

## **The Hong Kong Chartered Governance Institute**

### **Submission**

**The Law Reform Commission of Hong Kong  
Sub-Committee on Cybercrime**

**Consultation Paper on:**

**Cyber-Dependent Crimes and Jurisdictional Issues**

19 October 2022

By email only: [hklrc@hkreform.gov.hk](mailto:hklrc@hkreform.gov.hk)

The Secretary  
Sub-Committee on Cybercrime  
The Law Reform Commission  
4th Floor, East Wing, Justice Place  
18 Lower Albert Road  
Central  
Hong Kong

Dear Sirs,

## **Consultation Paper on Cyber-Dependent Crimes and Jurisdictional Issues (Consultation Paper)**

### **About HKCGI**

The Hong Kong Chartered Governance Institute (Institute/HKCGI), formerly known as The Hong Kong Institute of Chartered Secretaries, is the only qualifying institution in Hong Kong and the Mainland of China for the internationally recognised Chartered Secretary and Chartered Governance Professional qualifications.

With over 70 years of history and as the Hong Kong/China Division of The Chartered Governance Institute (CGI), the Institute's reach and professional recognition extend to all of CGI's nine divisions, with more than 40,000 members and students worldwide. The Institute is one of the fastest growing divisions of CGI, with a current membership of over 6,800, 300 graduates and 3,000 students with significant representations within listed companies and other cross industry governance functions.

Believing that better governance leads to a better future, HKCGI's mission is to promote good governance in an increasingly complex world and to advance leadership in the effective governance and efficient administration of commerce, industry and public affairs. As recognised thought leaders in our field, the Institute educates and advocates for the highest standards in governance and promotes an expansive approach which takes account of the interests of all stakeholders.

### **General support for proposals**

We support, in general, the proposals under the Consultation Paper. We agree with the Sub-Committee on Cybercrime that Hong Kong has a duty to safeguard national security under Articles 3 and 9 of the National Security Law, including internet-related regulation. We also agree with the approach to consider different stakeholders' interests in good governance to balance the interests of netizens, IT professionals, and the public's right not to be disturbed or attacked when using and operating their computer systems.

## **The Recommendations**

Concerning the recommendations under the Consultation Paper:

### **1. Recommendation 1**

We agree that there is to be a summary offence relating to unauthorised access to programme or data and higher sentencing under a piece of new legislation where there are aggravating factors. We have no issue with this being modelled under ss. 1, 2 and 17, CMA-EW.

### **2. Recommendation 2**

From the cybersecurity perspective, there can be ethical hacking and other system vulnerability testing. Therefore, we agree that there should be specific defences to persons authorised as a general proposition. In respect of an accreditation regime, this should be continuous with professional development requirements. Our Institute will be delighted to contribute to IT governance aspects under any such accreditation regime.

### **3. Recommendation 3**

We have no issue with the 2-year limitation as this is from the discovery date. The complexity of unravelling cybercrime justifies the time for running limitation from the discovery date.

### **4. Recommendation 4**

We have no issue modelling the proposed provision under s.8 of the Model Law on Computer and Computer Related Crime.

### **5. Recommendation 5**

From the governance point of view, if there are gaps between larger companies and small and medium enterprises (**SMEs**), resources should be committed to support SMEs. This covers the issue implicit under paragraph 54 that only larger businesses can have the meticulous terms and conditions to reserve the contractual rights to intercept and utilise data of customers or employees. For example, there can be contractual templates and training provided to SMEs.

### **6. Recommendation 6**

We support the recommendation. It is appropriate that intentional interference (damaging, deletion, deterioration, alteration or suppression) of computer data without lawful authority or reasonable excuse should be an offence under the new legislation.

We agree with tracking the drafting of the Crimes Ordinance (Cap 200) for consistency of legislation.

**7. Recommendation 7**

We support the recommendation. It is appropriate that illegal interference with computer system should be an offence under the new legislation. We agree with tracking the drafting of the Crimes Ordinance (Cap 200) for consistency of legislation.

**8. Recommendation 8**

We have no issue with the defences in the context of a purposive approach to deal with the vulnerabilities of a system from the security point of view, and API's security and integrity operating within a service provider system.

**9. Recommendation 9**

We have no issue with modelling a new offence of knowingly making available or possessing a device or data (irrespective of whether it is tangible or intangible, e.g. ransomware, a virus or their source code) made or adapted to commit an offence under ss. 8 and 10 of the Computer Misuse Act (Cap 50A) of Singapore.

**10. Recommendation 10**

There may be a defence where the offending material is for authorised cyber-attacks to test system integrity. Hence, this possibility still needs to be considered under the proposed new legislation.

**11. Recommendation 11**

We support the long-arm jurisdiction relating to illegal access to program or data based on the connections with Hong Kong set out under the proposal. Should some connection of the victim in Hong Kong instead of residency be sufficient?

**12. Recommendation 12**

We support the long-arm jurisdiction relating to the illegal interception of computer data based on the connections with Hong Kong set out under the proposal. Should some connection of the victim in Hong Kong instead of residency be sufficient?

**13. Recommendation 13**

We support the long-arm jurisdiction relating to illegal interference of computer data based on the connections with Hong Kong set out under the proposal. Should some connection of the victim in Hong Kong instead of residency be sufficient?

**14. Recommendation 14**

We support the long-arm jurisdiction relating to illegal interference of computer system based on the connections with Hong Kong set out under the proposal. Should some connection of the victim in Hong Kong instead of residency be sufficient?

**15. Recommendation 15**

We support the long-arm jurisdiction relating to making available or possessing a device or data for committing a crime based on the connections with Hong Kong set out under the proposal. Should some connection of the perpetrator in Hong Kong instead of residency be sufficient?

**16. Recommendation 16**

The issue is one of proportionality in relation to imprisonment for life for a number of the offences. Please kindly consider market consensus in this regard, if any, prior to finalising the new legislation.

If there are any questions, please feel free to reach out to Ellie Pang FCG HKFCG(PE), Chief Executive, HKCGI or Mohan Datwani FCG HKFCG(PE), Deputy Chief Executive, HKCGI at 2881 6177 or [research@hkcgi.org.hk](mailto:research@hkcgi.org.hk).

Yours sincerely

For and on behalf of  
The Hong Kong Chartered Governance Institute



**Ernest Lee FCG HKFCG(PE)**  
President