MINISTRY OF TECHNOLOGIES
OF INFORMATION

ITU International Telecommunication Union

N.A.C.S
National Agency for Computer Security

CERT/T.CC
(Tunisian Coordination Center)

Pr Nabil SAHLI

National Agency for Computer Security, CEO
Ministry of Technologies of Communication

n.sahli@ansi.tn

TUNISIA

world summit
on the information society
Geneva 2003 - Tunis 2005

PLAN

-Fast Overview about Tunisian strategy in Security of Information systems (Cyber security)

-Presentation of CERT/TCC Services & Activities :

- As a CSIRT
- As an ISAC
- As a "regular" CERT

- Some Particularities, of Less-Developing countries

(+ "Garbage reflexion")

Tunisian experience and strategy in Security of IS (Fast Overview)

Some History :

❑ **<u>1999 :</u>** Launch of a **<u>UNIT</u>**, specialized in IT Security (Secretary of state for Informatics) **<u>:</u>**

Objective :

- Awareness (Decision Makers and Technical staff).
- Monitoring the protection of highly critical national applications and infrastructures.
- Technological and **Impact** follows-Up.

❑ From **<u>End 2002</u>** (certification of the role of IT security as a pillar of the « Information Society ») **<u>:</u>**

➢ Establishment of a **strategy** and of a **National Plan in IT Security**

Tuned and refined (national survey, by end 2003) : priorities, volume of actions, needed supporting tools, ..

✓ 2004 : Promulgation of an “original” **law related to IT Security** (Law N° 2004-5, Feb 2004) :

- **Obligation** for national companies (public and some private) to do **Periodic (annual) Risk Assessment of their IS.**
  & Organization of the field of risk assessment (Should be made by **certified auditors from the private sector & definition of its object**),

- **Obligation to declare** (to the National Agency for Computer Security), any Incident (Viral, mass hacking attacks, ..)
  that could affect **other IS**, with guarantee of **confidentiality**, by law.

- Creation of the **National Agency for Computer Security** & Definition of its missions.
  (under the **Ministry of Technologies of communications**)

✓ Launch of the CERT/T.C.C (CERT/Tunisian Coordination Center), inside the National Agency for Computer Security

Tasks of the National Agency for Computer Security (N.A.C.S)

(Accordingly to the LAW on IT security)

Seeing to the **implementation** of the ***National policy and general strategy*** in the field of IT security

➢ Monitoring the implementation of **security plans and programs** in the public sector

(with the **exception** of applications that are proper to **National Defense and National Security**)

& The **Coordination** among stakeholders in the field of IT Security;

➢ Promulgate Best Practices, Methods **and regulations** in the field.

➢ Fostering the **development of national solutions** in the field of computer security and promoting such solutions in accordance with the National **Priorities** ,

➢ Consolidate **training and re-training** in the field of computer security and insure technological Follows-Up in this field;

And Follows-Up of the execution and of the execution of the recommendations of risk assessment operations

Other Tunisian legislative Measures, related to Cyber-security :

Ø Law on protection of **Privacy and Personal data (Law n° 2004-63)**
Ø Law on **Electronic Signature and e-commerce (Law N°** 2000-83 **)**
Ø Law **Against Cyber-Crimes (Law N° 99-89)**
Ø **Laws on consumer protection and** Intellectual property
+ amendment of various Laws to takes into account new IT capabilities and threats

Other law Amendments, under study :

• **Special amendments for Fighting Spam**
(Reinforcement of the Law on consumer protection (and Intellectual property), which yet covers SPAM activities)
• **Amendment of the law** concerning **Cyber-Crimes**
→ **Responsibilities of actors (ISP, Web Editors, Web authors, Access Providers) & Lawful Interception considerations (Cyber-Terrorism).**

Overview About

CERT/TCC
Services & Activities

CERT/Tunisian CC

- ➢ Incorporates a Computer Security Incident Response Team (CSIRST)

- ➢ Manages an Information Sharing and Analysis Center (ISAC)

- ➢ Is a CERT (Information, Alert, Awareness, training, …)

Established Under the
National Agency for Computer Security

Will Integrates Private Investors (Around 2007)

CERT/Tunisian Coordination Center

Watch and Alert
(ISAC)
&
Incident Report and Handling
(CSIRT)

N.A.C.S
National Agency for Computer Security

CSIRT

CERT/TCC
Computer Emergency Response Team / Tunisian Coordination Center

Law No. 2004-5 of February 3, 2004 relative to IT security

Article 10 : Anyone who operates a computer system or a network, whether a public or a private institution, must immediately inform the National Computer Security Agency of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network so that the Agency can take the necessary measures to tackle them.
The operator shall be required to comply to the measures decided upon by the National Computer Security Agency in order to put end to such disruptions.

