

## Cybersecurity related R&D Activities

- [Information Technology Industry Development Agency “ITIDA”](#):

Plays a pivotal function in developing the local IT industry by **Collaborative Funded Projects**. ITAC’s programs include **Cybersecurity as one of its strategic areas**, move a product concept out of the ideas shed, through the proof-of-concept and prototyping stages, until it turns into a complete product ready to hit the market.

- [NTRA “R&D department”](#):

was established in 2007 with key objectives **of supporting national research projects and activities** in the area of telecommunications, **Cybersecurity**, emerging technologies and applications, and aiming to bridge the gap between academic activities and technical developments from one-perspective and policy visions and real market needs from another.

- [Egyptian Ministry for Scientific Research](#):

has embarked on an ambitious exercise to overhaul Science and Technology (S&T) activities in Egypt. Science, Technology & Innovation Funding Authority (STDF) has stimulated the Egyptian scientific society by **funding distinguished research papers** and establishing scientific partnerships with scientists from many advanced countries in order to keep track of quickly advancing technology.

- [Egyptian Supreme Cybersecurity Council “EG-CERT”](#):

Program to support **scientific research and development and cybersecurity industry development** is one of the key strategic programs of the National Cybersecurity Strategy.

This program supports cooperation initiatives and projects between research institutions and local companies, especially in the fields of: advanced malware analysis, cyber forensics, protecting and securing industrial control systems, developing devices and systems for securing systems and networks, encryption and e-signature, protecting ICT infrastructure, securing cloud computing and protecting major databases. High priority must also be given to establishing national centers/labs to adopt the systems, devices, software and applications used at key agencies and critical infrastructure.