LCQ1: Strengthening information security

â€‹Following is a question by Dr the Hon Johnny Ng and a reply by the Secretary for Innovation and Technology, Mr Alfred Sit, in the Legislative Council today (May 25):

Question:

It has been reported that due to geopolitical changes, certain foreign governments often impose sanctions on the Chinese Government, including cutting off the export of certain technological products to China and banning China's use of such products. There are even hackers in western countries waiting for opportunities to launch cyber attacks on China in attempts to affect the operation of the Chinese Government and related organisations, and Hong Kong may also be affected. On strengthening information security in Hong Kong, will the Government inform this Council:

(1) whether it has assessed the impacts of the aforesaid restrictions imposed on technological products and cyber attacks on the information security (including computer systems and applications) of various government departments, and what plans are in place to strengthen the information system security and incident response capability of various government departments, so as to ensure that their operation and services are not affected;

(2) how it detects and blocks foreign hackers' intrusions and attacks targeting the computer systems of various government departments, and whether it will formulate relevant management, technical and security mechanisms; and

(3) given that cyber attacks may undermine the operation of critical information infrastructure, causing chaos to the daily lives of members of the public and bringing about economic impacts, whether the Government will regulate the cyber security standards for such infrastructure, and require infrastructure operators to assume greater cyber security responsibilities?

Reply:

President,

I am grateful to the question raised by Dr the Hon Johnny Ng. The Government attaches great importance to information security, including cyber security. We have been tackling information security issues through a multi-pronged strategy to mitigate the risks brought by cyber threats. Bureaux and departments (B/Ds) actively implement multiple layers of security measures to monitor, detect and block potential malicious attacks on their information systems and networks, and take commensurate measures promptly to ensure the security of the Government's systems and data. We also closely collaborate with related organisations and departments to enhance the overall defence

capability and resilience of Hong Kong against cyber attacks, and strive to build Hong Kong as a safe and secure smart city.

Having consulted the Security Bureau, my reply to the questions raised by Dr the Hon Johnny Ng is as follows:

(1) & (2) The Government has been closely monitoring the trends of cyber attacks and the associated security threats around the world to ensure the continuity of normal operation of the Government's systems and services.

In procuring information technology (IT) equipment products, Government departments place high importance to the relevant security standards and the support services offered by the suppliers in addition to functionality and compatibility. Moreover, we also remind departments to procure IT and communication products from diverse sources so as to manage the risks of potential restriction imposed on technology products.

In light of targeted and organised cyber attacks on a global scale, the Office of the Government Chief Information Officer (OGCIO) has formulated a comprehensive set of Government IT Security Policy and Guidelines (Policy and Guidelines), which are reviewed and updated regularly with reference to the latest international standards and industry best practices. All B/Ds must abide strictly by the Policy and Guidelines to ensure the security of government data and information systems. The OGCIO also regularly conducts compliance audits for B/Ds to ensure the compliance of their information systems with relevant security requirements.

On technical aspect, the Government commits itself to the overall information security measures to respond to all types of cyber security threats. Leveraging on modern cloud technologies, the Government launched the Next Generation Government Private Cloud Infrastructure Platform in September 2020 to provide a more secure, reliable and scalable infrastructure for the digital government services of different departments. The platform has so far supported over 350 digital government services. At present, the government websites and systems have adopted multiple layers of security measures including data encryption, firewalls, content delivery networks, scrubbing function, intrusion detection and prevention systems against distributed denial of service (DDoS), anti-malware software, endpoint protection solutions and real-time monitoring tools, to detect, block and tackle different types of security threats. In addition, the Government also implements spam filtering systems to tackle malicious email attacks.

On the other hand, in order to respond to emergency incidents effectively, the OGCIO has established the Government Computer Emergency Response Team Hong Kong to assist and co-ordinate departments in handling the work of computer emergency response and incidents. The OGCIO also organises the Inter-departmental Cyber Security Drill annually to strengthen the capability of government departments in defending and responding to cyber security incidents.

Meanwhile, the Government attaches great importance to the co-operation

and information sharing with the Mainland and other regions on cyber security in order to respond to the cyber security threats in a prompt and timely manner. The OGCIO has also joined the Forum of Incident Response and Security Teams and the Asia Pacific Computer Emergency Response Team, etc, and is working closely with the National Computer Network Emergency Response Technical Team/Coordination Centre of China on exchanges, co-operation and notifications of cyber security intelligence. We also actively participate in related activities organised by these organisations.

(3) A safe business environment is crucial for fostering economic development, prosperity and stability. Critical infrastructures are of great significance to the normal operation of the society. If the information systems, information networks or computer systems of the cricial infrastructures are being disrupted or sabotaged, the normal operation of their main facilities may be affected, and will seriously jeopardise the economy, people's livelihood, public safety and even national security.

â€‹The increase in cyber attacks in recent years has brought substantial challenges to the cyber security of critical infrastructures around the world. Currently, Hong Kong does not have specific legal requirements on the cyber security of critical infrastructure. Therefore, in addition to industry best practices as well as guidelines and requirements on cyber security imposed by individual regulatory authorities, the Government is currently making preparatory work to clearly define the cyber security obligations of operators of critical infrastructure through legislation, with a view to strengthening the cyber seucrity of critical insfrastructure in Hong Kong. In formulating relevant cyber security standards, reference will also be made to standards adopted by other jurisdictions and around the world. The Government intends to launch a public consultation exercise by the end of this year.

Thank you again for the question of Dr the Hon Johnny Ng. I am eagerly looking forward to more exchange and cooperation with LegCo Members in promoting and strengthening the information security of Hong Kong together. Thank you, President.