- Hotline (Call-center) and automated secure incident-reporting system.
- Assistance in Incident Handling and Foresenics (NACS Task Force)

→ With **authority** (by law): Able to consign to Security Officers of IS (&ISPs, IDCs), to **takes proactive measures** against disruptions, affecting other Information Systems .

Law No. 2004-5 of February 3, 2004 relative to IT security

Article 9 – The employees of the National Computer Security Agency and security auditors are Responsible about the preservation of the **confidentiality** of any information they came to know in the exercise of their functions.
Shall be liable to the sanctions stipulated in Article 254 of the **Penal Code** anyone who discloses, participates in, or incites to, the disclosure of such information

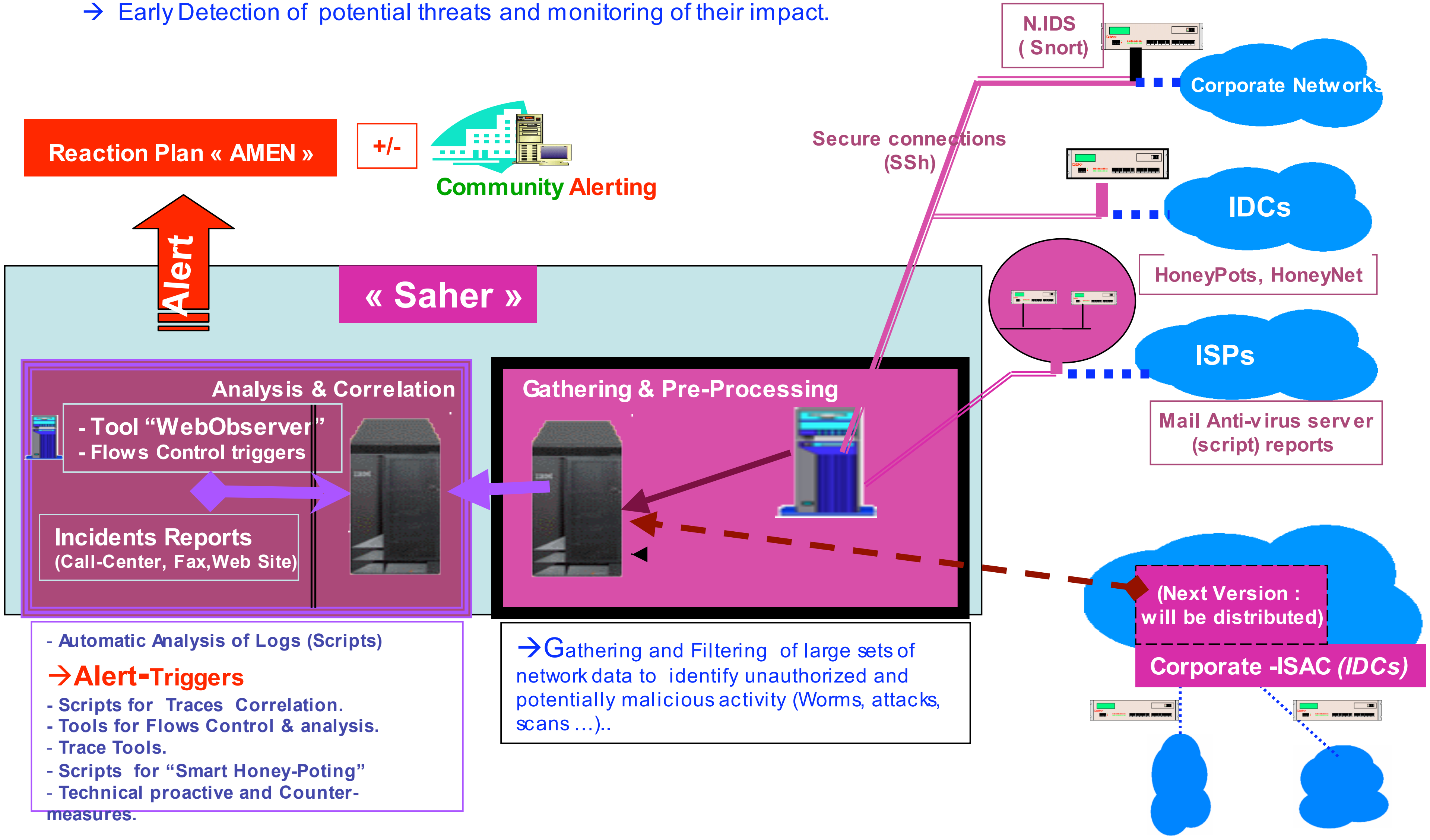
➤Private and public organizations should **trust** the CERT/TCC
➔ **Confident** report (and request for assistance) for **ANY KIND of incidents**

