Tunisia's experience in establishing the first public CSIRT in Africa, as a case example for developing countries, and some guidelines and schemes for International cooperation

Prof Nabil SAHLI,
Header of the Cert-Tcc
National Agency for Computer Security, CEO
TUNISIA
n.sahli@ansi.tn

Plan

I- Fast overview about the Tunisian experience and strategy in ICT security,
II- Insights into the Cert-Tcc's activities

- Overview about **Awareness & Information actions**
- Overview about **assistance for Incident Handling**
- Overview about **the launch of Watch and Alert Center**
- Overview about **Professional Training & Education actions**
- Overview about **Open-source** strategy
- Cooperation with associations and at the International level

III- Some urgent needs of developing countries and schemes for International cooperation
IV- Some points to take into consideration, while creating CSIRTs in developing countries

I- Fast overview about the Tunisian Experience in ICT Security

Historical events

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

Task :

Sensitize policy-makers and Technical staff about security issues.

& ***create 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** ») **:**

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

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

❑ **January 2003 : The Council of Ministers, headed by the President, and dedicated to informatics and IT Security, decided :**

❑ creation of a National Agency, specialized in ICT Security

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

❑Introduction of Mandatory and Periodic Security audits

(Pillar of our strategy)

❑ Creation of a "body of certified Auditors" in ICT Security

\+ accompanying measures (launch of masters in ICT security, …)

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

- **Promulgates Mandatory and Periodic Security Risk Assessment,** for national IS

- **Obligation to declare** security Incidents that could affect **others** IS, with guarantee of **confidentiality**, by Law.

- *Created and defined the tasks of the* **National Agency for Computer Security**

National Agency for Computer Security

MINISTRY OF COMMUNICATION TECHNOLOGIES
TUNISIA

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

(created under the **Ministry of Communication Technologies)**

In charge of the **implementation** of the ***National plan and strategy*** in ICT 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 ICT Security;
- Promulgation of **Best Practices** and **Regulations**
- Fostering the **development of national solutions** in the field of ICT security and promoting such solutions in accordance with the National **Priorities** ,
- Consolidation of **training and re-training** in the field

And the **follows-Up** of the execution of the measures related to **mandatory security audits**

II- Overview about CERT-TCC

(Computer Emergency Response Team
- Tunisian Coordination Center

SERVICES & ACTIVITIES

CERT-TCC
Computer Emergency Response Team- Tunisian Coordination Center

Governmental CSIRT, officially launched in 2004 & Hosted by the National Agency for Computer Security (Ministry of Technologies of Communication)

(16 people → Will collapse in the future : Some of its activities will be delegated to private CSIRTs)

CERT-TCC

Computer Emergency Response Team- Tunisian Coordination Center

Awareness Activities

Cert-TCC 's **Awareness** activity :

✓ Development of awareness material (french, arabic) : Brochures (8), CDs (3), small guides (10)

✓Organize Booths in ALL national and regional Exhibitions (7 in 2007)

✓Co-organizes & Intervenes in all IT Conferences & Workshops (16 during 2007, 62 from 2005)

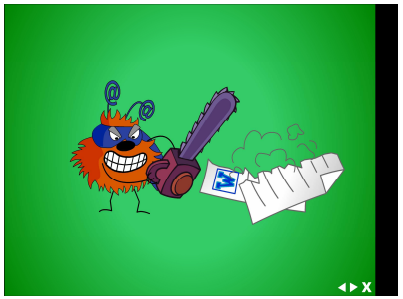
+ Publish Awareness material through our Web site and mailing-list .

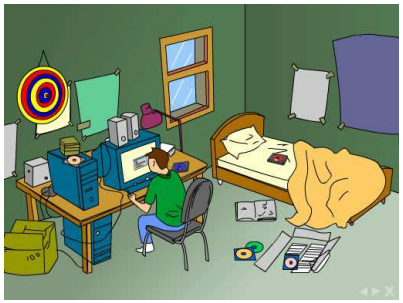
- Rely on **the Press**, for raising awareness of ***Broad population***
  - Press-Relations position in CERT-TCC (a journalist→ Motivation of papers and furniture of information material to Journalists).

