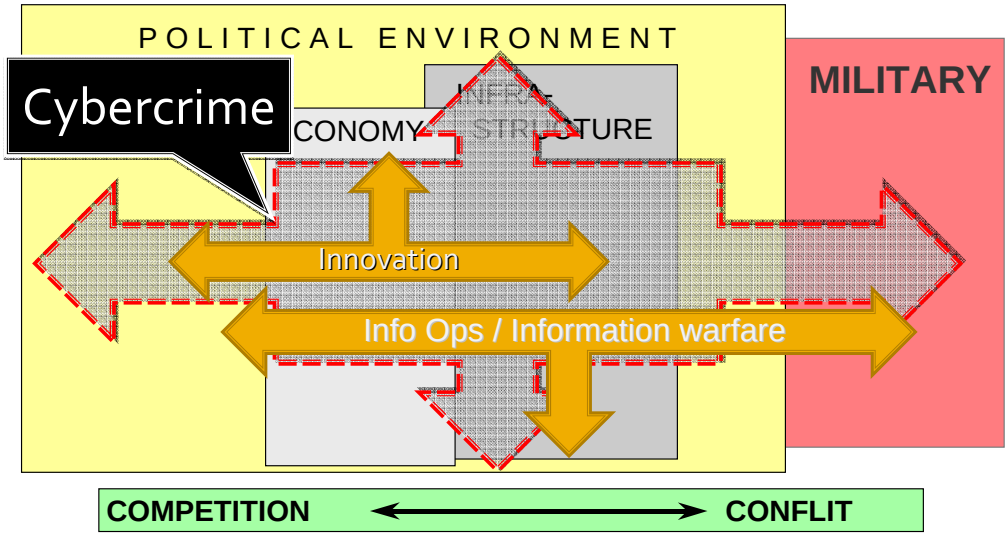
"The boss of Indian software firm LxLabs was found dead in a suspected suicide on Monday.

Reports of the death of K T Ligesh, 32, come in the wake of the exploitation of a critical vulnerability in HyperVM, a virtualization application made by LXLabs, to wipe out data on 100,000 sites hosted by the UK web hosting firm VAserv.

The effect of his death on the development of updated software by LxLabs is unknown at time of writing."

Read more: http://www.theregister.co.uk/2009/06/09/lxlabs_funder_death/

## Context: The economy & information security & cybercrime environment




Source: Ir. H.A.M. (Eric) Luiijf - Info Ops R&D programma



## FBI worried as *DoD* sold *counterfeit Cisco* gears


Source: <http://www.usedcisco.com/press-my-esm_used_cisco_identifying_fake_chisco.aspx>

## Definition of some of the actors (state and non state)



- Hacktivist (could be simple civilians as well)
  *Using Networks to promote political motivations*
- Hackers (white hat / ethical)
  *Social & personal motivations*
- Cyber mercenary
  *Using their skills to earn money without moral or legal concerns*
- Cyber terrorist
  *Using Networks to spread fear, to recruits members, to get funds, to target, to prepare action…*
- Cyber criminals
  *Selling goods as a B2B market of illegal stuff (CC, Botnets, logins)*
- Intelligence services
  *Using proxy behavior to get competitive advantage*



## The asymetry of the conflict



- I can be in Switzerland attacking some computers or critical infrastructures in another country, while making believe that I'm in a third one…
- Each country, especially every democracy, could be a host for cybercrime or/and cyber-mercenary.
- Each citizen can become involve in a fraud scheme without to be aware of that (eg. botnets)
- Each cyber-mercenary could be autonomous
- Each cyber-mercenary could be a civilian among civilians

## The asymetry of the society



- The asymmetry of the knowledge
  *The knowledge of computing and code will make the difference in the terms of the capability to access to the systems. The way to assess that knowledge (for governments and private sector) is very difficult (because security is dynamic and you need knowledge to assess knowledge) this difficulty create a gap between the reality and the perception*
- The asymmetry of the model
  *Governments and private sector have to work with "employees", while the underground community (cybercrime, hacktivists, cyber-mercenary, hackers) can work in collaborative intelligence and sharing information knowledge network*



