**Annex**

## Key Research Themes of the NUS-Singtel Cyber Security Research and Development Laboratory

---

Over the next five years, research staff at the NUS-Singtel Cyber Security Research and Development Laboratory will work towards developing enabling technologies and prototypes under four research themes:

- **Network, Data and Cloud Security:** There is growing interest and demand in the gathering, sharing and analysis of large volumes of data. Efforts under this research theme will focus on the common objective of facilitating secure sharing of information and resources via security services.

  NUS will contribute expertise in computer network design, database systems, and data privacy techniques, including new cryptographic mechanisms, to create new services that will allow secured communication and storage of private, sensitive data in the cloud, for both individuals and enterprises.

  By integrating advanced technology with its Software-Defined Networking (SDN) capabilities, Singtel would have greater situational awareness of devices and networks. This allows Singtel to detect and mitigate cyber attacks and roll-out cyber security services in a more flexible and scalable manner.

- **Predictive Security Analytics:** Research activities under this theme will involve developing technologies that automate and update organisations' predictive capabilities for early detection of potential network and software threats through analysis of a variety of data streams.

  NUS will contribute expertise in machine learning, software security, human behaviour modelling and network domain knowledge to create advanced techniques and tools to enable IT systems to detect security threats and other abnormal activities, such as malicious software intrusion or leakage of data, more accurately and in real time.

  With predictive security analytics, Singtel Managed Security Services can receive timely intelligence, and allow its security professionals to quickly take pre-emptive action to thwart any impending cyber threats. Further, through the aid of analytics, enterprises and government agencies will have access to relevant data and information that will help in making more accurate decisions.

- **Internet-of-Things (IoT) and Industrial Control Systems (ICS):** Cyber-physical systems collect and process fine-grained and real-time information from sensors. By integrating the information with computational algorithms and physical systems, enterprises can enhance the capability, performance, and resilience of engineered and industrial control systems. However, these systems are exposed to a wide range of vulnerabilities.

  This research theme aims to develop a security platform that allows service providers to monitor, detect, and mitigate threats and unusual cyber activities. NUS will contribute expertise in developing security solutions for cyber-physical

systems, from applications and software to the physical communications medium, to develop future services such as immunity platforms for next-generation defence and protection for Internet-of-Things (IoT) devices and ICS.

Capabilities to protect the collection and exchange of data by various types of sensors will have a wide range of important applications, including smart homes, smart energy grids and smart transportation systems.

Singtel will use advanced machine learning, mathematical models and telemetry data gathered from users, mobile devices or applications and networks to develop predictive threat analysis and intelligence. This would allow Singtel to predict, discover and identify emerging, abnormal security activities before they happen.

- **Future-Ready Cyber Security Systems:** Under this theme, researchers will look into the implementation of quantum technology for communication security.

  Traditional security mechanisms will become vulnerable to new attacks as data is vulnerable to cyber eavesdropping by hackers. In addition, current technology is limited as it does not provide true end-to-end data encryption.

  At the Lab, researchers will use the quantum properties of light particles to facilitate the secure exchange of digital information in future quantum computers and networks. NUS, which is home to the Centre for Quantum Technologies, will provide expertise in Quantum Key Distribution (QKD), or quantum cryptography, as well as in the design and implementation of quantum-based computation and communication infrastructures.

  Singtel will use QKD to deliver encrypted information over its dark/optical fibre network to provide secure communications between intended senders and recipients.