Insights into the Tunisian experience and strategy in the establishment of National watch, warning and Incident Response capabilities

Pr Nabil SAHLI,
Ministry of Communication Technologies
National Agency for Computer Security, TUNISIA
n.sahli@ansi.tn

Plan

- Fast Overview about the Tunisian Experience in IT Security, as a case example for developing country
- Insights into the Tunisian experience and strategy in the establishment of national and regional watch, warning and incident response capabilities :
The Tunisian CERT/TCC

- Overview about **Awareness & Information actions.**
- Overview about **Assistance for Incident Handling (CSIRT)**
- Overview about **Establishing Watch and Alert Center (ISAC "Saher")**
- Overview about **Professional Training & Education actions**
- Overview about **Research & Development strategy.**
- **The role of NGO.**

-Some specificities and Needs of Less developing countries and opportunity of a "Regional approach"

Fast overview about the Tunisian Experience and strategy in IT Security

a fast Historical Overview

❑ end **1999 :** Launch of a **UNIT (a “Micro-CERT”)** , specialized in IT Security

Objective :

- **sensitize policy-makers and Technical staff about security issues**.
- Assists in Monitoring the security of highly critical national applications and infrastructures..

+ ***creates a first Task-force of Tunisian Experts in IT Security***

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

➢ The unit starts the establishment of a **strategy** and of a **National Plan** in IT Security

(**national survey** , for fixing: priorities, volume of actions, needed logistic, supporting tools, .).

❑ **January 2003 :**

- Decision of the Council of Ministers, headed by the President, and dedicated to informatics and IT Security , of :

❑ The creation of a National Agency, specialized in IT Security

(The Tool for the execution of the national strategy and plan)

❑ The Introduction of Mandatory and Periodic Security audits

(Pillar of our strategy)

❑ The creation of a “body of certified Auditors” in IT Security

+ A lot of accompanying measures (launch of masters in IT security, ...)

In addition of existent Laws :

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° 1999-89, Art 199)**

Ø **Law on consumer protection and respect of Intellectual property** **(Law N°1994-36)**

✓ February **2004** : **Promulgation of an "*original*" LAW,** on **computer security**
(Law N° 5-2004 ***and 3 relatives decrees***) :

➢ **Obligation** for national companies (<u>ALL public</u> + "big" and sensitive <u>private</u> ones) to do **Periodic (Now annually) Security audits of their IS.**

➢ **Organization of the field of Security audits**

→ Audits are Made by **<u>CERTIFIED auditors</u>** (***from the private sector***),
→ *definition of the process of certification of auditors*
→ *definition of the auditing missions and process of follow-up* (**ISO 1 77 99**)

➢ *Creation and definition of the Missions of the* **National Agency for Computer Security** **(which does not deal with National Security & Defense issues)**
(created under the **Ministry of Communication Technologies)**

➢ **Obligation to declare** security Incidents (Viral, mass hacking attacks, ..)
that could affect **others** IS, with guarantee of **confidentiality**, by law.

Main Current Axis of the Tunisian strategy in IT Security

Permits a secure « opening » and strong integration of National Information Systems (e-administration, e-banking, e-commerce, ..)

Promotes Training and Awareness activities in IT Security

Improve the safety of the National Cyber-space and confidence in the use of Internet and ICTs

Launch of R&D activities, relatively to our priorities

Make Law and regulations "Up To date » and adhere to all international conventions and treaties

+ Work for the ROI, through Employment, Export of services & Attraction of foreign investment

Instruments (National Plan) =
National Agency for Computer Security & its CERT/TCC

Insight into CERT/TCC

(Computer Emergency Response Team / Tunisian Coordination Center

SERVICES & ACTIVITIES

Hosted by the National Agency for Computer Security → **In the Future: Some activities Will « go » to the Private Sector**

CERT/TCC’s

Information&Alert Activities

Information & Alert

Cert/TCC disseminates Information about Vulnerabilities and Malicious Activities & Awareness material :

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

→More than **6 300** ***Voluntary*** subscribers

→More than **250** e-mails sent during 2005 (More than 400 products **vulnerabilities** declared)

Various Rubrics :

- ❑ **Threats** : **.Vulnerabilities** | **.Virus.** | .Spam | .Hoax | .Precaution | **.Administrators** | **.Alert**
- ❑ **Information** : .Tools | .Open-source | .Announces | .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 :

Development of guides on Best practices and Open-source security solutions & A Monthly Newsletter .

