State of the art:

In a stage of over changing technology worldwide which has more impact to the Cyberspace and the Internet of Things (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 a few. Cybersecurity needs to address different concern and critical gaps to ensure security and to reach a vision of international pace, especially when the global scenario contains Cyber-Terrorism and or Cyber-Crime who is a dangerous player in our current and future society. Cyber-attacks exist with the aim to disrupt and put at risk our society’s wellbeing by imposing a global de-centralised treat for different reasons that are identified as political, historical, social and religious. The overspread crime inside of the IT’s Pandora box increases the many risk’s elements that are deterrent for ensuring a safer place.

Current state:

Some cyber-security elements that are commonly used are:

* Identity verification through biometrics,
* Creation and use of effective credentials, authentication and passwords,
* User account control with not access to full administrator privileges, and file access to encrypted data.
* Full monitoring through remote access into operating system, firewalls and network security.

Before human intervention is employed there are machine monitoring technique for scanning purpose that would identify and isolate cluster data to extrapolate behaviours traits that are potentially identified as risk. After the extrapolation of distinctive identification traits, a more closer analysis will be applied through a direct human monitoring technique which will enable a more comprehensive way to define the psychological profile that has being highlighted and selected by computers data patterns analysis.

Foreseen Future State:

Even though this approach is being adapted and classified as the best method so far, still cyber-attacks are always more de-centralised and difficult to predict in a more precise and direct way.

To tackle these critical issues on a more chaotic and overcrowded cyberspace, awarded technologies are more directed towards their implementation.

*Clouds services/Servers:*

One of the designed scenario are clouds services. Clouds services are predicted to grow in a fast and profitable fashion there are being sponsored and advertised as one of the advantageous technological advancement. Their features are just versatile and modern and futuristic way to overcome storages issues such as data corruption as result of an obsolete or redundant hardware storage, it is the smart way to adapt better and faster, to an encompassing and overcharging tech revolution. It is the cheapest way to approach the need to have archives. Major business will be accountable to manage those servers which are offering clearly data back-up and recovery. Clouds are directed so that all data can be centralised and monitored central servers’ points so to minimise any potential risk and overcome critical issues.

*Biometric:*

Biometric will be the next step, google and other web-sites as well as pre-recorded telephone messages are perfecting voice recognition. Even though issues are found on voice recognition of foreigner languages these honing biometrics will be one of the cool future features which will bring the complete elimination of passwords to leave place to unmistakable personal authentication.

*Machine Learning/AI chatterbots:*

Algorithm will be directed and developed so that will include a vaster repertoire of human language so that can be develop learning machine that will surely predict identified phrases cluster which will facilitated the scanning and screening of potential treats with more accuracy with a faster collection of data mining.

*Merging of Human and Computer Cyber Defenders:*

In conjunction with computers cyber defenders will be increased the human factor. Security positions demands by public and private sector will increase as more direct human intervention will be essential to a better risk definition and assessment so to ideally abolish cyber-crimes.

*Towards Global Education:*

Promoting global and community awareness towards cyber-threats so to direct prevention and data protection. This is implemented already into universities and will be extended in various educational platforms as well as into work places as the predicted exertion of technologies will make employees accountable towards data security, data protection and data management.

*Other technologies:*

Other awarded developments towards cyber-security are:

* Inspired by bitcoin it is likely to be implemented the Blockchain and cryptocurrencies so that clusters data traces are left as information-record for any virtual monetary transactions.
* Autonomous vehicles (AV) are already tested for implementation; all technology is available that said it will likely be introduced gradually in a decade cycle of a time frame, so not to have a strong economic impact and to moderate and promote a social progressive adaptation to it. Its implementation will be based on a mix between biometric and location as well as subliminal reliance’s message.
* Robots are the next linking piece between usability as AVs and centralise data retrieval.

Even if their future use is blurry for technological development reasons. Robots usage requirements are already defined. Beside their employability as extensions to supports human daily activities as well as for security/military purpose, robots will be also used as data collectors of user behaviour; by utilising biometric sensors as well as the application of AI languages or Natural Language Processing, they will promptly elaborate the user profiles not just locally but also globally. Robots will be also linked to clouds services for data collection purpose, thus all data will be stored to some comprehensive data-storage points ready to be easily accessed and retrieved.

* Raspberry Pis, Arduinos, Makey Makeys and others will be taking place and developed for a future replacement of current computers with Hard Drive Diskless ones.

All people worldwide will be affected, probably privacy boundary will be thinner however cybersecurity is most necessary to ensure a safer society where the priority need to be addressed towards other wrights more important, such as life protection, prevention of any disruptions on society’s infrastructure by for example targeted electricity black-out or infiltration aiming weapons’ control, prevention of data theft and or leaking.

As we’re going towards a brighter future all global society, including my family, friends and I will enjoy the countless advantages from different technologies that will offer smoother infrastructure that will improve many aspects of our daily life; from life extension to enhanced health system to support our elderly, our differently-abled and every-day users. Cybersecurity implementation it’s most needed as technology improvement will bring unfortunately an increasing cyber-threat hence it is it is essential to ensure the safeguard of civil liberties and wrights worldwide through applied regulations, even if it could imply some privacy loss.

References:

Moving forward with cybersecurity and privacy (2017) - Source: PwC.

A Comparative Analysis Of Cybersecurity Initiatives Worldwide By Myriam Dunn for WSIS Thematic Meeting on Cybersecurity (2005).

Cybersecurity: Threats Challenges Opportunities - ACS Cybersecurity Guide (2016).

A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies By G. Nikhita Reddy, G. J. Ugander Reddy (2014) - Source: https://www.researchgate.net/publication/260126665.

DARPA Wants to Merge Human and Computer Cyber Defenders By Joseph Marks (2018) – Source: Nextgov

Cloud Computing By Wong Tsz Lai, Hoang Trancong, Steven Goh.

Introduction to Cloud Computing architecture. White Paper - 1st Edition, June 2009.

5 Building Blocks Influencing the Cloud Evolution By Edris Amiryar (2018) – Source: Nextgov.

Safety and Liability of Autonomous Vehicle Technologies By Richard Ni and Jason Leung (2015).

Cloud Networked Robotics By Koji Kamei, Miki Sato, Shuichi Nishio, and Norihiro Hagita (2012).

How Form Automation is Democratizing Government Services By Jonathon Ende (2018) – Source: Nextgov.