PRESS RELEASE

18 September 2017

CYBERSECURITY SECTOR GETS $16 MILLION BOOST TO SPUR MORE READY-TO-USE SOLUTIONS

More than $16 million will be invested into new cybersecurity projects aimed at strengthening Singapore's cybersecurity research and development (R&D) capabilities and developing cyber tools and technologies that can be readily adopted for public and industry use. Nine research projects have been awarded a total of $15.6 million under a grant call by the **National Cybersecurity R&D Programme** [1] to develop capabilities in key technology areas to meet Singapore's cybersecurity needs. Another six projects have been awarded close to $0.6 million under a seed grant call by the **Singapore Cybersecurity Consortium** to spur the commercialisation of cybersecurity technologies. These efforts will strengthen Singapore's cyber defences, and prepare our critical infrastructure and digital services against rising global cyber threats.

National Cybersecurity R&D Programme Grant Call

2 The National Cybersecurity R&D Programme Grant Call was launched in November 2016 to develop Singapore's cybersecurity R&D capabilities to meet the security needs of the Public Sector and of Singapore as a whole. Three key priorities in cybersecurity R&D have been identified for the grant call, namely, National Security, Critical Infrastructure and Smart Nation. Research projects that examine key technology areas including Effective Threat-based Detection, Analysis and Defence, Secure IoT System, and Security-by-Design and Testing of Emergent Technologies were welcomed.

3 The emphasis of the grant call is on the translational and deployability of ideas and technologies. Dual use of new capabilities outside of the Public Sector is encouraged. To ensure scientific rigour and commercialisation capacity, only proposals submitted by Singapore-based companies in collaboration with Institutes of Higher Learning, research institutions or government agencies were eligible. Twenty three proposals were received. Out of these, nine projects were awarded based on the significance of their research areas to create impact in Singapore, and potential for translation and commercialisation. See **Annex A** for details on projects.

4 One of the awarded projects by local start-up Attila Cybertech Pte Ltd seeks to improve the security of cyber-physical systems. It will use machine learning techniques to detect anomalous behaviours in computer systems. Carried out in collaboration with researchers from the Singapore University of Technology and Design (SUTD), the technology will be trialled on a testbed at SUTD. **Mr David Ong, Chief Executive Officer of Attila Cybertech Pte Ltd, said:** "When successfully validated, this tool will complement network intrusion detection systems with insights generated through Deep Learning that

[1] The National Cybersecurity Research & Development Programme is coordinated by the National Research Foundation Singapore, the National Security Coordination Centre, Cyber Security Agency, the Ministry of Home Affairs, the Ministry of Defence, Government Technology Agency, and the Economic Development Board to promote collaboration among government agencies, academia, research institutes and private sector organisations.

will provide cyber-physical system operators with greater cybersecurity protection and visibility on the asset utilisation."

5 Another project by local company i-Sprint Innovations Pte Ltd uses blockchain technology to provide secure protocols and mechanisms for the e-logistics sector, such as tamper-proof financial records and shipping documents. Innovations in this area can help to reduce administrative, legal and execution costs. Carried out in collaboration with Nanyang Technological University, this project will also develop a prototype of a cargo tracking system for goods. The outcome of this project will be incorporated into i-Sprint's product identity solution, AccessReal, which provides a platform for product identity, counterfeit detection, track and trace, logistic tracking, big data analytics and direct marketing.

6 **Mr Albert Ching, Chief Technology Officer of i-Sprint, said:** "The outcomes of the research project will enable our AccessReal product to leverage the immutable and decentralised nature of blockchain with smart contract implementation. This will help to eliminate conflicts of interest and increase trust among suppliers by improving the transparency, integrity and confidentiality of information in a supply chain network. This will further enhance our product capabilities to gain a bigger share of the global logistics market in the digital age, and help position Singapore as a world leading hub for logistics and supply chain management."

7 On the awarded projects, **Mr George Loh, Director (Programmes) of the National Research Foundation Singapore and Co-Chair of the National Cybersecurity R&D Joint Programme Committee, said:** "Cybersecurity research is crucial in building up Singapore's cybersecurity experts as well as developing technologies and capabilities, which are necessary for Singapore's Smart Nation vision. We are confident that these nine newly-awarded projects will spur closer collaboration among researchers, industry and the government to translate technologies into effective solutions that address the rising cyber threats worldwide."

Singapore Cybersecurity Consortium Seed Grant Call

8 The Singapore Cybersecurity Consortium was launched in September 2016 to promote research, commercialisation and training in cybersecurity. A national programme anchored at the National University of Singapore (NUS), it aims to encourage use-inspired research, technology translation, manpower training and technology awareness among industry members. In June 2017, a seed grant call was launched to invite proposals from consortium members for proof-of-concepts of new cybersecurity technologies and innovative ideas. Ten proposals were received. Out of these, six projects were awarded based on their technical merits and potential for commercialisation. See **Annex B** for details on the projects.