CERT/TCC's

Awareness Activities

Cert/TCC started with concentring in the **Awareness field**

✓organizes & Intervenes in all ***Conferences & Workshops*** (12 interventions , in 2006) and acts in more sensitizing decision-makers & public controllers, for smoothing the “bureaucratic” barriers.

✓organize Booths in all National and Regional Exhibitions (***demonstration*** of attacks → get in touch with **reality of risks**)

✓ Develops and distributes awareness material : brochures (8), CDs (3: free security tools for domestic use , open-source tools, voluminous patches), 2 guides (under development)

+ Publish Awareness material through its Mailing-list (rubrics .Precaution, .Flash,/. Tools, .open-source),

+ Acts for raising **Youth and parents awareness** **,**In Collaboration with specialized centers and associations :

❑ Preparation of a first pack of short (awareness) courses for Primary school.

❑ Starts the Development of special pedagogical material for childrens&parents : 3 “Cartoons”, Quizs

- Development of a special rubric in the Web site and Inclusion of a special Mailing-List rubric for parents (Parental control tools, risks, ..)

+ Rely on the Press, for raising awareness of **broad population**

about the existence of risks (with precautions to NOT FRIGHTENING).

& the existence of *simple precautionary* measures to protect themselves

→ Creates a ***Press-Relations position*** in CERT/TCC (a journalist, which prepares and provides Information Material to Journalists : motivation ..)

→ Average of 3 papers/week published, during last semester

→ Participates in the animation of ***weekly rubrics*** in ***5*** Regional and National **radio stations (3 in 2005)**.

+ Preparation of a ***course*** on IT security trends, for **students in Journalism**

The promulgation of the Mandatory annual security audit (**Law on computer security)**

= Best Awareness tool for IT professionals and decision-makers

+ the audit includes the realization of awareness sessions for the hole staff

CERT/TCC's

ISAC

(Information Sharing and Analysis Center)