→ Participate in the animation of weekly rubrics in **6** Regional and National **radio stations** (3 in 2005) + preparation of awareness modules for students in Journalism

- **Youths and parents awareness** :

  - Development of a **manual& Quiz (for schools), 3 "Cartoons", pedagogic game, brochures**.





-Organisation of awareness workshops for **Youth and children**, In Collaboration with specialized centers and associations (4 workshops during 2007)

-Organisation of short training sessions for educators and teachers of high schools

& In preparation : awareness sessions in High schools

+ A "Citizen assistance Desk "

→ Where **Home users** can **bring their PC to solve security problems or install free security tools** (free for domestic use : anti-virus, PC firewall, anti-spam, ..) and get light training, brochures, guides, CDs…

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

IT professionals and Policy-makers :

Best Awareness Instrument

=

Promulgation by Law of Mandatory (Now annual) Security Audits

(Law N°5-2004 related to ICT security) :

- **Obligation** for national companies (ALL public + "big" and sensitive private ones) to do **Periodic (Now annually) security risk assessments of their IS.**

+ Organization of the field of Security audits

- → Audits are Made by **CERTIFIED auditors** *(**from the private sector**),*
- → *definition of the process of certification of auditors*
- → *definition of the content of the audit missions* **(ISO 1 7799 + Technical vulnerabilty assesment)** *and of the process of follow-up*

+ The audit mission includes awareness sessions, made by auditors for ALL the Staff
(Including Live simulation of attacks)

CERT-TCC

Computer Emergency Response Team- Tunisian Coordination Center

Information & Alert Activities

National Agency for Computer Security

Information & Alert

Ministry of Communication Technologies Tunisia

- Broadcasts information (Collected through the monitoring of multiple sources) through our Mailing-List(s) :
  (103 e-mails sent, in 2007)

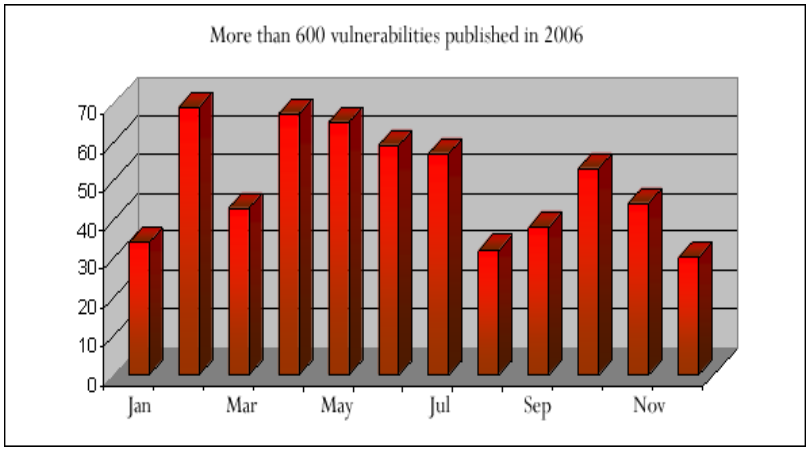
Various Rubrics :

- **Threats** :

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

- **Information** :

.Tools	Threats	.Open-source	Events



1- Highly critical vulnerability in ……., which permits ……
2- Medium crtical 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)

+ Development of **Guides** on Best practices and Open-source security solutions
  (~30 small guides)

National Agency for Computer Security

Ministry of Communication Technologies
Tunisia

CERT-TCC
Computer Emergency Response Team- Tunisian Coordination Center

ISAC
and Incident Response

National Agency for Computer Security

Ministry of Communication Technologies Tunisia

A **Watch- center** (based on **open-source solutions**), which permits to monitor the National Cyber-Space security
→ Early Detection of **Mass attacks** and analysis of their impact.
(First prototype, deployed during WSIS, November 2005)

→ **open-source AGENTs**
(NIDS, Traffic-analysis agents, honey-pots,..)