Watch and Alert

Watch System « SAHER » (CERT/TCC.ISAC)

A **Watch- center** (based on **open-source solutions**), which can monitor the National Cyber-Space in **Real time** (Fully operational, during WISIS, November 2005).

→ Early Detection of potential threats and monitoring of their impact.



- Automatic Analysis of Logs (Scripts)

→**Alert-Triggers**

- Scripts for Traces Correlation.
- Tools for Flows Control & analysis.
- Trace Tools.
- Scripts for "Smart Honey-Poting"
- Technical proactive and Counter-measures.

→Gathering and Filtering of large sets of network data to identify unauthorized and potentially malicious activity (Worms, attacks, scans …)..

“Amen” **Alert Handling (reaction plan) :**
--- Formal **Global** Reaction Plan.
--- Establishment of **Coordinating Crisis Cells** (ISPs, IDCs, Acess Providers, Big Infrastructures).
With CERT/TCC acting as a **coordinator** between them

→ Between 2003-2005 : **“Amen” was deployed 5 times**, During Sasser& MyDoom worms attack, during suspicious hacking activity and, proactively, during big events hosted by Tunisia (only between ISPs and national telecommunication operator)

✓ Motivation and support (training, assistance) for the establishment of **corporate CSIRT** (E-gov , Health, Energy, Education, Transportation)

✓ Launch and Follows-Up of a Project for building a “**Disaster-Recovery Infrastructure**” (financed by a loan from the World Bank)

✓ Funds for **studies** for :

- ✓ Establishment of ***Disaster Recovery Plans*** for some critical national applications.
- ✓ Schemes for improving the ***protection of National Cyber-Space* against DDOS**.

CERT/Tunisian Coordination Center

Awareness & Information

Information & Alert

Information about Vulnerabilities and Malicious Activities :

We Convey information (Collected through the Monitoring of multiple sources) through Mailing-List(s) :

→ Around **5200 *Voluntary*** subscribers

→ Around **110 e-mails sent during 2005** (450 during 2003-2004)

Various Rubrics :

❑ **Threats** :

.Vulnerabilities	**.Virus**	.Spam	.Hoax	.Precaution	**.Administrators**	**.Alert**

❑**I nformation** :

.Tools	.Open-	.Announce	.Books

.VIRUS

Object : ....
Concerned Plate-forms and systems :

Effects	
Visible traces	
Ways of propagation	
National propagation	
International propagation	
More details (urls)	
Preventive Measures	

1- Highly critical vulnerability in ...., which permits ......
2- Medium level vulnerability in ...., which permits ......
3- ....

1- "Product name"
Concerned Plate-forms : ......
Concerned versions : ....
Brief Description :
....
....
For more details : (urls)

SOLUTION
....
....

2- "Product name"
....

. Vulnerabilities (users)
. Administrators (Security Officers)

+ On going Work :

- Preparation of a ***guide on*** **Open-source security solutions** *(in advanced state), Security practices Manuals,*

- Publication of A Monthly **Newsletter** (*Summaries* about , *Incidents and vulnerabilities, International Events and News).*

Awareness

- **Maintain of Users Awareness about security issues, Best practices & Solutions**

Through :

✓ Specialized Mailing-list rubrics (**.Vulgarisation/ .Flash,/. Tools**),
✓ Permanent rubrics in Regional and National **radio** stations (and some ISP Web sites).