## The asymetry of the society



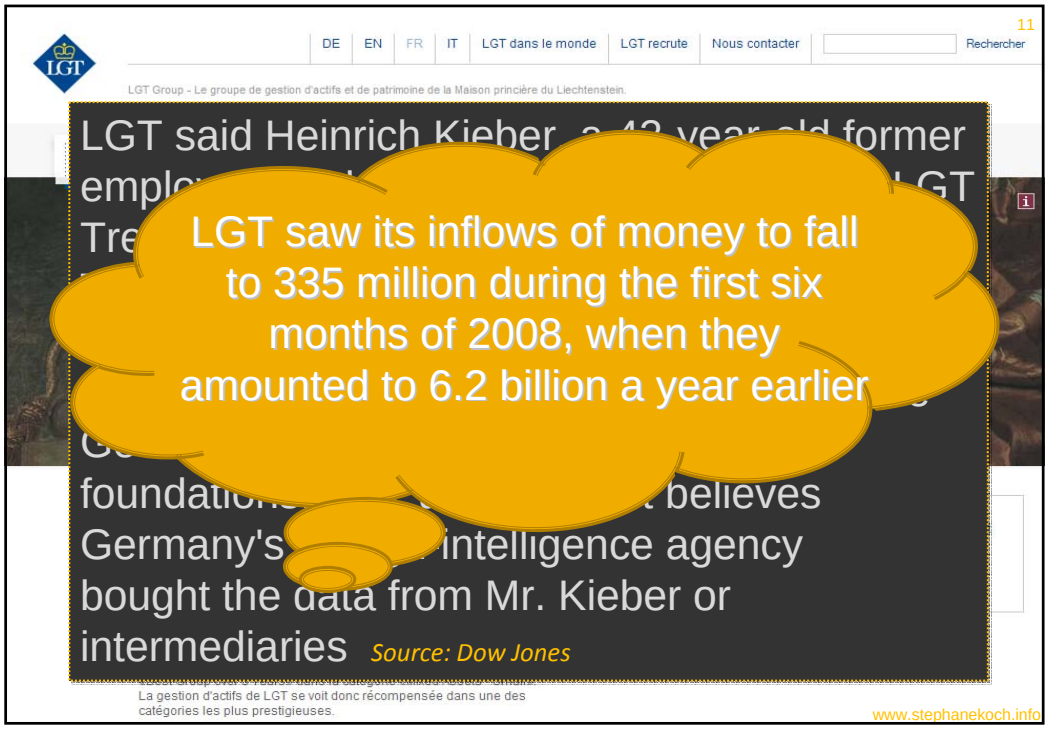
- The asymmetry of the economy
  *The actual economic situation (economy – unemployment - restructuration), and the gap in term of incomes between some technically educate countries and some "riche" ones create a big potential of "ready to hire" of very skilled human resources for the cybercrime market*

## The cybercrime education


- Knowledge is everywhere on the Net, everything is available to get trained

## Using criminal behaviour to get competitive advantages

The Net is a really nice background for cover operations or proxy attack. Intelligence services can play to appear as cybercriminals or whatever they want to looks like… But, cybercriminal can play as well to appear as intelligence services.. ;)




## Awarness & Information security are the keys

- *We have to change our culture (information society)…*
- *We have to take security not as an « access rights problem » but rather like the blood system of the human body.*
- *Complexity is the rule !*
- *Like with the human, when we diagnostic a disease we have to care it ASAP. Security obscurantism is not a solution*

# Available ressources for the cybercriminals

In add: The Cybercrime market can bring assistance and munitions to the cyber warrior & cyber terrorism.

They can get :

- Attack tools (DDoS, virus, scripts, Oday),
- Fake identity (eg Social security numbers, passports),
- Way to get money (eg, credit cards, click fraud),
- Way to damage communications (eg Botnets, malwares).



# Cybercrime market is an open market


- You can order what you want, you can as well ask for custom needs (specific scripts, specific malware – which are not going to be detected by security programs)

Source image : http://www.wired.com/threatlevel/2008/11/the-nets-underg/

15

## Cybercrime market is an open market

| Attack Kit Type | Average Price | Price Range |
|---|---|---|
| Botnet | $225 | $150–$300 |
| Autorooter | $70 | $40–$100 |
| SQL injection tools | $63 | $15–$150 |
| Shopadmin exploiter | $33 | $20–$45 |
| RFI scanner | $26 | $5–$100 |
| LFI scanner | $23 | $15–$30 |
| XSS scanner | $20 | $10–$30 |