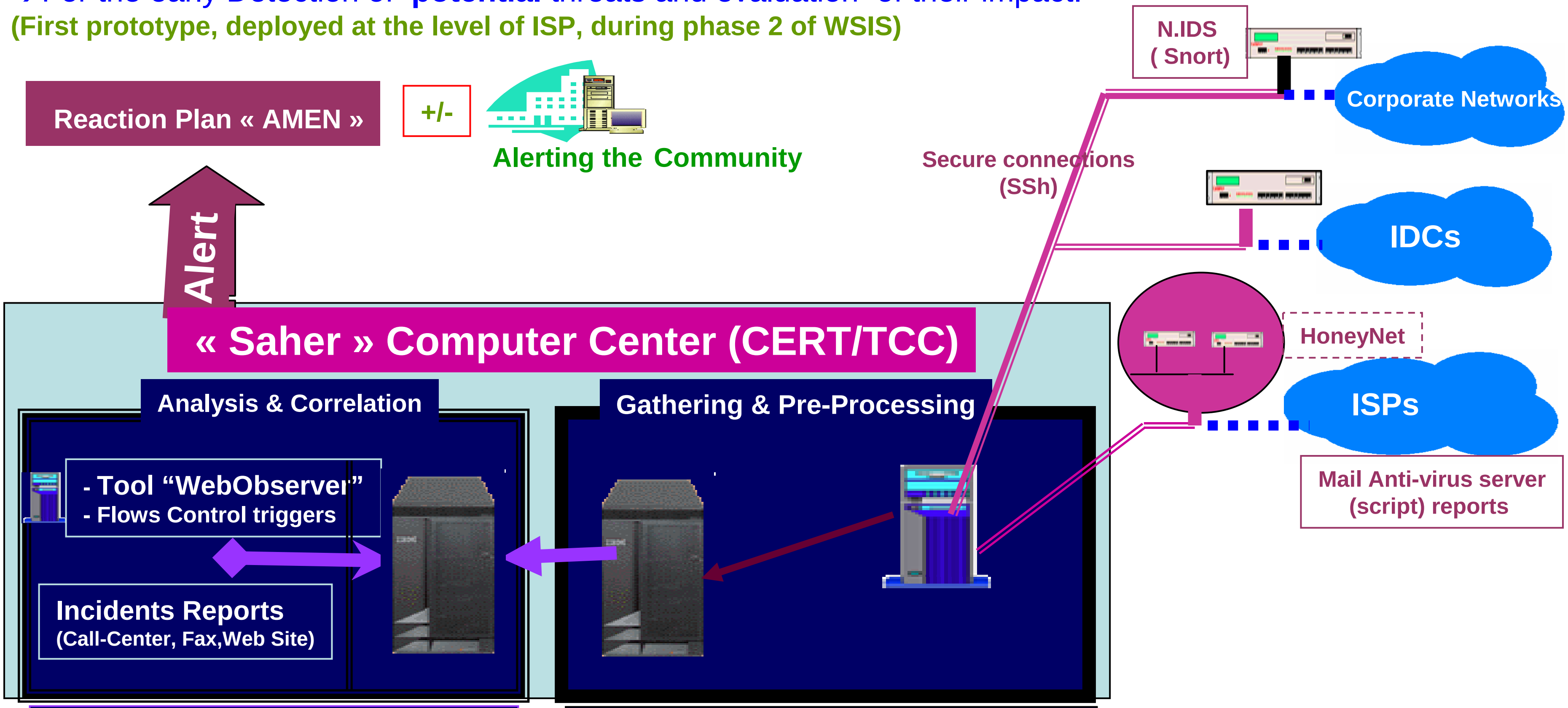
Project "Saher"

ISAC "Saher"

A **Watch- center** (based on **open-source solutions),** which permits to monitor the National Cyber-Space security in **Real time**

→For the early Detection of **potential** threats and evaluation of their impact.

(First prototype, deployed at the level of ISP, during phase 2 of WSIS)



Reaction Plan « AMEN »

+/-

Alerting the Community

Alert

« Saher » Computer Center (CERT/TCC)

Analysis & Correlation

- Tool "WebObserver"
- Flows Control triggers

Incidents Reports
(Call-Center, Fax,Web Site)

Gathering & Pre-Processing

N.IDS
(Snort)

Corporate Networks

Secure connections
(SSh)

IDCs

HoneyNet

ISPs

Mail Anti-virus server
(script) reports

Automatic 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 plan**

--- "Formal" **Global** Reaction Plan.

--- Establishment of **Coordinating Crisis Cells** (ISPs, IDCs, Acess Providers).

With CERT/TCC acting as a **coordinator** between them

"Amen" was deployed 6 times, During Sasser& MyDoom worms attack, during suspicious hacking activity and, proactively, during big events hosted by Tunisia (only with ISPs and telecommunication operator)

Disaster-Recovery Infrastructures

- ✓ National Project for building a **National Disaster-Recovery Center** (managed by the National Center for Informatics, with **funds from the World Bank**)
- ✓ Funds for **studies** :
  - ✓ for the establishment of ***Disaster Recovery Plans*** for some critical national applications**.**
  - ✓ for the improvement of ***protection of the National Cyber-Space* against** big **DDOS attacks**.