✓ Presentations in (~) All (Third-party) **Conferences & Workshops** (IT meetings, IT associations Conferences, Auditors Workshops, …) awareness and **induction of nest of voluntary "pushers"**

→ Presentations for public controllers & auditors (smoothing of "**bureaucratic**" barriers)

✓ Booths in National and Regional **Exhibitions** (platforms for ***simulation of real attacks***, CDs of **free (for domestic use) versions of security tools** and voluminous patches, brochures)

Children & parents :

- Inclusion of a special **Mailing-List rubric for parents (.PARENTS)** : Internet risks (paedophile risks, …) & Parental control tools
- In **Collaboration** (technical guidance and funds) with centers and associations, acting for **childhood education** :
  - ❑ Start the preparation of a first pack of short (awareness) courses for Primary schools.
  - ❑ Start the Development of pedagogical material for children : Series of **Cartoons** (**Virus, Worm** – Risks for Childhood, Trojans, spywares, …)

-Press Medias :

-Creation of a **Press-relation position** in CERT/TCC (a journalist)

→Inform and Assists Journalists (Information Material, ..)

- **We used Press Channels to alert** broad population **, during the last wide viral attacks (MyDoom, Sasser)**

→ Raise awareness about

- the existence of risks

+ the existence of EASY steps to protect themselves **(with precautions to NOT FRIGHTENING).**

CERT/Tunisian Coordination Center

Professional Training & Education

Professional Training & Education

Goal **:** Establish of a task force of **Trainers** in IT Security.
→ Launch of training courses for ***trainers*** (University, private and public training organizations) in the basic field of IT security

- First 3 Courses (under a loan of the WB) for 35 trainers each :
  - Network security techniques
  - Network security organization (security policy development, security plan development, tools.).
  - -Methodologies of security assessment (ISO 1 7799, ISO 1 9011. BS 2 7799)

❖ **Re-Training** : organisation of training for security auditors

(2 Night sessions for 50 professionals, as a preparation to NACS certification exam)

❖ **Academic institutions** : Collaboration to develop (*common*) **curricula in IT security** :

(A master in IT security audit provides (Now) **automatic certification for students**).

→ in **2004** : Launch of a ***first*** Master in IT security (Collaboration between two universities).

→Scholar year **2004-2005** : **4** masters (2 public & 2 private universities).

❖***Private Training Centers*** : *Professional seminar-courses*

(average of 2 seminars by month).

-**Collaboration with academic/education entities** for :

- Launch of a **Research/Training laboratory** specialized IT security (Loan from the World Bank).
- -Introduction of (awareness) security courses inside ALL academic and secondary programs.
- -Launch of 2 Regional Masters (South : Sfax, North : Jendouba) .

-Preparation of specialized training for **Press/ Judicial and investigation staffs.**

- Preparation of training courses for technical staff of **corporate CSIRTs.**

-Motivation and Assistance for professional, for getting **international certifications** :

- -Paid certification preparation courses for “Majors” (Masters and NACS courses),
- - Funds for ALL professionals (Ministry of Technologies of communication funds).
- - Recognition of Major International certifications (CISA, CISSP, GIAC, ..), as “equivalents” for NACS certification and as a proof of quality (CV criteria in tender of offers, ..)

CERT/Tunisian Coordination Center

Synergic and Catalytic Actions

Research & Development

Accordingly to the task of NACS : “Fostering the **development of national solutions** in the field of computer security and promoting such solutions in accordance with the National **Priorities”.**

Strategic Catalyser = Open-Source → “Motivation” of the Private sector/ R&D entities:

- Launch of 4 projects of development of security tools (from open-source) for the private sector.

- Definition of **5 thematic projects of Research&Development** for academic laboratories (with the collaboration of the Ministry of Scientific Research)

- In trend of Promotion : Local **Security Products** (Secure e-mail “**Hannibal**”, Distributed Firewall “**Seventh**”

Professional Associations (representative Interlocutors & synergy)

Motivation (creation) and support (recognition, logistic) for Professional associations in IT security :

• A professional association : “National Association of the Professionals of IT Security”.

• An academic association : “Association for Numerical Security”.

"Miscellaneous"

Promotion of Self-assessment methods & Best Practices (guidelines)

- **(Temporary) Adoption of ISO 1 7799 (Best Practices),** as basis for mandatory (By Law) risk assessment (future step -- : BS 2 (ISO) Certification) .

