State of the art:

In a stage of over changing technology worldwide which has more impact to the cyberspace and the internet of thing (IoT), cybersecurity plays an important role in society by employing different sources and people across all cultures, as well as the latest technology which also includes data mining, analysis, behavioural trends, authentication and data protection to name just few. Cybersecurity needs to address different holes and challenges to ensure security and reach a vision of international pace or equilibrium especially when Cyber-Terrorism is playing a major role in our actual and future society acting and aiming the destruction of the wellbeing of our modern society by imposing and de-centralised power through justified means of political, historical, social and religious nature. Therefore, cyber-terrorism will show different actors on the cyber-stage for example a criminal who’s acting upon is personal gain would be part of a chain reaction inside a “Pandora box” and this is the challenge cyber-security is facing at this very stage.

The reason for this challenge is the shattered chaos the crimes are proliferating so security just realise that the human intervention must be more active part on the scanning or screening process.

Current state:

Identity Verification through biometrics, creation and use of effective credentials, user account control with not access to full administrator privileges and full intervention through remote access into software’s are some elements that are commonly used. However, before any intervention would be employed there are monitoring technique for scanning purpose which at the first stage will be done through “machine learning” computers which are analysing clusters words and only after if required human intervention will take actively part to separate key point trough data mining and after applying direct monitoring. Many techniques for monitoring are still classified which are not including a pure algorithm but other technologies will be used to suit the purpose. That said security holes are still many and most of them need to be addressed in different ways.

Foresight state:

* Global education on how to protect data from threats and how to prevent them.
* Honing biometrics.
* Potentiate cloud services with significant cuts on physical data retention.
* Extendedly develop artificial intelligence and machine learning.
* Potentiate Data Processing and Data Setting.
* Implementing more human application and enhancing critical thinking.

Future Stage:

The clouds technology will be gradually transferred over a period of ten years.

Services will be divided roughly in three main sectors: business, public and security sector with free access or paid one. Clouds services are already on the arising for business use offering operating business platforms.

It will be broadening educational security awareness through schools, university and research field, including into work places as the future will bring the exertion of more devices will introduce a security approach for a safer data management.

Data analytics will be potentiated/refined through the applications of AI logarithm a more feasible and efficient approach to human language widening phrases clusters search. While biometric sophistication will be used to ensure authentication is secured with a possible use’ elimination of passwords.

The implementation of it would be gradually introduced through law requirements and technological education of the global society.