Source image : http://www.wired.com/threatlevel/2008/11/the-nets-underg/

16

## Cybercrime market is an open market

| Rank for Sale | Rank Requested | Goods and Services | Percentage for Sale | Percentage Requested | Range of Prices |
|---|---|---|---|---|---|
| 1 | 1 | Bank account credentials | 18% | 14% | $10–$1,000 |
| 2 | 2 | Credit cards with CVV2 numbers | 16% | 13% | $0.50–$12 |
| 3 | 5 | Credit cards | 13% | 8% | $0.10–$25 |
| 4 | 6 | Email addresses | 6% | 7% | $0.30/MB–$40/MB |
| 5 | 14 | Email passwords | 6% | 2% | $4–$30 |
| 6 | 3 | Full identities | 5% | 9% | $0.90–$25 |
| 7 | 4 | Cash-out services | 5% | 8% | 8%–50% of total value |
| 8 | 12 | Proxies | 4% | 3% | $0.30–$20 |
| 9 | 8 | Scams | 3% | 6% | $2.50–$100/week for hosting; $5–$20 for design |
| 10 | 7 | Mailers | 3% | 6% | $1–$25 |

Source image : http://www.wired.com/threatlevel/2008/11/the-nets-underg/

# The Underground Ecomomy

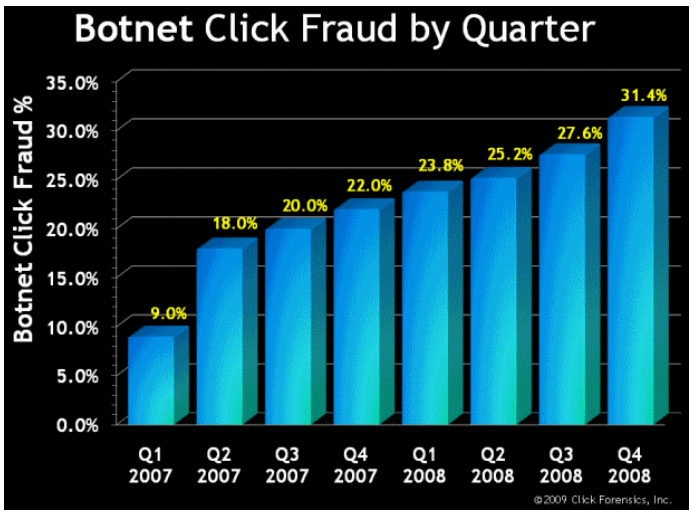

**Job description :**

- Trojan creators – high quality malicious code writers wanted
- Web exploiters – talented infectors sought
- Exploit experts - tech geeks, programmers and researchers required
- Traffic sellers - confident sales people required to market traffic
- Fraudsters – ambitious, well connected crooks required to steal data
- Outsourced rogue hosting companies – industry knowledge essential, must appear legitimate

Source image : http://www.economist.com/daily/chartgallery/displaystory.cfm?story_id=12670461



# Fundraising : Botnets increasingly used to perpetrate click fraud




- Estimation of the click fraud's money lost : more than 1 billion in 2009

Source image : Click Forensics & http://news.cnet.com/digital-media/?keyword=click+fraud

## Click fraud



Finjan Malicious Code Research Center:

- We found that 1.8 million unique users were redirected to the rogue Anti-Virus software during 16 consecutive days. Members of the affiliate network are rewarded for each successful redirection with 9.6 cents "a piece", which totals $172,000. If we calculate it per day, it translates to a whopping **$10,800 for one day of criminal activity!** Based on a normal workweek, this would put our criminals in the **$2M+ annual income bracket**.



## Critical infrastructures & SCADA

(Supervisory Control And Data Acquisition)

*"The problem is not to protect only domestic Critical Infrastructures, but is to protect also all the way the information need to take to go through (eg. Undersea cables)"*

21

## Damaged Critical Infrastructures have impact on economy

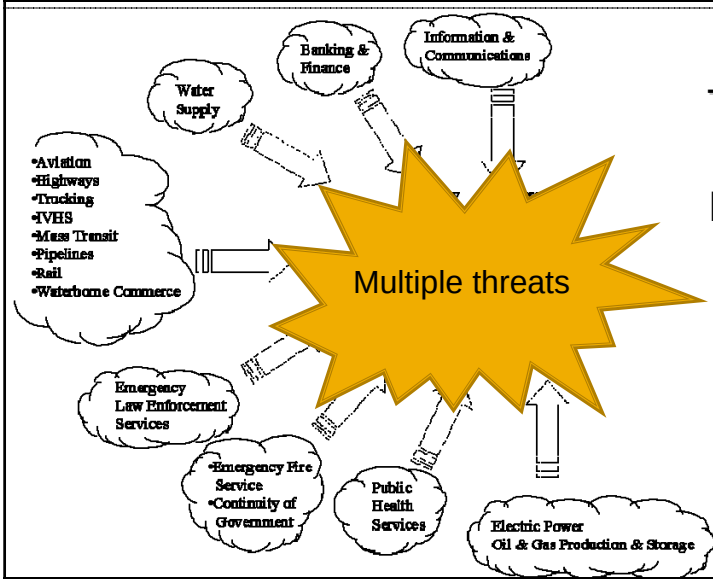
It's easy to create confusion in any city today:

- Optical fibers are usually easy to access by the basements or by the sewers.
- SCADA is a weak protocol and is not always well dissociated from the network (internet).
- Disrupting energy like power supply could create chain reaction.
- *It's quite easy to create big loss in economy by acting in a such way*

Source image : Source: Joe St Sauver, Ph.D. www.uoregon.edu/~joe/highrisk/

22

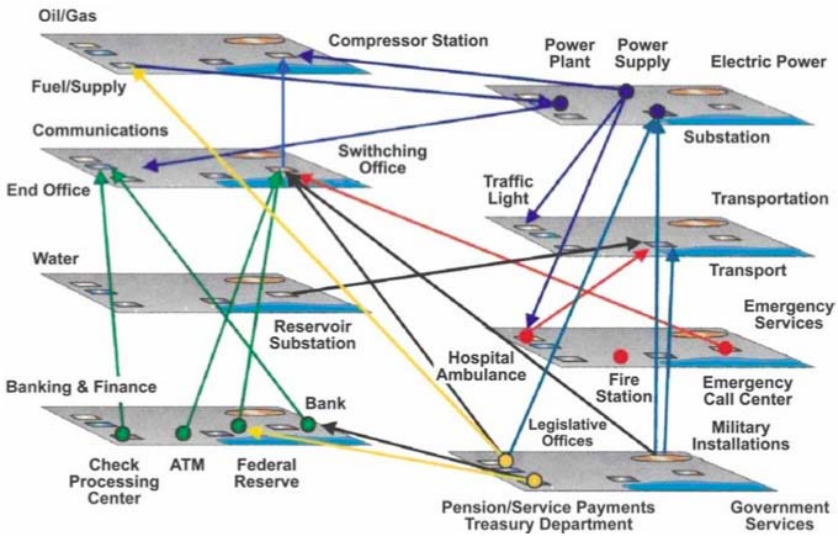
## SCADA (Supervisory Control And Data Acquisition)




The Supervisory Control And Data Acquisition (SCADA) can be use to access to lot of facilities

www.stephanekoch.info

## Critical Infrastructure Interlocks




Source image : Source: Joe St Sauver, Ph.D. www.uoregon.edu/~joe/highrisk/

## What can we do..?

Cyber security is based on knowledge…
…Knowledge is everywhere and available to who want to get it (good side or bad side of the force) and we cannot fight this knowledge with laws, we have to fight knowledge with knowledge !

## First : Raising Global Awarness

Like we cannot dissociate the venous system and the blood of the body, we cannot dissociate "human" ; "technology" and "security"

Source image : http://www.liquidmatrix.org/blog/2008/08/30/waterisac-document-leak-cover-up-failed/



## Lauching preventive structures

Create a think tank or weak alert signals network with

- Hackers (ethical one)
- University (research)
- Private sector and government and CERT (CERTs have to collaborate across states, like a neuronal network)

That structure will dynamically have to

- Preventively identify potentials targets and make its difficult to get.
- Use as possible data mining of web queries to try to prevent or identify the evolution of the situation

## Fighting obscurantism

Raising awareness

- We don't born "digital native" regardless of when it arises… So, educate users and politicians, and TEACHER !!!
- Communicate security gap/holes transparently
- Security is dynamic, so too much trust is counterproductive…;)





Contact:

stéphane koch
internet & information strategy advisor
online reputation management

Website: www.intelligentzia.net
Rue des Corps-Saints 4
CH-1201 Geneva

Fax: +41 22 731 6007
Mobile: +41 79 607 57 33
Skype: stephanekoch
FaceBook : www.facebookme.in
Twitter: www.twitter.com/stephanekoch
LinkeDin: www.linkedin.com/in/stephanekoch
My location: http://tinyurl.com/intelligentzia-net
Email: skoch@intelligentzia.ch