CERT/TCC's

CSIRT team

&

WARP (Warning, Advice and Reporting Point),

CSIRT

Article 10 of the Law No. 2004-5 relative to IT security

Public & Private institutions, must inform the National Agency for Computer Security about any Incident, which can affect other Information Systems

CERT/TCC provides :

- **A CSIRT team** in charge of providing (free of charge) **Assistance for Incident Handling**
- Call-center, **available 24Hours/24 and 7 days/week**

With Guarantees for the confidentiality :

Article 9 of the Law No. 2004-5 relative to IT security

Stipulate that The employees of the National Computer Security Agency and security auditors are Responsible about the preservation of confidentiality and are liable to penal sanctions

➢ Private and public organizations should **trust** the CERT/TCC

→ **Call for assistance**

+ A "Citizen's assistance service ",
To which Home users can bring their PC to solve security problems or install security tools (anti-virus, PC firewall, anti-spam, ..), free for domestic use.

+ Acting for the emergence of **corporate CSIRT in some sensitive sectors** (E-gov, E-Banking → Energy, Transportation, Health)

CERT/TCC's

Training & Education

Professional Training

- ***Establishment of a Task Force of*** Trainers in IT Security.

→ Launch of training courses for ***trainers*** (private sector)

- 3 Courses (Loan of the World Bank) for 35 trainers each made in basic trends : Network security, Systems security, Methodologies of security assessment (ISO 1 7799, ISO 1 9011. ISO 27 001) and security plan development.

- Preparation of 4 additional training courses for trainers in 2006.

❖***Re-Training of professionals*** *:*

- ***organisation of trainings*** *(with collaboration of training centers & associations)*
  - ❖ *for security auditors (Night sessions for professionals, as a preparation to the certification exam)*
  - ❖ *for Security administrators (Periodic sessions for the adminsitrators of e-government applications)*
  - ❖ *Preparation of 2 training sessions for* ***judges and Law enforcement staff****.*

- *Acting in Motivating* ***Private*** *Training Centers* activities in IT Security (average of 2 seminars by month in 2005) .

- Acting to Helps professionals for getting **international certifications** : CISSP exam preparation courses

Education

-Collaboration with academic institutions for :

-Developing **Masters** in IT security :

(Now, A master degree in IT security permits the **Obtention of Auditor Certification**).

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

→ **Now : 4 masters** (2 publics & 2 privates universities).

→ Next academic year → **7** (3 in preparation)

- Organization of **training modules** (5) **for teachers from the university** (Loan from the World Bank).