Corporate Networks

IDCs

ISP

Honeypots

System "Saher"

Cert -Tcc SOC

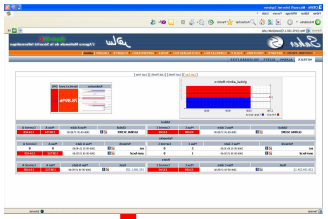
Events gathering Database

→ Gathering and filtering of large sets of network logs to identify Mass attacks (Worms, cyber-attackers, distributed scans,…)

Hot-Line

+ Real-Time Monitoring of DNS/ Mail/ Web servers

Analysis& correlation (automatic Alert-Triggers)



Reaction Plan « AMEN »

"Amen" : **Alert Handling plan**
--- **Global** Reaction Plan.
--- Establishment of **Coordinating Crisis Cells** (ISPs, IDCs, Access Providers).
With Cert-Tcc acting as a central **coordinator** between them

+/-

Alerting the Community

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

Disaster-Recovery Infrastructures

✓ launch of a national Project for building a **National Disaster-Recovery Center**
(managed by the National Center for Informatics, with funds from the World Bank)

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 may affect other Information Systems

With Guarantees for 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 for the preservation of **confidentiality** and are liable to penal sanctions

- Private and public organizations should **trust** the CERT-TCC
  → **Call for assistance**

CERT-TCC provides :

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

+ Acting for the creation of **corporate IRT in some sensitive sectors** (E-gov, finance, Transportation, Health,..)

CERT-TCC

Training & Education

Training of Professionals

- Creation of a ***Task Force of*** **Trainers** in ICT Security.
  → Launch of training modules for ***trainers*** (100 trainees from the private sector, during 2006)
  → In 2007 : 4 additional training modules

- ***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*** *of e-government applications*
    - ❖ *Preparation of 2 training sessions for* **judges and Law enforcement** ***staff****.*

- *Motivating* ***Private*** *Training Centers*
  → In partnership with the private sector : Project for the Launch of a **Regional Training center** in ICT security
  (Start-Up fund from the World Bank) .

- Encouragement of professionals for getting international certifications :
  - Organization by Cert-Tcc of **CISSP training sessions**

Education

-Collaboration with academic institutions for :

- The launch of **Masters** degrees in IT security :

(Motivation: A master degree in IT security permits the **Obtention of NACS Certificatio**n).

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

→ **Now : 7 masters** (3 publics & 4 privates universities/ 1 Regional).

(other regional masters in preparation for 2007-2008)

- Inclusion of **security modules** (awareness) inside **all** academic and education Programs :

→ Training sessions for **teachers** (800 new teachers from high schools trained in 2006)

