**ÉTUDE DE CAS DE CYBERCRIMINALITÉ**

**Faits :**

***Contexte* *:***

L’État de Gondor est un pays en développement d’Asie et un voisin du Rohan. Membre de l’OMC, de l’ONU et du Commonwealth, le Gondor est traditionnellement un centre bancaire et financier prospère au niveau régional et international. Grâce au nouveau câble sous-marin de fibre optique qu’il a installé (et auquel il permet à d’autres pays voisins comme le Rohan de se connecter), le Gondor a connu une augmentation de la bande passante Internet. Le nouveau câble a encouragé dans le pays des innovations telles que les services bancaires par internet et les paiements électroniques sur ordinateur, ainsi que les connexions internet 3G à haut débit sur les appareils mobiles pour les clients nationaux et les titulaires de comptes étrangers. L’une des plus grandes banques du Gondor, la Gondor National Bank (« GNB »), s’est associée à GonTel, le fournisseur de services de téléphonie mobile du Gondor, pour proposer des paiements mobiles utilisant des cartes IP.

***Le cas :***

La GNB et Gontel ont récemment découvert l’existence de courriels d’hameçonnage provenant de sites Web piratés et se faisant passer pour des messages en provenance des entreprises notamment en arborant leur logo et leur marque commerciale. Ces courriels informent les destinataires que leur compte a été réinitialisé pour des raisons de sécurité et que, pour rester en mesure d’y accéder, ils doivent cliquer sur les liens fournis dans le courriel en cause afin de valider leur compte. Les liens semblent correspondre aux adresses authentiques des sites web de GNB et/ou Gontel (noms de domaine), alors qu’ils renvoient en fait les destinataires vers un site Web différent ou vers un nom de domaine ressemblant (typo-squatté) à celui de GNB et/ou Gontel, ou encore vers un site Web caché au deuxième ou troisième niveau d’un nom de domaine différent. Les sites Web ressemblent exactement à ceux du GNB et/ou de Gontel. En arrivant dessus, les destinataires sont invités à saisir les détails de leur compte et divers renseignements d’ordre personnel et confidentiel (y compris le numéro du compte, l’identifiant clients, le mot de passe et d’autres informations relatives à la sécurité), lesquels sont ensuite utilisés pour accéder illégalement à leur compte et retirer des fonds.

L’enquête initiale permet de relever des traces IP au Rohan et il semble que les expéditeurs recourent au Fast Flux pour faciliter les attaques par hameçonnage, masquer l’origine des noms de domaine et usurper l’adresse électronique de l’expéditeur. On soupçonne le Gouvernement du Rohan d’être derrière ces attaques cybercriminelles. Les services répressifs de cet État ont refusé de coopérer en réponse aux demandes d’entraide judiciaire en invoquant des motifs relevant de la souveraineté et la sécurité nationales. Cependant, le seul moyen de déterminer l’origine réelle des courriels est de demander l’aide des fournisseurs d’accès internet du Rohan et des bureaux d’enregistrement des noms de domaine en question.

Les enquêtes et des discussions avec d’autres services répressifs ou autorités de réglementation œuvrant à l’étranger suggèrent que ces courriels sont envoyés par des criminels avertis travaillant pour le compte soit d’organismes étatiques, soit de puissantes organisations criminelles. Le produit de ces crimes sert parfois à faciliter les transmissions illégales de devises étrangères et les transferts transfrontaliers, contribuant ainsi à des opérations de blanchiment de capitaux et à la commission d’autres infractions graves.

Le Gondor est dépourvu d’une législation relative à la cybercriminalité prévoyant des infractions ou des pouvoirs procéduraux spécifiques. Pour poursuivre ces enquêtes, il a recours aux dispositions de son Code pénal définissant les infractions traditionnelles de fraude et de criminalité financière.

Le Gondor dispose d’un organisme de réglementation des télécommunications indépendant du gouvernement, dont le mandat n’englobe ni la gouvernance ni la politique d’internet. Le ministère de la Politique internet traite des questions liées à ce réseau, tandis que le ministère de la Justice est chargé de l’application de la loi. La réglementation bancaire relève exclusivement de la Banque d’État du Gondor (SBG) laquelle constitue une entité puissante et indépendante.

Vous êtes le conseiller juridique/politique du Gouvernement du Gondor en matière de gouvernance d’internet et de cybercriminalité.

Ledit gouvernement vous a demandé de suggérer des solutions au problème décrit plus haut. Voici quelques-unes des options qu’il vous a demandé d’envisager :

* Blocage des noms de domaine et/ou des adresses IP
* Bloquer tous les courriels en provenance du Rohan, ainsi que les sites Web domiciliés dans ce pays
* Contacter directement les FAI du Rohan pour solliciter leur aide
* Contacter Interpol
* Refuser la connexion du Rohan au câble sous-marin du Gondor
* Déclarer que les attaques relèvent du cyberterrorisme et constituent une agression de la part du Rohan et porter l’affaire devant l’ONU
* Mettre en place une surveillance et un contrôle en temps réel non seulement des données de trafic, mais aussi des données de contenu

**Questions à débattre dans le contexte des meilleures pratiques**

***Cybercriminalité***

* Quels types d’infractions ont été commis dans ce cas ?
* Serait-il utile que les agissements en cause soient définis en infractions pénales dans des termes identiques au Gondor, au Rohan et dans d’autres pays coopérants ?
* De quels modèles le Gondor peut-il s’inspirer pour introduire une législation sur la cybercriminalité ?
* Comment le Gondor peut-il s’assurer que le Rohan est tenu, en vertu du droit international, de répondre à ses demandes de coopération ?
* Le Gondor devrait-il être en mesure de contacter directement les fournisseurs d’accès internet du Rohan et de recevoir des informations et une assistance de leur part ?
* Le Gondor peut-il demander l’assistance d’Interpol ?
* Quel rôle l’ONU peut-elle jouer en ce qui concerne la lutte contre la cybercriminalité liée au blanchiment d’argent ?
* Quelle aide peut apporter l’UIT ?
* Quelles solutions le Commonwealth peut-il apporter, en particulier dans ce cas précis ?
* Quelles solutions la Convention de Budapest peut-elle apporter, en particulier dans ce cas précis ?