The security, safety, continuity, sustainability, and robustness of the Internet (Morocco)

With the development of the internet as a global infrastructure for business and as a new tool and resource for productivity and added value for economic sectors and for the public administration, the threat of cyberspace has become a central topic for national and international security.

Every day, news websites and social networks report attacks against personal accounts, businesses and government agencies.

In response to the increasing number of attacks in the cyberspace and to secure the ICT infrastructure and networks, protect the citizens and ensure the business continuity of critical Information Infrastructures, the Moroccan government has adopted the digital trust program as a support measure to implement the Moroccan National Strategy for Information Society and Digital Economy "Digital Morocco 2013", launched in October 2009.

Ensuring business trust, enhancing security capabilities, securing critical information infrastructures and combating cybercrime are the ambitions of the Moroccan digital trust plan.

Through the digital trust plan the Moroccan government has identified the following initiatives and actions to develop the security, safety, continuity, sustainability, and robustness of the Internet:

Initiative 1: Update and reinforce the legislative framework

- Upgrade/update the legal and regulatory framework related to the Information Security System (ISS), digital trust, electronic exchange, protection of personal data, protection of online consumer

Initiative 2: Put in place appropriate organisational structures

- Set up a committee in charge of Information Systems Security,
- Put in place a centre of coordination and response to incidents related to Information Systems Security (ma-CERT) at a national level,
- Support the creation of PKI provider for ensuring electronic signature,
- Encourage the development of backup sites and data center to ensure the Business Continuity of Critical Information Infrastructures of Morocco.

Initiative 3: Promote and sensitise social operators to information systems security

The improvement of the Information Systems Security and the response to cybercrime requires the development of a real culture of security. In addition to developing a good understanding of Information Systems Security, this awareness

program should allow individual citizens to be aware of the measures taken to promote digital confidence.

- Raise awareness within the children, young people and parents of the Cybersecurity and cyberconfidence issues,
- Implement a sensitisation and communication program about ISS in order to raise awareness within the children, young people, parents, administrations and enterprises of the Cybersecurity and cyberconfidence issues,
- Integrate the Information Security Systems (ISS) in the Higher Scientific Education and training programs,
- Set up and develop training programs in ISS for judges and magistrates,
- Set up and develop training programs in ISS for administration employees/officials,
- Encourage training in ISS for the private sector.

Realizations

As a result of actions undertaken within the framework of the digital trust program to develop the security, safety, continuity, sustainability, and robustness of the Internet, Moroccan government has succeeded to:

Initiative 1:

- Adopt the law no 07-03 related to the information Systems infractions,
- Adopt the law no 53-05 related to electronic exchange of legal data to facilitate the use of encryption means and electronic certification,
- Adopt the law no31-08 related to the protection of online consumers,
- Adopt the law no 09-08 related to the protection of the personal data,
- Elaborate a global study of the legal instruments related to the information technology, cybersecurity and cybercrime to strengthen the Moroccan legal act and fill existing gaps that may be an obstacle to ensure the digital trust and combat cybercrime,

Initiative 2:

- Create the Strategic Committee of Information Security Systems responsible for elaborating the policy related to the protection of critical information infrastructure,
- Create the General Directorate of Information Security Systems,
- Create the Morocco-Computer Emergency Response Team (maCERT) to respond to security incidents, coordinate responses at the national level and propose different services related to the handling of these incidents, the analysis of their vulnerability and the restoration of systems under attack,
- Create the National certification authority and service provider of electronic certificates.

Initiative 3:

- Implement an awareness and communication program about cybersecurity and safe internet
- Provide training programs on cyber security for engineering and IT students to enlarge the pool of ISS experts
- Provide training programs on cyber security for legal professions (magistrates, judges),
- Encourage innovation in cybersecurity, electronic signature, cryptography… and support private initiatives and activities in ISS.