- Funds (for the University & Private and public corporations) to develop (adapt) a ***self*** assessment method, adapted to our STEP, integrating software tools for its easy deployment (risk evaluation and guides for corrective actions)

Publication of Professional Material : Models for Tender of offers (Fair concurrency and confidence for investors)

• Publication of a "Model for tender of offers" for **Risk Assessment operations**
(With consultation and **validation** by private auditors)

• Development of Drafts of tender of offers for **Security Tools** acquisition (Firewalls, IDS, …, Assistance for Open-source product deployment)
(Under consultation with private integrators)

Periodic Electronic Surveys on security (Assesment of the situation & Revision of Action Plans)

- Periodic Surveys on IT Security concerns
  - An Electronic National Survey was done in end 2003
    (tuning of the national Plan (weakness, urgent actions and their volumes)
  - A new survey in preparation for end 2005.

.

Hosting of students projects …..

Incorporation inside International associations and organizations

- CERT/TCC will Contribute in a “Steering committee” for the launch of an OIC CERT (KICT4D Conference, Malaysia, June 2005)

- CERT/TCC Foresees to be asap Incorporated, as a member of the FIRST

(Project of assistance by an International CERT & CSIRT, financed by a Loan from the WB) → Collaboration & Sponsorship by a member of the FIRST.

- CERT/TCC staff are Willing to be active inside workgroups, related to IT Security, inside International Organizations : ITU, OCDE, ….

Collaboration at the International level

CERT/TCC is Willing to :

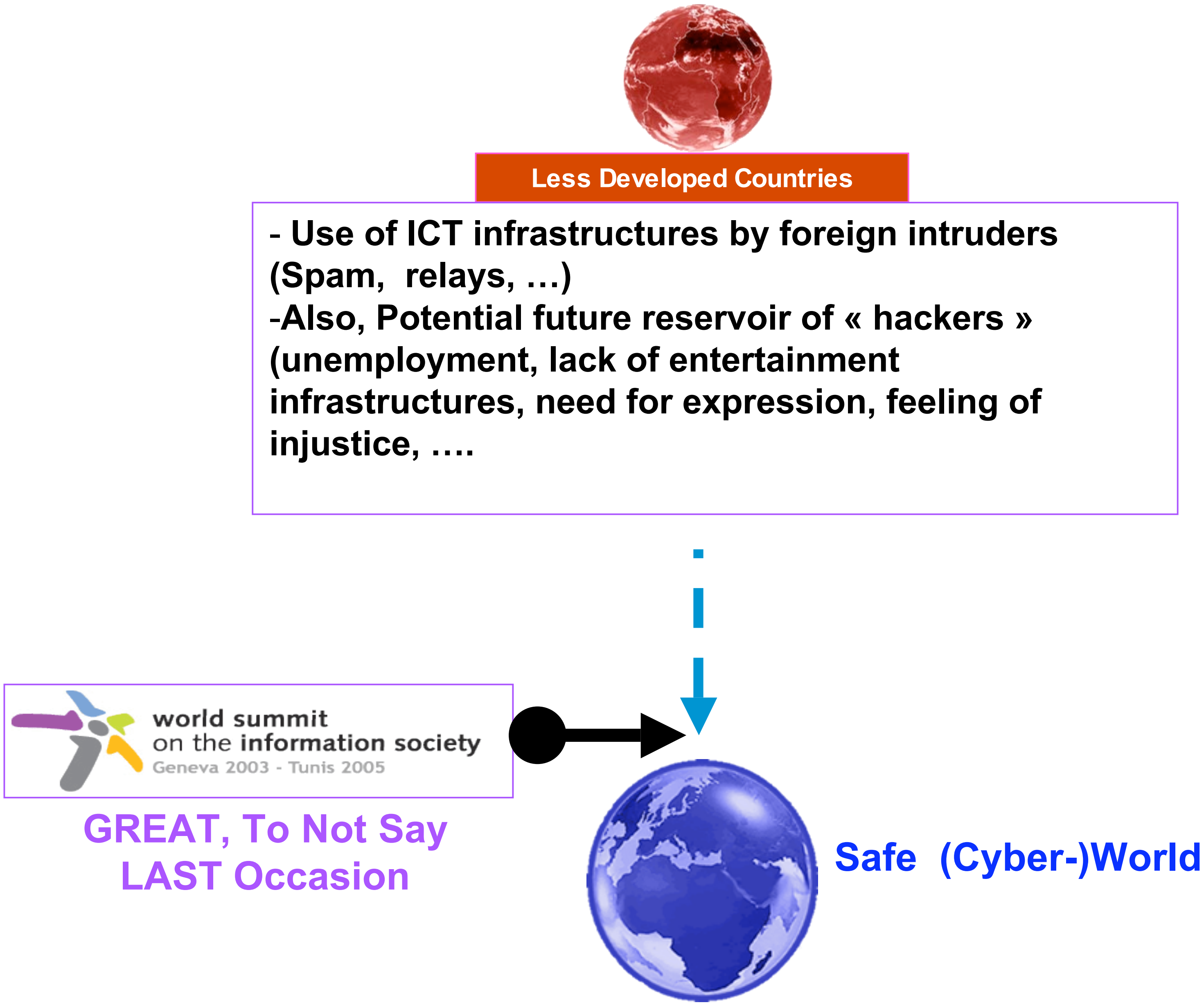
-Establish collaboration with international organizations committed to IT security (ENISA, APCERT, WWISAC,*…).*