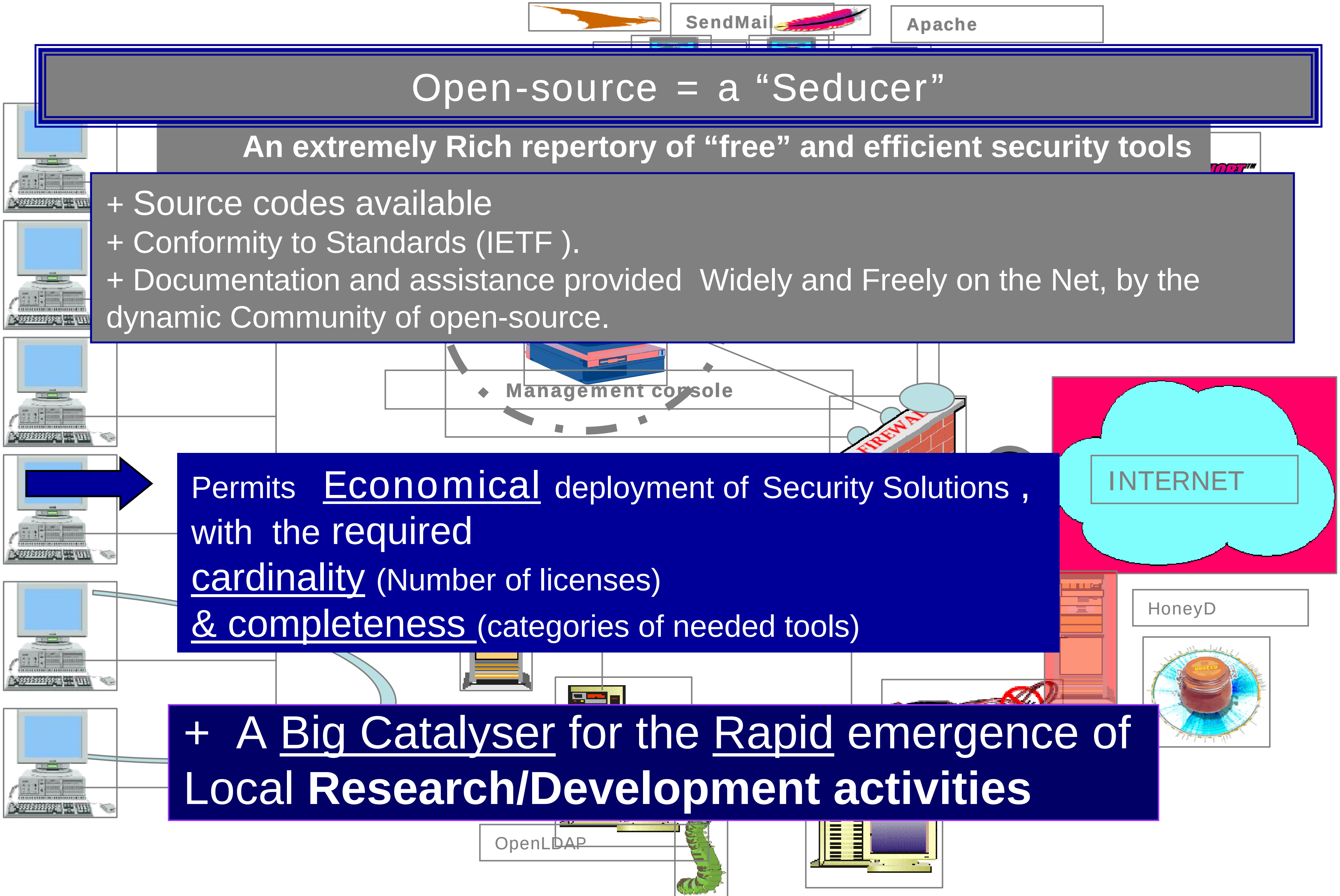
-Acting for the inclusion of security modules (awareness) inside **ALL** academic and education programs.

+ Hosting of students projects by the CERT/TCC (15 in 2006)

Insights into the Tunisian Strategy for the Emergence of Research & Development activities

Accordingly to one of the task of National Agency for Computer Security :

→ “Fostering the **development of national solutions** in the field of computer security and promoting such solutions in accordance with the National **Priorities”.**



Open-source = a “Seducer”

An extremely Rich repertory of “free” and efficient security tools

+ Source codes available
+ Conformity to Standards (IETF).
+ Documentation and assistance provided Widely and Freely on the Net, by the dynamic Community of open-source.

Permits Economical deployment of Security Solutions , with the required cardinality (Number of licenses) & completeness (categories of needed tools)

+ A Big Catalyser for the Rapid emergence of Local **Research/Development activities**

- Acting in **Raising awareness about the benefits (&limits) of the deployment of open-source tools.**

- Formulation (funds) of **4 projects for the development of security tools (from open-source**) for the **private sector** (including improvement of the system “Saher”).

- Definition of **5 federative projects of Research&Development** for **academic laboratories** (under the supervision of the **Ministry of Scientific Research**)
- Collaboration, with the university for the launch of a **Research laboratory** specialized in open-source security tools (Loan from the World Bank).