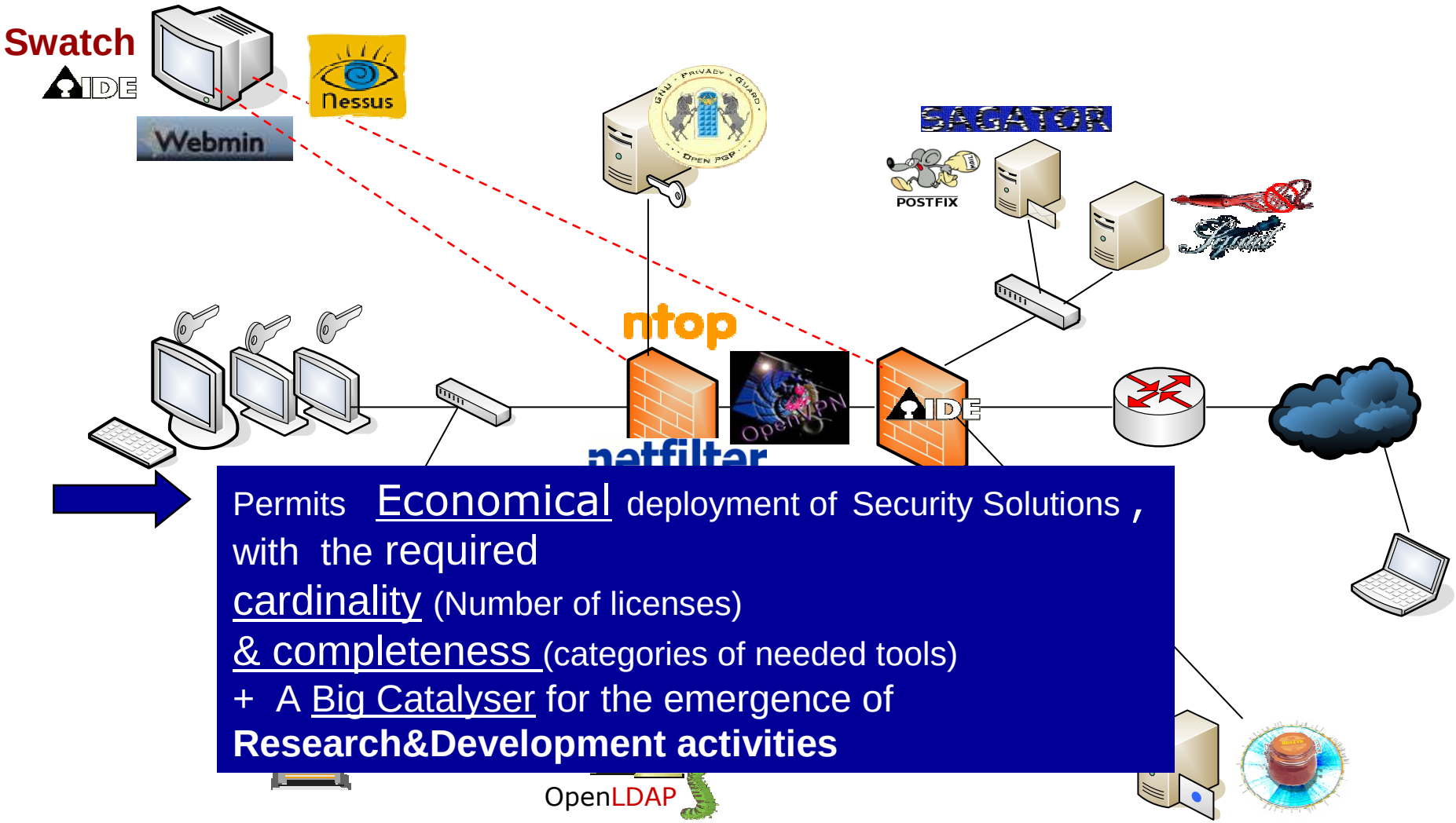
→ Development of ***pedagogical material and programs***.

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

Open-source

Open-source = a "Seducer"

An extremely Rich repertory of "free" and efficient security tools



Permits Economical deployment of Security Solutions , with the required cardinality (Number of licenses) & completeness (categories of needed tools)
+ A Big Catalyser for the emergence of **Research&Development activities**

Strategy of Cert-Tcc in Open-source :

First Step : Raise **Awareness** + create **Skills** (private sector) , in open-source tools' deployment (installation, training, "maintenance")

Then → Launch of projects of "Customization" of open-source solutions

End → Launch of Real Research/Development activities

- Acting in **Raising awareness of professionals** about the benefits (&limits) of the deployment of open-source tools (training, workshops, guides, , …)
& consolidating training at the university + sensitizing private sector :

- Formulation (funds) of **4 projects for the "development" of security tools (from open-source**) by 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 **Secretary of state of Scientific Research**)
- Collaboration, with the university for the launch of a **Research laboratory** specialized in open-source security tools.

Induction of Synergy between National actors

Rely on Associations (NGO)

Motivate the creation of specialized Associations in ICT security :

• An ***academic*** association was **launched** in 2005: **ATSN** ("Association Tunisienne de la Sécurité Numérique").
• Another ***professional*** association in 2006 : **ATESI** ("Association Tunisienne des Experts de la Sécurité Informatique").

- In collaboration with associations (NGO) :

-**Organisation of awareness actions (15 seminars and workshops in 2006) with IT associations (ATIM, ATSN, JCI, ATAI, ...)**

- Motivation for the creation of Technical Workgroups (self-assessment methodologies adapted to the size of our IS, guides of best practices, models of books of Tender of Offers, ..)