9 One of the awarded projects is carried out by local cyber company, Custodio Technologies Pte Ltd, in collaboration with StarHub and SUTD, to research and develop a method of identifying Internet of Things (IoT) devices, while preserving subscriber privacy. This is an essential building block in the development of a full-fledged solution, providing telecommunications providers with the ability to detect potentially malicious traffic and to protect their infrastructure by blocking attacks.

10 **Mr Gil Gilad, Chief Technology Officer of Custodio Technologies Pte Ltd, said:** "Custodio is honoured to accept this grant from the Singapore Cybersecurity Consortium.

We are proud of our cooperation with StarHub and SUTD and see this project as a cornerstone in our work to develop innovative cyber early warning technologies and solutions. This project has the potential to mature into a solution that will provide telecommunications providers advance detection and mitigation capabilities to safeguard critical national ICT and Smart Nation infrastructure, in Singapore and around the world."

11 Another project awarded under the consortium's seed grant call aims to develop a proof-of-concept testing environment for cybersecurity technologies. It provides simulations of various network-based attack scenarios and techniques, and serves as a demonstration platform for solution developers. This project is a collaboration between NUS, local start-up InsiderSecurity and the National Cybersecurity R&D Lab.

12 **Associate Professor Chang Ee-Chien from the Department of Computer Science at NUS School of Computing, said:** "This project is a synergistic collaboration between industry and academia to tackle real-world cybersecurity challenges. Businesses and agencies may use this testing environment for rigorous security solution testing, demonstration and validation. In addition, security solution providers could also use this platform to raise their capabilities and engage potential clients, especially those from overseas, more effectively in the near future."

13 On the awarded projects, **Professor Abhik Roychoudhury from the NUS School of Computing, who is the Academic Director of the Singapore Cybersecurity Consortium, said:** "The inaugural seed grant call by the Singapore Cybersecurity Consortium attracted joint submissions from industry and academia containing innovative proposals – both for benchmarking existing cybersecurity solutions, and for developing new solutions. The new solutions proposed range from readily translatable solutions for enhancing resilience of critical infrastructures and home IoT network, to future-proof cybersecurity solutions that securely manage traffic of unmanned aerial systems. Success of such endeavours would encourage more meaningful interaction between industry and academia in Singapore, and will help secure Singapore's cyber-infrastructure of today and tomorrow."

Annex A

Details of Awarded Projects under the National Cybersecurity R&D Programme Grant Call

1.	**Project Title: Advanced anti-malware solution using deep learning**
	This project aims to develop an anti-malware solution based on deep learning technologies. The solution should reach a high accuracy at identifying fresh and stealthy malwares, and be able to adapt quickly to new trends and changes in the malware population. It should also be able to detect new malwares in a timely manner, while incurring a small memory and central processing unit footprint. The solution should be able to decide in real-time if a running application is malicious, without affecting other applications' performance. This project is a collaboration between Singapore-based company **SecureAge Technology Pte Ltd**, the **National University of Singapore** and the **Cyber Security Agency of Singapore**.
2.	**Project Title: Advanced-intelligent anomaly detection system**
	This project aims to improve the security of cyber-physical systems, by employing data analytics to detect the physical constraints and anomalous behaviours in large-scale cyber-physical systems. It will develop methods to continuously access data from multiple sources of a cyber-physical system and develop a machine learning system for anomaly detection. The detection solution developed will be validated in a testbed at the Singapore University of Technology and Design. This project is a collaboration between Singapore-based start-up **Attila Cybertech Pte Ltd** and the **Singapore University of Technology and Design**.
3.	**Project Title: Building next-generation secure environments on smartphones for critical mobile applications**
	This project aims to develop secure environments on smart phones for critical mobile applications. This allows applications dealing with sensitive or private information to be run in secure environments, hence protecting the data and code execution for critical applications. This project is a collaboration between Singapore-based company **i-Sprint Innovations Pte Ltd** and the **Singapore Management University**.
4.	**Project Title: Cybersecurity protocol and mechanism for e-logistics of dangerous goods tracking using block chain**
	This project aims to study the cybersecurity protocol and mechanisms for e-logistics using smart contracts and blockchain technology. Blockchain technology can provide distributed consensus, protection against tampering and de-centralised ledger maintenance, hence reducing administrative, legal and execution costs. The project will also develop a proof-of-concept cargo tracking system for goods. This project is a collaboration between Singapore-based company **i-Sprint Innovations Pte Ltd** and **Nanyang Technological University**.