CERT/TCC is Acting :

- For sensitizing young investors (by providing “Markets”),

To

First Step : Provides support for open-source tools deployment (installation, training, “maintenance”)

Then → Customization of open-source solutions (for clients specific needs)

End → Launch of real Research/Development activities

Induction of Synergy
Between National actors

Rely on Associations (NGO)

Motivates the creation of specialized Associations in IT security :

- An ***academic*** association was **launched** in 2005: “Tunisian Association for Numerical Security”.
- A ***professional*** association : “Tunisian Association of the Professionals of computer Security”.

In project : An association of ISPs

With access providers, ISP and content developers :

Debate for :

- establishing a **consensus** about **responsibility rules for “content”** and **consolidation of control mechanisms, concerning abuses :**
  - **Controlling Spam** (and all abuses by the means of networks or electronic facilities).
  - Insuring the respect of ***personal data privacy***
  - detection of infringements to **intellectual property**,
  - control of fraudulent and misleading commercial conducts.

- The **Consolidation of International Collaboration, with foreign ISPs** (Mutual assistance, recognition and reciprocity provisions,..)

- IN Collaboration with associations (NGO) :

-Organisation (ATIM, ATSN, JCI, ATAI, ...) of awareness actions (10 seminars and workshops)

Motivation (funds) for the Development of Self-assessment methodologies (adapted to our STEP)
& Guides of Best Practices

Implication for the Development of Models of books for Tender of offers (Insures Fair concurrency → attracts more private investments in the field)

- Publication of a “Model for tender of offers” for **Risk Assessment operations** (With consultation and **validation** of private auditors)

•Development of Models of books for tender of offers for
-**Commercial** Security Tools acquisition (Firewalls, IDS, …,)
•**Open-source** Security tools deployment (Training, assistance)

Implication for Evaluation of actions & Revision of Action Plans

- Realization of **National Surveys** about IT Security
  - An Electronic National Survey was done in end 2003, for the tuning of the national Plan (weakness, urgent actions and their volumes)
  - A new survey is prepared for 2006, with participation of the 2 associations

.

After consolidation of its (national) activities

→foreseeing International Collaboration

(Thanks to ITU)

International Collaboration

-CERT/TCC is acting (with colleagues from other Islamic CERTs, from Malaysia, Nigeria, UAE, Pakistan) for the launch of an **OIC CERT** (recommendations of the KICT4D Conference, Malaysia, June 2005).

→ Meeting in july 2006, in Malaysia

- CERT/TCC Foresees to be member of the " FIRST"

→ Launch of a Mission of Assistance for ***Sponsorship***, by a private member of the FIRST : CERT-IST (Loan from the World Bank)

(In trend of being incorporated into an international security program of Microsoft**)**

+ CLEAR COMMITMENT TO :

- To participate more actively in the actions of WSIS C5 action line, under the supervision of ITU.

- Shares our modest experience (errors, success stories) and provides (FREE of CHARGE), as available in this step, assistance and logistic (hosting of trainees, awareness material, Saher, open-source training,…) For the establishment of CERT/ ISAC/CSIRT in countries, calling for such collaboration.

- - Collaborates with other CERTs and provides collaboration in investigations about incidents, seeming, originating from Tunisia.

- To contribute in developing measures to deal with large-scale or regional network security incidents & Share information relating to security incidents

- To Improve links to international network security groups and to collaborate with the international frameworks for the Launch of collaborative actions on subjects of mutual interest

- To establish Partnership with the private sectors to promote network security in the region

- To Participate in the setup of regional CERT (Africa, Arab countries), to help other countries that does not have National CERT bodies and to contributes in building emergency task forces.

Less Developed Countries “In Mind”

About Less Developed Countries

Less Developed Countries

- Use of their ICT infrastructures by foreign intruders (relays of Spam, Botnets, Phishing, …)
-Also, Potential future “Reservoir of hackers” (unemployment, lack of entertainment, feeling of injustice and need for expression ….)

