**CYBERCRIME CASE STUDY**

**Facts:**

***Background:***

The State of Gondor is a developing country in Asia and a neighbour of Rohan. Gondor is a member of the WTO, the UN and the Commonwealth. Gondor has traditionally been a centre of a thriving banking and finance industry in the region and internationally. As a result of Gondor’s new undersea optical fibre cable (connections to which Gondor provides to neighbouring countries such as Rohan), Gondor has experienced growing internet bandwidth. This has led to innovations in Gondor such as internet banking and electronic payments both using computers as well as high speed 3G internet connections over mobile devices for domestic customers as well as foreign account holders. One of the largest Banks in Gondor, the Gondor National Bank (“GNB”) has tied up with GonTel, the Cellco/mobile phone service provider in Gondor to provide mobile payments using IP.

***The case:***

GNB and Gontel have recently discovered the existence of phishing emails from spoofed websites pretending to be emails from GNB or Gontel with their trademarks and logos. These emails inform recipients that their account has been reset for security reasons and in order to maintain access to their accounts they should click on links provided in the email to authenticate their accounts. The links seem to be the authentic GNB and/or Gontel website addresses (domain names) but they either direct recipients to a different website or direct recipients to a domain name which is similar (typo squatted) to that of the GNB and/or Gontel domain name or direct them to a website hidden at the second or third level of a different domain name. The websites look and feel exactly like the GNB and/or Gontel websites. On arriving at these websites recipients are asked to enter their account details and other personally identifiable information (including account numbers, customer IDs, passwords and other security information), which is then used to access their accounts illegally and withdraw funds.

Initial investigation leads IP traces to Rohan and it seems that the senders are using fast flux to facilitate phishing attacks and mask the origins of the domain names and also spoof the sender’s email addresses. It is suspected that the government of Rohan may be behind these cybercrime attacks. Rohan Law Enforcement has refused to cooperate in response to requests for mutual legal assiatance citing sovereignty and security. However, the only way to ascertain the actual origin of the emails is to seek assistance from Rohan's ISPs and the Registrars of the domain names in question.

Investigations and discussions with other foreign law enforcement and regulators suggest that such emails are sent by sophisticated criminals which could either be state actors or sophisticated organised crime. At times the proceeds of such crime are used to facilitate illegal transmissions of foreign exchange and cross border transfers thereby assisting money laundering operations and other serious crime.

Gondor does not have any cybercrime legislation which provides for specific cyber offences or procedural powers and is looking at traditional fraud and financial crime offences in its penal code to pursue the investigation.

Gondor has an independent Telecom Regulator that does not answer to the Government but Internet Governance and Policy is excluded from its scope. The Ministry for Internet Policy deals with Internet related matters. The Ministry of Justice deals with Law Enforcement. Banking regulation is exclusively dealt with the strong and independent State Bank of Gondor.

You are the Legal/Policy Advisor to the Gondor Government on Internet Governance & Cybercrime.

The Gondor Government has asked you to suggest options to address this problem. Some of the options the Government has asked you to consider include:

* Blocking of domain names and/or IP addresses
* Block all emails from and websites of Rohan
* Contacting the Rohan ISPs directly to seek assistance
* Contacting Interpol
* Denying Rohan connection to Gondor's undersea cable
* Declaring the attacks cyber terrorism, an aggression by Rohan and taking the matter to the UN
* Implement real-time surveillance and monitoring not just of traffic data but also of content data

**Questions for discussion in the context of best practice**

***Cybercrime***

* What types of offences have been committed in this case?
* Would it help if the definition of offences in Gondor, Rohan and other cooperating countries were similar and were criminalised?
* What models can Gondor look to for the introduction of cybercrime legislation?
* How can Gondor ensure that Rohan is obliged under international law to respond to its requests for cooperation?
* Should Gondor be able to directly contact and receive information and assistance from Rohan's ISPs?
* Can Gondor seek assistance from Interpol?
* What role can the UN play in regards the cybercrime linked to Money Laundering?
* What help can the ITU provide?
* What solutions can the Commonwealth provide, especially in this case?
* What solutions can the Budapest Convention provide, especially in this case?