INQUIRY INTO THE TRADE SYSTEM AND THE DIGITAL ECONOMY

Submission to the Australian Parliament Joint Standing Committee on Trade and Investment Growth

A response from Kaspersky Lab

Kaspersky Lab highly appreciates the opportunity to make this submission, and welcomes the Inquiry into the Trade System and Digital Economy.

Digital transformation of Australian business and society will deliver enormous growth potential for Australia – advanced digital technologies (Big Data, robotics, artificial intelligence, blockchain technology, the Internet of Things, cybersecurity) and their inclusion into economic sectors will raise efficiency and provide the foundation for innovative, diversified and dynamic economy.

As a global cybersecurity firm we call for a regulatory environment that fosters collaboration between the domestic industry and international cybersecurity vendors in building the strong, dynamic and competitive cybersecurity ecosystem of Australia, and supports its integration into the cybersecurity value chain.

1. Keeping the digital marketplace open

1.1. Cybersecurity is among the areas bringing massive challenges and opportunities to Australian businesses. Australia's Cyber Security Strategy rightly focuses on Growth and Innovation as one of its five pillars. As the success of Australian cybersecurity businesses will largely depend on their ability to access new markets, the Government promises to '*support Australia's cyber security sector to expand and promote their capabilities*'[i]. We argue that facilitating digital trade liberalization shall continue to be an important feature of both Australia's International Cyber Engagement Strategy[ii] and the nation's Cyber Security Strategy and regulatory practices.

1.2. As outlined by the Cyber Security Sector Competitiveness Plan of Australian Cyber Security Growth Network (ACSGN – currently AustCyber), capitalizing on Australia capabilities in software development will require significant investments in research and development[iii]. The flagship national R&D initiatives, such as Singapore's National Cybersecurity R&D Programme, of which Kaspersky Lab is among the grant recipients, require close cooperation

between the domestic firms and academia and multinational cyber vendors[iv]. The access to the sizable market, as well as to the high-quality local talent and expertise incentivizes cybersecurity vendors to gradually expand their sales-office presence and choose Australia as the hotspot of company's R&D efforts. The regulatory restrictions do the contrary, reducing the potential to attract investments, knowledge and expertise from the foreign companies and MNCs.

2. Addressing regional divides in cybersecurity regulation

2.1. The interconnected global Internet creates a wide variety of benefits for both nation states and citizens. However, it has also led to the emergence of new types of transnational threats. Governments increasingly rely on protectionist policies or restrictive regulatory practices in response to those threats, citing national security concerns. Increasing regulatory fragmentation in this field – from Europe's GDPR to China's Cybersecurity Law - inevitably leads to the so-called "Cyber-Balkanization" or 'splinternet'.

Australia is proudly one of the most open economies in the world, however the recent OECD Economic Survey notes that the country's advantage in lighter regulation has been eroded[v]. We foresee that in certain circumstances Australia's Security of Critical Infrastructure Bill[vi] may limit the choice of cybersecurity products available to Critical Infrastructure Assets (CIAs) operators, pushing the owners away from the thorough risk assessment of suppliers towards 'tick-the-box' compliance.

2.2. 'Localizing' or 'regionalizing' cybersecurity regulation does little to help Australian enterprises to gain a share of the global $93 billion information security market projected for 2018 by Gartner[vii] or the growing $22 billion market of industrial cybersecurity (by 2023[viii]).

The breakthrough technologies driving this market -- such as AI and machine learning -- require access to large troves of historical threat data from across the globe to develop efficient threat detection and prediction models. Even the relatively niche segments of IoT security (estimated to reach USD 547 million in 2018[ix]) and automotive cybersecurity (estimated to reach USD 32 million by 2021[x]) will depend on accessibility of local markets to the technologies developed in US, China, Israel, Japan, Russia, Europe and elsewhere.

Regulatory fragmentation may lead to reciprocal measures and/or similar regulatory initiatives in other markets in the Indo-Pacific region in particular, hampering the potential of a global digital marketplace, and affecting the exportability of Australian cybersecurity products and services

3. Building trust to cybersecurity products and services providers

3.1. Third-party trust is a fundamental requirement for any large-scale implementation of a network security product[xi] – be it public key cryptography or critical infrastructure protection. Kaspersky Lab recognizes that trust is not a given – it must be repeatedly earned through an ongoing commitment to transparency and accountability. We strongly believe that cybersecurity industry needs to address the question of trust with more robust criteria than the geographic location of company's headquarters – be it Melbourne or Moscow.

3.2. One of the widely accepted benchmarks of trust in cybersecurity is ICT certification and standards – both driven by government entities, such as Australasian Information Security Evaluation Program (AISEP) and the proposed EU Cybersecurity Certification Framework or industry-specific certification such as OPC Foundation's Certification and Compliance program. The certification process, however, is often fragmented, slow and costly for companies, and it risks failing to keep up with the disruptive changes of the digital age.

As Microsoft noted in its feedback to EU Cybersecurity Package, a 'one-size-fits-all' cybersecurity certification (such as the one envisioned by the participants of the cyber security–focused 360° Discovery Exercise conducted by RAND Corporation and the National Security College at The Australian National University[xii]), may not be ideal, especially if its scope covers vastly different ICT products and services, from critical infrastructures to consumer goods[xiii].

In our view, a customized certification with multi-layered assurance is a better solution. We call for adopting a risk-based approach to cybersecurity, which relies on performance-based standards and industry's best practice, enables private and public sectors actors' flexibility to mitigate their risks as they see them, and adopts a sufficiently light regulatory framework to drives innovation and growth in Australia's cyber-security market. Australia's own specific cybersecurity requirements should consider compatibility with (and/or incorporation of) international standards in order to encourage inbound investment and access to external markets by domestic industry.