+ Risk of More Digital Divide, by undermining confidence in ICTs

=« Last Chance »

Urgent   AID start

In fact, Not only a matter of ‘AID ’ but MUTUAL SELF-INTEREST to prevent the creation of criminal havens

world summit
on the information society
Geneva 2003 - Tunis 2005

Safer (Cyber-)World

Characteristcs and Needs of Less-Developing countries

Lack of Awareness :

Necessity of a pragmatic approach :

- Raise Awareness of Politicians and policy-makers

+ Provides Funds (Loans, donation via “AID” programs)& **Technical Assistance**,

→ **Launch of “Nucleus” of local CERTs**,

Which provides a first “Nest” of **local experts, which will** be in charge of :

→ raising awareness of IT Managers & administrators,

whom will be the **task force in charge of** “Attacking” IT users

& Finally, the broad Population, by a progressive approach (with care to not frightening).

→**Establishing a National strategy and plan for treating cyber-security issues, accordingly to the state of development of each country.**

Lack of Experts

-Necessity to help the Set-Up of a first Task-force of local Experts :

→ Need for training

“Poor” economies (& Quite total Lack of Protection Tools)

- **Crutiality of awareness and information about Best practices (the “proactive approach”).**
→ Provides help to local CERTs (awareness material, …).

- **Encourages the use of Open-source products (in parallel with commercial ones)**
→ Need for raising awareness about capabilities offered by the open-source field
→ Need for trainers in the open-source field
+ Private sector should provides special discounts (accordingly to the “level of life” and as a marketing action for,hopefully, growing markets)

- Helps for the provision of protection (NIDS, Anti-virus, ..) at the level of ISPs :
→ ISPs connecting Less-DC ISPs (little size) should foresee how to better « clean » flows & Provides (cheap) training and assistance for local ISP.

- Provides/dedidactes CSIRST teams, ready to intervene in case of emergencies in LDC (“**Cybenetic Red-Cross**”, It is Information society …)

+ The necessity for Developed& Developing countries to pay the needed attention & take the needed Precautionnary measures, against the abuse made by « their » Intruders, of Less-DC Infrastructures.

Opportunity of a " Regional Approach"

**To best effect and to maximise success of International « Aid » for LDC,
it is important to takes into account the "Regional" approach benefits :**

-it is essential that we try to combine Regional skills (of all stakeholders : private sector, NGO, governments) from Both Developed and Developing Countries
With inputs and guidance from eminent International experts, research centers and organisations, specialized in the field .

- Help to LDC for establishing CSIRTs, could efficiently rely on public and private Regional CSIRTs
For better addressing problems that may be Specific and common to
several countries in each region (similar Langage/culture, same Time/Adress Block/, …)

→Motivates the Launch of additionnal Regional CSIRTs, to cover all regions (African , arab countries, South America, ..), with their assignation of the task of acting in helping regional LDC countries establishing CSIRSTs.

- At a regulatory and government level, and besides the great actions carried by the ITU and the WB :
Much can be achieved by raising awareness of Regional organisations
(Arab league, African organization, GCC, ASEM, …) and Regional development Banks
(African Bank for Development, Islamic Bank, …).

CERT/TCC's COMMITMENT : Our Modest Experience & Logistic
Is Offered "FREE of Charges"
For participating with Others Countries, in International "AID" programs,

And

Is ready to host in Tunisia, a multi-stakeholder meeting, dedicated to
Less-DC, with invitation of representatives from those countries,
under the supervision of ITU and
other international organisations

THANKS YOU

Pr Nabil SAHLI,
Ministry of Communication Technologies,
Header of the CERT/TCC
National Agency for Computer Security, CEO

n.sahli@ansi.tn

Objectives of OIC-CERT (DRAFT) :
The purpose of OIC-CERT is to encourage and support the smooth collaboration and cooperation between CERTs among the OIC members.
The objectives are as follows:

-- Education and Outreach Program for setting-up CERTs / CSIRTs among OIC members that do not have CERT / CSIRT within their respective organisations. The OIC CERT also is able to assist other CERTs and CSIRTs in the region to conduct efficient and effective computer emergency response.