- Implication in the evaluation of action Plans & their revision

(Project of preparation of a national survey in 2007, with the associations)

.

International Collaboration

+ CERT-TCC is **CLEARLY COMMITED :**

- 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 regional collaborative programs

- To establish Partnership with the **private sector** to promote network security technologies

- To participate in international efforts for the setup of a **regional CERT (African),** which will help regional countries in launching CSIRT.

About Developing & LD Countries

III-Some specificities and needs of Developing&LD Countries and a scheme for International cooperation

Developing & Less Developing Countries

- **Potential future "Reservoir of hackers"**
(unemployment, lack of entertainment, feeling of injustice and need for expression ….)
- **Infrastructures = "Open-Platform" for intruders (relays of Spam, Botnets, Phishing, …)**

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

Urgent actions (« Aid »)

In fact, SELF-INTEREST of the International community to avoid creation of cyber-criminality Heavens

Safer (Cyber-)World

Characteristics and Needs of Developing countries

Lack of awareness :

International actors should :

- Help Raising **awareness of Politicians & policy-makers**
  + Motivate **Development Banks** programs, for providing **funds**.

- Provide assistance for establishing National strategies and plans in ICT security
  → **Clear frameworks** adapted to the stage of development of each country

Lack of Skills

- Assistance for the launch of **Local CSIRT** (**as "NESTs" for Local Experts' task-force**)
  → training & assistance

- Assistance for building up a task-force of **trainers**

Lack of Tools (modest economies)

- Encourage the use of **Open-source tools** (in complement to commercial ones)
  - → Raise awareness about capabilities (and limits) offered by open-source tools
  - → Need for **trainers** in the open-source field

- Push the "proactive approach" **as a balance** to the lack of protection tools,
  - → Importance of best practices.
  (need for awareness material & training).

+ **Software editors** should forsee the possibility :
  - To provide **special prices** (accordingly to the "level of life" and as a marketing action for, hopefully, growing markets)
  - To multiply the offer of free licences, for domestic users .
  - To study the possibility to **pursue the maintenance** of "old" versions (security patchs) of their products.

- **ISPs connecting Less-DC** (small ISPs) should foresee how to Help for the provision of "centralized" protection (NIDS, Anti-virus, parental-control tools, ..) at their level & cheap **assistance and training** (IRT teams).
+ Pay the needed **attention** & take precautionnary measures, against the abuse of Less-DC Infrastructures(botnets, spam relays, ..) by « their » Intruders,.

"How To " help

(+ "be helped" in case of attacks originating from those countries)

→ Assist for the launch of CSIRTs

CERT = "Good&practical Model" for efficiently **canalizing a** Multi-stakeholders assistance

Opportunity for a " Regional Approach"

(similar state of development/Language/culture, same Time/Address Block/, …)

→ Combine skills of all stakeholders from BOTH Developed and Developing Countries, for the Launch of Regional CERTs (Africa , South America, ..), to which will be assigned the task of :

→ Providing assistance for the launch of local CSIRTs in their areas.

+ Raising attention of Regional Organisations (organization of African unity , Arab league , ASEM, GCC ...) → push political awareness

+ Raising awareness of Regional Development Banks (African Development Bank, Inter American Development Bank,IDB, ...) → provide funds .

National Agency for Computer Security

Ministry of Communication Technologies Tunisia

Call For Contribution

In preparation :
An International conference,
devoted to **Developing Countries**
Hosted by TUNISIA
&
sponsored by ITU,
March 2008 **(To be confirmed)**

+ CERT-TCC 's **COMMITMENT** : ***With guidance from forums specialized in the field and International organisations :***

→ Share our little experience ***(errors, success stories)*** ***and provide , free of charge, our modest logistic (trainers, open-source skills, awareness material, ..), to help other regional countries in the launch of CSIRTs + ..***

→ Assistance to RITA (Rwanda's CSIRT project)

→ Cert-Tcc is part a project of an OIC-CERT (funds from IDB)