-Collaborate with other Regional CERTs/CSIRTSs, especially to help for the establishment of Agencies/ CSIRT/CERT in Less Developing countries, especially (langage), but not limited to, African and Arab countries).

-Collaborate with IT industrials (Vulnerability analysis& Discovery of Arabic software versions, ….).

-Provides Help in investigations about cyber crimes or attacks, seeming, originating from Tunisia.

& Do technical preparatory work to makes Tunisia Adherents to ALL International Conventions and Treaties, concerning Cyber-Security.



Less Developed Countries

- Use of ICT infrastructures by foreign intruders (Spam, relays, …)

-Also, Potential future reservoir of « hackers » (unemployment, lack of entertainment infrastructures, need for expression, feeling of injustice, ….

world summit
on the information society
Geneva 2003 - Tunis 2005

GREAT, To Not Say
LAST Occasion

Safe (Cyber-)World

CERT/TCC COMMITMENT :
Our Modest Experience & Logistic
Is Offered “FREE of Charges”
For Helping Others Countries, concerned by the Digital Divide

Some Particularities, of Less-Developing countries

Characteristic = Early stage of development of ICT

→ **Quite total Lack of Awareness** :

Necessity of a pragmatic approach :

- Start by High-level Awareness (by providing Foreign Funds and "free" Assistance)

→Start awareness of IT Professionals,

which will be in charge of :

→"Attacking" the common IT users & Finally, the broad Population, by a progressive approach, with care to not frightening about ICT use

→**Quite total Lack of Protection Tools and modest funds**

→ Importance of **vulnerabilities "lock-down"**

→ Information about Vulnerabilities and assistance for patching (**taking into account big presence of old OS versions and equipments**, usually no longer maintained by manufacturers !!).

→ Few "technicity"

→ Launch of a task force of **trainers** and Experts.

→ Few Internet users and some ISPs

→ Start by focusing the protection at the level of ISPs (Anti-virus, Anti-spam, NIDS)

→ Push-Up the Open-source culture.

THANKS YOU

Nabil SAHLI
National Agency for Computer Security

n.sahli@ansi.tn

« Raw
« Reflexions »

« Raw » Personal « Reflexions »

-Pursue the maintenance of « old » versions (It is their responsability)
Or Provides LIGHT versions, requesting less processing Power.

-Take care to raise attention about hidden risks
(also those where usual basic competence is assumed)
and still provide « more pedagogic » Documentation

- Security Industry : Provide special prices
(relative to the level of life)

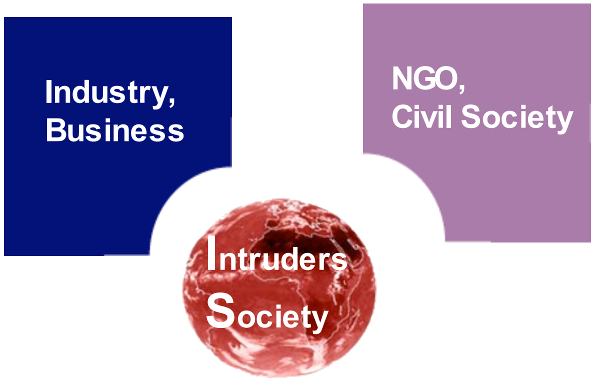
- ISPs connecting Less-DC should foresee how to « clean » flows
& Better : Provision of cheap training and assistance for local ISP staff

