LAKSHMAN KADIRGAMAR INSTITUTE
OF INTERNATIONAL RELATIONS AND STRATEGIC STUDIES

TAKEAWAYS

LKI *takeaways* are executive summaries of LKI events.

Developing Robust Cyber Security Mechanisms in the 21st Century: Lessons from the UK'

An LKI Roundtable with Dr. Henry Pearson
UK's Cyber Ambassador

Discussants: Dr. Rohan Samarajiva, Chairman, Information and Communication Technology Agency (ICTA); and Mr. Lal Dias, CEO, Sri Lanka Computer Emergency Readiness Team | Coordination Team (Sri Lanka CERT)

Reported by Chattalie Jayatilaka and Malinda Meegoda*

October 2019

***Chattalie Jayatilaka** is a Research Assistant at LKI. **Malinda Meegoda** is a Research Associate at LKI. These *Takeaways* summarise the insights and discussion at a recent LKI event. They are not the views of the reporting author or the institutional views of LKI, and are not a complete report of the event

Three key takeaways from the round table discussion with Dr. Henry Pearson:

1. **The exponential growth of the global digital economy has brought enormous opportunities—particularly for developing countries—as well as new security vulnerabilities targeted by various criminal elements.**

2. **Since 2011, UK's cyber security strategy has evolved into a sophisticated and well-resourced cluster of institutions aimed at reducing the risk of the UK's use of cyberspace, exploiting cyber opportunities, and improving knowledge capabilities and decision making.**

3. **Each country must develop a cybersecurity strategy that is tailored to its own specific needs, but it is crucial for government and the private sector to cooperate on measures that can safeguard the integrity of the nation's digital infrastructure.**

Introduction

- Dr. Henry Pearson, UK's Cyber Ambassador, addressed a Foreign Policy Round Table titled 'Developing Robust Cyber Security Mechanisms in the 21st Century: Lessons from the UK,' on 14 October 2019 at the Lakshman Kadirgamar Institute (LKI).
- The discussants were Dr. Rohan Samarajiva, Chairman, Information and Communication Technology Agency (ICTA), and Mr. Lal Dias, CEO, Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT). The session was moderated by Dr. Ganeshan Wignaraja, Executive Director of LKI.
- The round table was attended by senior officials from the Ministry of Foreign Affairs and other government agencies, as well as senior representatives from academia, the media, armed forces, think tanks, and the private sector.

Takeaways from Dr. Henry Pearson's Presentation:

<u>Developing a National Cyber Security Strategy</u>

- The British cybersecurity strategy of 2011 identified two key problems with the UK's approach to cybersecurity.
    - While the UK was achieving important outcomes, it was well below the scale and pace of change required to stay ahead of the fast moving threat.
    - Secondly, there was no single authority on the UK's cybersecurity environment to provide guidance and leadership on key national issues.
- The British government, therefore, decided to be more active in cyber defence, and significantly enhanced the levels of cyber security across UK networks. This was coupled with a boost in funding, and the creation of the National Cybersecurity Centre (NCSC).
- The current National Cyber Security Strategy (the Strategy) runs from 2016 to 2021. It has a £1.9 billion budget.

- The 2016 National Cyber Security Strategy identified three core principles; Defend, Deter, and Develop.
    - **Defend**: Improve sensible advice, and support of critical national infrastructure to improve active cyber defence;
    - **Deter**: Improve intelligence gathering, develop offensive cyber capabilities, increase investment in law enforcement, and create a national cyber crime agency; and
    - **Develop**: Encourage innovation in industry, utilise world leading research in universities, and create a pipeline of young talent for the future of cyber defence.

Responsibilities and Roles of the National Cyber Security Centre

- After much deliberation, the British government incorporated the National Cyber Security Centre (NCSC) within the institutional framework of Government Communications Headquarters (GCHQ), UK's signals intelligence agency.
- In 2018, NCSC led the response efforts on 516 major incidents. Cyber threats assessments in the UK are categorised based on the scope and potential of the vulnerabilities posed.
    - These categories include; localised incidents (C6), moderate incidents (C5), substantial incident (C4), significant incidents (C3), highly significant incidents (C2), and national cyber emergencies (C1).
    - Responses to the threat categories of C1, C2 and C3 are typically led or coordinated by the NCSC, while most of the C4 to C6 is partially or wholly lead by local or regional units.
- The NCSC aims to work closely with industry contacts by pairing top practitioners in the cyber security industry with government counterparts, ensuring knowledge and expertise from all areas of the field can be combined to share intelligence and fight threats.

Developing Skills in Cyber Security Related Education and Research

- The NCSC advises universities on curricula to increase the standards of undergraduate, and graduate-level cyber security programs.
- The NCSC continues to certify Masters level programs in cyber security, and has expanded into certifying bachelors degrees in cyber security at various Universities in the UK.
- The NCSC created four research institutes that are multi-disciplinary through the participation of a number of existing universities.

Takeaways from the Remarks by Dr. Rohan Samarajiva and Mr. Lal Dias:

- Sri Lanka's current primary defence against cyber threats is CERT which does not have the capacity to be the only front against cyber threats. The government must develop further legislation and a skilled workforce to ensure a safe digital environment.
- Sri Lanka is vulnerable to cyber attacks, and the state must ensure a basic level of security to businesses that have based their operations in Sri Lanka to sustain an

efficient economy. Effective cyber security policy is key to ensuring an innovating economy.

- Government, cybersecurity agencies and industry in Sri Lanka must work together in a cooperative manner to exchange knowledge and information to create a safe digital environment.

- **Takeaways from the Discussion**

- The NCSC works on a non-regulatory model. It works to support industry, and government without a restrictive legal environment in order to facilitate its role as the helpful middleman in the tech sector.
- Sri Lanka ranks 84th out of 193 on the Global Cybersecurity Index which is an indication of its slow progress. CERT and cyber security agencies require more funding and capital expenditure for the establishment of a security centre to increase efficiency.
- Public-private partnerships are the cornerstone to success in cyber defence. There are limits to the capabilities of the government, and the private sector should, therefore, be able to step in instead.
- The internet knows no geographic boundaries, and nations must work together to share experience and knowledge to create a better digital environment and economy.

Suggested Reading

Gunawardena, N. (2018). *Convention on Cybercrime*. [online] The Lakshman Kadirgamar Institute. Available at: https://www.lki.lk/publication/convention-on-cybercrime/ [Accessed 31 October 2019].

HM Government. (2016). *National Cyber Security Strategy 2016 to 2021*. [ebook]. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 [Accessed 31 October 2019].

Steed, D. (2019). *The UK's National Cyber Security Strategy Beyond 2021: The International Dimension.* https://rusi.org/commentary/The_UKs_National_Cyber_Security_Strategy_Beyond_2021_The_International_Dimension [Accessed 31 October 2019].