4. Stimulating workforce capacity building, job creation and diversity

4.1. Digitalization, while bringing direct benefits for industry and society, may pose significant threats. With many jobs set to disappear[xiv], the demand for other qualifications is on the rise. The acute shortage of cybersecurity professionals is currently estimated at 1.8 million people globally by 2022[xv]. In Australia the conservative estimated shortage of cybersecurity

professionals is set to reach at least 11,000 professionals over the next 10 years – that is more than the size of cybersecurity workforce currently employed by all external cybersecurity services providers' in Australia[xvi].

We commend the Government strategy to enable people to acquire cyber skills through initiatives such as Australia's first national skills-based cyber security qualifications offered by TAFE[xvii], and will seek opportunities to support Australia's educational institutions in the provision of those programs.

4.2. Kaspersky Lab calls for greater women's inclusion in cyber and tech through tailored programs. In 2017 we undertook a study[xviii] and revealed that only 11% of young people have met a woman who works in this industry. Increasing participation of women in cybersecurity is one of the key objective of the national Cyber Security Strategy[xix], and we hope to see more initiatives in this field.

Higher education and vocational training alone may not be enough – a healthy labor market of cybersecurity professionals will be driven by competition between the firms investing in workforce development and on-the job training. The measures should also include Australia's SMEs, which on the one hand are increasingly affected by cybercrime, and on the other are at forefront of offering innovative cybersecurity solutions, products and services.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company registered in the United Kingdom with 35 representative offices in 31 countries on 5 continents, and operations in 200 countries and territories worldwide. Kaspersky Lab regional office for Australia and New Zealand is located in Melbourne, Victoria. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users and 270,000 corporate clients around the globe are protected by Kaspersky Lab technologies. Kaspersky Lab is the first largest security software vendor in the European retail market and a consumer market leader in a number of European countries. Kaspersky Lab Global Transparency Initiative is a reaffirmation of the company's commitment to earning and maintaining the trust of the company's customers and partners every day.

Contact

For more information, or to discuss the contents of this submission in more detail, please contact Oleg Abdurashitov, Head of Public Affairs Asia Pacific

References:

[i] Australia's Cyber Security Strategy https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
[ii] Australia's International Cyber Engagement Strategy http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_1_digital_trade.html
[iii]Cyber Security Sector Competitiveness Plan. Australian Cyber Security Growth Network, April 2017 https://www.acsgn.com/wp-content/uploads/2017/04/Cyber-Security-SCP-April2017.pdf
[iv] "S$15.6 million awarded to 9 public-private research projects under Singapore's National Cybersecurity R&D programme", OpenGov, October 2017 https://www.opengovasia.com/articles/8024-s156-million-awarded-to-9-public-private-research-projects-under-singapores-national-cybersecurity-rd-programme
[v] OECD Economic Surveys Australia, March 2017 http://www.oecd.org/eco/surveys/Australia-2017-OECD-economic-survey-overview.pdf
[vi] "Infrastructure owners and operators: Proposed Security of Critical Infrastructure Bill", Holding Redlich, October 2017 https://www.lexology.com/library/detail.aspx?g=3ec7577c-89ae-4c42-878c-b22e7e083449
[vii] "Gartner: Worldwide information security spending to hit $93B in 2018", CSO Online, August 2017 https://www.csoonline.com/article/3219165/it-careers/gartner-worldwide-information-security-spending-to-hit-93b-in-2018.html
[viii] Industrial Cybersecurity Market - Global Forecast to 2023 https://www.researchandmarkets.com/research/2qw22d/industrial
[ix] Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016 https://www.gartner.com/newsroom/id/3291817
[x] Automotive Cyber Security Market - Global Forecast to 2021 https://www.marketsandmarkets.com/Market-Reports/cyber-security-automotive-industry-market-170885898.html
[xi] Public Key Infrastructure White Paper, Government of Canada, February 1998 http://hca.nat.gov.tw/download/011.pdf
[xii] "Exploring Cyber Security Policy Options in Australia". RAND Corporation and Australian National University, https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2017-08/issues_and_options_paper-3_2_0.pdf
[xiii] Microsoft Feedback to EU Cybersecurity Package https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477/feedback/F7992_en
[xiv] 5 million jobs to be lost by 2020. World Economic Forum, January 2016 https://www.weforum.org/agenda/2016/01/5-million-jobs-to-be-lost-by-2020/
[xv] "Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher" (ICS)2, June 2017 https://www.prnewswire.com/news-releases/global-cybersecurity-workforce-shortage-to-reach-18-million-as-threats-loom-larger-and-stakes-rise-higher-300469866.html
[xvi] Australian Cyber Security Growth Network, "Cyber Security Sector Competitiveness Plan" April 2017 https://www.acsgn.com/wp-content/uploads/2017/04/Cyber-Security-SCP-April2017.pdf
[xvii] National TAFE Cyber Security Program Launch https://www.acsgn.com/training/
[xviii] Beyond 11%: A study into why women are not entering cybersecurity. Kaspersky Lab, January 2018 https://d1srlirzdlmpew.cloudfront.net/wp-content/uploads/sites/86/2017/11/03114046/Beyond-11-percent-Futureproofing-Report-EN-FINAL.pdf
[xix] Supporting the next generation of women in cyber. Department of the Prime Minister and Cabinet, November 2017 https://www.pmc.gov.au/news-centre/cyber-security/supporting-next-generation-women-cyber