5.	**Project Title: Malware source attribution through multi-dimensional code-feature analysis**
	This project aims to create automated solutions for malware source attribution, as it has becoming increasingly challenging for human analysts to analyse malware and identify its evolving trend and developers. This will help malware analysts and security response teams to understand the similarities in malware used across cyber attacks more efficiently, and identify the attacker quickly. This project is a collaboration between **Kaspersky Lab Singapore Pte Ltd**, the Singapore laboratory of Russia-headquartered cybersecurity and anti-virus provider Kaspersky Lab, and the **National University of Singapore**.
6.	**Project Title: Research & develop assessment tool and system – OpsTrace**
	This project aims to improve the security assessment of industrial control systems by developing the OpsTrace tool. The tool can passively monitor the entire industrial control system's assets in real-time, map out the network architecture and identify any unauthorised device in the network topology by comparing it with the approved system architecture diagram. This project is a collaboration between Singapore-based company **Excel Marco Industrial Systems Pte Ltd** and **Nanyang Technological University**.
7.	**Project Title: Secure, privacy-preserving data exchange/computation platform for the Smart Nation**
	This project aims to create innovative encryption and secure data management technologies to enable secure multi-party computation platform for business-to-business and business-to-government transactions. By creating encryption algorithms and methods for secure data computation, encrypted data can be shared between multiple un-trusted parties while keeping shared data secret and business user anonymity. This project is a collaboration between **Acronis Asia Research and Development Pte Ltd**, the Singapore R&D centre of global data protection provider Acronis, and **Nanyang Technological University**.
8.	**Project Title: Smart binary-level vulnerability assessment for cyber-attack prevention**
	This project aims to develop a commercially-viable product that automates the detection of vulnerabilities and their causes in a timely manner, regardless of the platform. This provides a vulnerability detection and analysis tool that is platform agnostic, efficient and requires minimal human or expert intervention. This project is a collaboration between Singapore-based start-up **Scantist** and **Nanyang Technological University**.
9.	**Project Title: Testing for blockchain security by design**
	This project aims to develop a security reference architecture for blockchain, and identify components in the design that requires security controls to be implemented. It will also create capabilities and tools to validate the security by design of the blockchain components. This project is a collaboration between **TNO Singapore**, the Singapore office of The Netherlands Organization for Applied Scientific Research (TNO), and the **Singapore University of Technology and Design**.

Annex B

Details of Awarded Projects under the Singapore Cybersecurity Consortium Seed Grant Call

1.	**Project Title: An integrated safety-security approach for engineering Unmanned Aerial Systems (UAS) traffic management solutions**
	This project aims to develop an integrated safety-security approach for Unmanned Aerial Systems (UAS) traffic management (UTM) systems, through a safety-security co-analysis and risk assessment framework. It will establish best-practice and safety-and-security-by-design guidelines for this approach. This project is a collaboration between **Advanced Digital Sciences Center,** a Singapore-based research centre that is an affiliate of the University of Illinois at Urbana-Champaign, Singapore-based company **Nova Systems & Engineering**, Canada's **Critical System Labs Inc**, **University of Illinois at Urbana-Champaign**, and Singapore-based company **NSHC Pte Ltd**.
2.	**Project Title: Identification of IoT devices behind NAT while ensuring the preservation of data privacy**
	This project aims to develop a method to passively map out Internet of Things (IoT) devices in users' premises while preserving privacy. This will help build a security layer between IoT devices and telecommunications infrastructure to monitor and detect potentially malicious traffic. This project is a collaboration between Singapore-based company **Custodio Technologies Pte Ltd**, the **Singapore University of Technology and Design** and **StarHub**.
3.	**Project Title: Learning to detect anomalies in cyber-physical systems with generative adversarial networks on networked sensor time series data**
	This project aims to develop a machine learning approach using generative adversarial networks. It will simultaneously train a deep learning network to model normal behaviour in a cyber-physical system, while also detect anomalies due to cyber attacks in the networked sensor time series. It will be evaluated using a realistic complex cyber-physical system dataset from the Secure Water Treatment Testbed. This project is a collaboration between Singapore-based company **ST Electronics (Info-Security)** and the **National University of Singapore**.
4.	**Project Title: Mobile (iOS) security study for cyber-attack prevention**
	This project aims to build an assessment framework for iOS malware, which is less studied than Android malware. The framework aggregates iOS malware into a database and performs a suite of analysis and classification techniques to derive a risk score, and hence recommend actions to fix or mitigate the malware impact. This project is a collaboration between **PayPal** and **Nanyang Technological University**.

5.	**Project Title: No more snake oil - Objective evaluation environment for security technologies**
	This project aims to develop a proof-of-concept testing environment for security technologies, which could also serve as a demonstration platform for solution developers. It will include simulation of various network-based attack scenarios and techniques, and an automatic scoring or measurement framework. It will be validated through applications on Singapore-based start-up InsiderSecurity's technologies. This project is a collaboration between Singapore-based start-up **InsiderSecurity**, the **National Cybersecurity R&D Laboratory**, and the **National University of Singapore**.
6.	**Project Title: Secure dataset sharing for remote artificial intelligence innovations on clinical data**
	This project aims to develop a platform for secure sharing and consumption of research data, with automatic data sensitisation, centralised access control, cryptographic key exchange, and a client application to execute user codes on the data. It will be built on Singapore-based start-up Cloak's existing platform and tested with clinical data from the Agency for Science, Technology and Research (A*STAR) Bioinformatics Institute's partner hospitals. This project is a collaboration between Singapore-based start-up **Cloak Pte Ltd** and **A*STAR Bioinformatics Institute**.