IV- Some points to take into consideration, while creating CSIRTs in Developing Countries

(coming from the Tunisian experience)

Awareness

→ Start by focusing on sensitizing **policy-makers and professionals** about computer security issues and their impacts

→ **Target the media**, to exploit their ability to reach wider population (creates a press relations position)

- Start a **specialized mailing list**, with inclusion of awareness and assistance sections

- Initiate the development of **awareness material** (brochures, guides, ..), using existing materials developed by other CERTs, and adapting it for local requirements and languages

- Organize **periodic awareness campaigns** + put people in touch with the reality of risks (simulation of intrusions , presentation of statistics about attacks, associated vulnerabilities and financial losses and impacts)

- Prepare awareness campaigns for **youth and parents**

- Encourage **synergy** between security experts and the launch of **specialized associations**

- Raise **professionals**' awareness about the advantages and limits of **open-source tools** and inform **domestic users** about the existence of **free** commercial security solutions

Training

- Reinforce the potential of **Trainers** in ICT Security (provides training)

- Provide assistance for the launch of **specialized diplomas** (Masters, ..) in ICT Security (provide trainers, promote professional recognition)

- Encourage the Introduction of ***basic (awareness) courses in academic and scholar programs*** (provide programs, documentation and trainings for trainers)

- Encourage professionals for obtaining **International certification** (CISSP, …) (motivate & provide training)

Mechanisms and tools for reinforcing the security of the National Cyber-space

- Provide assistance for **incident handling** : a hotline + task force, able to intervene in case of emergency, 24 Hours and 7 day/week.

- Draft **reaction plans for mass attacks**, based on coordination between key actors (ISPs, access providers, IDCs).

- Start deploying a system permitting the **monitoring and early detection of mass attacks,** using, in case of lack of funds, solutions from the open-source field.

- Provide training for the deployment of **open-source security tools** (In case of economic difficulties for deploying commercial solutions).

-In case of lack of protection tools at the user level, motivate **ISPs** to provide "up-stream" protection at their level (anti-virus and anti-spam gateways, NIDS, etc.).
+ assistance for domestic users, in deploying **commercial security tools, free for domestic use**

-Promote the use of **parental control** tools, as well as measures against pedophilia activities

+ Additional "special" tasks : Help **draft national strategies and implement security plans** in ICT security, and try to **coordinate** between all stakeholders, concerned by the reinforcement of the security of national IS

- Launch **surveys** (priorities, volume of actions, …), to perfect national strategies and plans in ICT security

-Identify national "heavy" investments to engage (disaster recovery infrastructures, mass Training...) and **regroup efforts** made to this end

-Define **rules** (national information security policies, procedures and practices) for the follow-up of efficient security plans, taking into account the reality of human and financial resources

-Reinforce the role played by the **private sector** (motivate the public sector to call for private services, provide training for trainers and help for certification, establish rules for fair competition, motivates private investment)

-Motivate the emergence of **academic associations** in the field of ICT security, with the goal of motivating national R&D in strategic fields

-Establish national cyber crime and information **security councils** that include the participation of all stakeholders (private sector, government authorities, telecommunications service providers, law enforcement officials, the judiciary, NGOs).

Regulatory level :

The CSIRT could also help through :
-providing assistance in adopting **norms and certification procedures**, related to ICT security tools and procedures

-helping **enhance the skills of judicial and law enforcement bodies** in dealing with cyber-crime, by providing **technical assistance** and **training** opportunities and ensure that codes of conduct and best practices are reflected in the criminal procedure laws of the country, where appropriate

-participating in defining and implementing **regulatory rules and mechanisms for controlling abuses** (copy right, respect for privacy, consumer protection, etc.) and promotes **self-regulation in the private sector**

-strengthen **international collaboration** in dealing with cyber security incidents (mutual assistance with CSIRTs, transfer of proceedings, etc.), and encourage acceptance of, and **compliance with, international legal instruments**.

THANKS YOU

Prof Nabil SAHLI,
Header of the Cert-Tcc
National Agency for Computer Security, **CEO**

n.sahli@ansi.tn