-Strengthen Relationship amongst CERTs / CSIRTs in the OIC member domain. This is to build cooperation amongst
-OIC members for an effective coordination and management of security incidents. This also will enhance the
-international cooperation on information security Information Sharing in terms of findings from reported incident cases,
-so that the information can be used to identify and to correct security vulnerabilities before they can be exploited.
This also enables OIC members to share experiences and best practices.
This objective will enable the OIC CERT to jointly developing measures to deal with large-scale or regional network security incidents

- Prevent / reduce cyber terrorism and computer crimes.

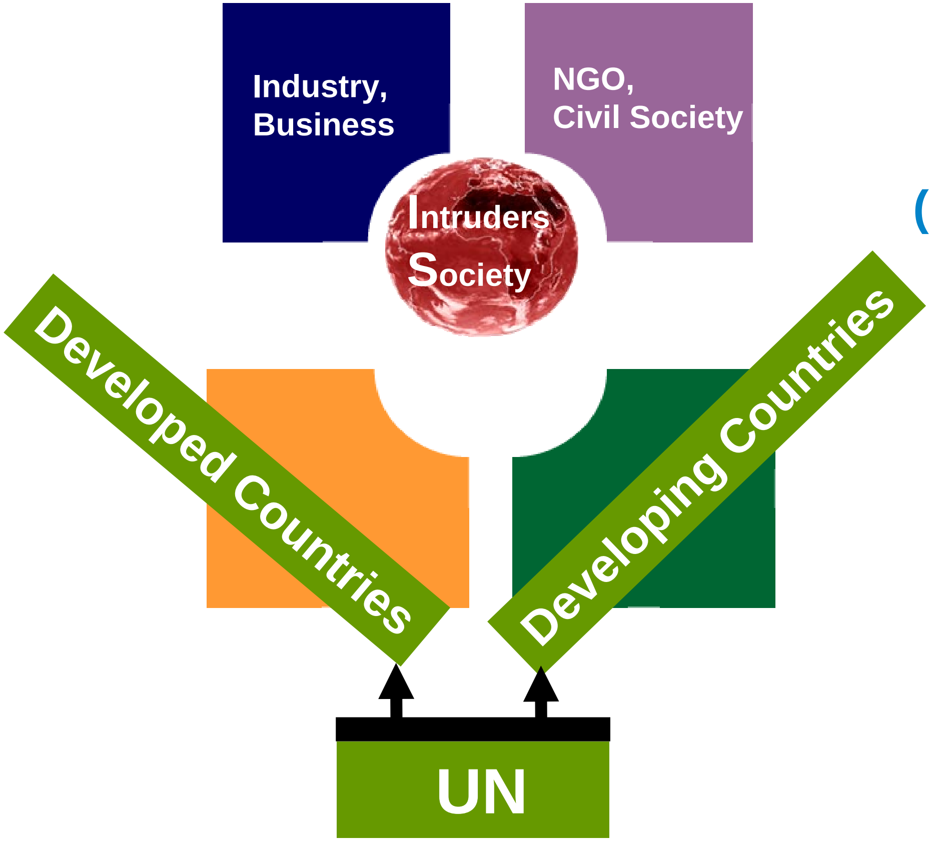
-Promote Collaborative Technology Research and Development such as advisory information on potential threats and emerging incident situations, exchanging information on information security reviews and facilitation of research activities in specific area.

-Providing inputs and/or recommendation to help address legal issues related to information security and emergency response across regional boundaries

-Report all development and propose recommendations on decided issues and resolutions to the OIC Secretariat / IDB Secretariat for further action.

IT STILL POSSIBLE TO DREAM & LOVE

(Beautiful mysteries Of BRAIN & LIFE)



Industry, Business

NGO, Civil Society

Intruders Society

Developed Countries

Developing Countries

UN