-Access Providers connecting Less-DC should forsee how to provide
-protection Against DDOS attacks.
(Cheap Back-Up connections)
…………

Industry,
Busines
s

Special Treatment
= As an Investment in, hopefully, future
Growing markets (= **Marketing**)

« Raw » Personal « Reflexions »



- Associations& Forums in IT Security (FIRST, …) :

Should :

- Include a special rule for becoming A member = « Help » provided to Less-DC
- Encourage more work on solutions, adapted to Less-DC stage and reality.

-International Normalisation Organisations (ITU, …) :

Should Takes into account « specific stage » of Less-DC for

- More Clear Guidelines about strategies of Evolution.
- More representatives from Less-DC in Workgroups
  (Clear schemes of migration (of –DC) to new technologies and norms).

- Humanitary NGO, should

- Create cyber-protection emergency Units (It is Information Society …).
- -Rules for duties of Developed& Developing countries to takes immediate Measures, against using Less-DC Infrastructures (as « hostages ») by local Intruders

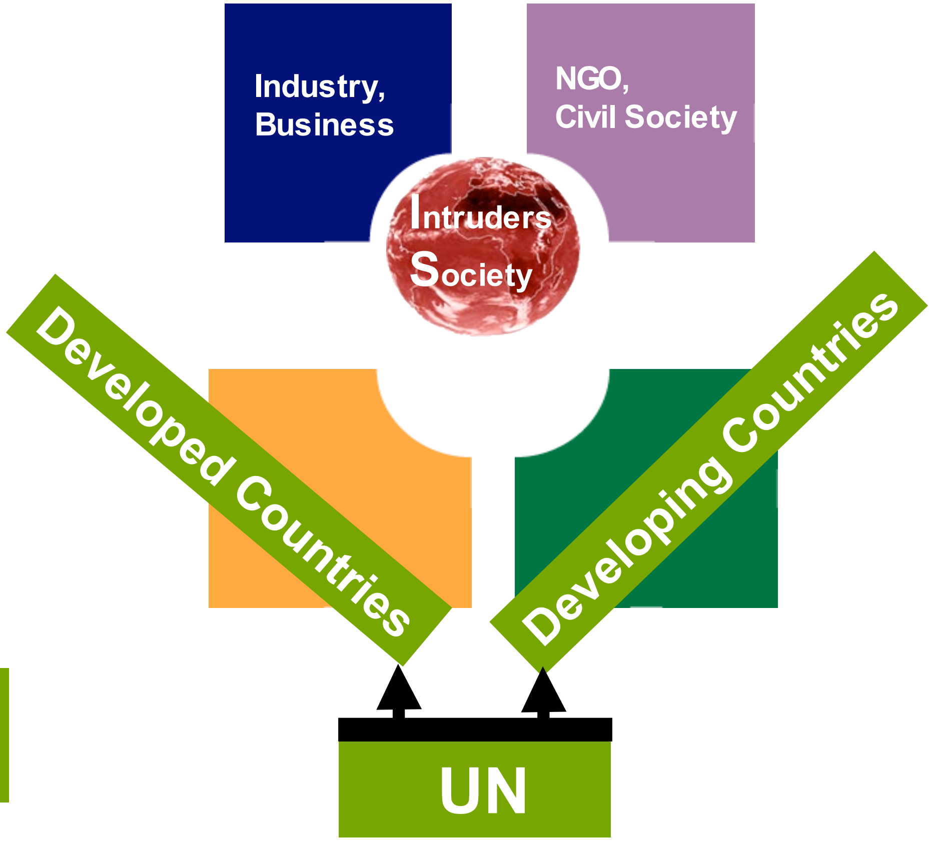
…………………

« Assumer leur rôle »

« Raw » Personal « Reflexions »

Developing Countries Should :

- Provides Guidelines about the lessons learned in their evolution (they were Less-DC)
- Provides « cheap » Technical Assistance.
- Be a « comprehensive » link between DC & Less-DC



Developed Countries :
« ARE CALLED TO DO ALL THE REST »,

« Raw » Personal « Reflexions »

IT STILL POSSIBLE TO DREAM & LOVE

(Beautiful mysteries Of BRAIN & LIFE)