**ESTUDO DE CASO SOBRE CIBERCRIME**

**Matéria de facto:**

***Enquadramento:***

O Estado de Gondor é um país em desenvolvimento na Ásia e vizinho de Rohan. Gondor é membro da OMC, da ONU e da Commonwealth. Gondor tem sido tradicionalmente o centro de uma indústria bancária e financeira próspera na região e a nível internacional. Em resultado do novo cabo submarino de fibra ótica (ligações que a Gondor fornece a países vizinhos como Rohan), Gondor tem uma largura de banda de Internet crescente. Esta situação conduziu a inovações em Gondor, como a banca via Internet e os pagamentos eletrónicos, utilizando tanto computadores como ligações à Internet 3G de alta velocidade através de dispositivos móveis para clientes domésticos e titulares de contas estrangeiros. Um dos maiores bancos de Gondor, o Gondor National Bank (“GNB”), ligou-se à GonTel, o fornecedor de serviços Cellco/telemóvel em Gondor para disponibilizar pagamentos móveis utilizando IP.

***O caso:***

O GNB e a GonTel descobriram recentemente a existência de e-mails de *phishing* a partir de sites *spoofed* que pretendem passar por e-mails do GNB ou da GonTel com as suas marcas e logótipos. Estes e-mails informam os destinatários de que a sua conta foi reinicializada por razões de segurança, devendo, a fim de manter o acesso às suas contas, clicar nas ligações fornecidas no e-mail para as autenticar. As ligações parecem ser endereços autênticos do site do GNB e/ou da GonTel (nomes de domínio), mas reencaminham os destinatários para um site diferente ou para um nome de domínio semelhante (*typosquatted* – sequestro de URL) ao do nome de domínio do GNB e/ou da GonTel ou para um site ocultado no segundo ou terceiro nível de um nome de domínio diferente. Os sites têm o mesmo aspeto dos do GNB e/ou da GonTel. Quando acedem a esses sites, os destinatários são convidados a introduzir os seus dados de conta e outras informações pessoais identificáveis (incluindo números de conta, ID de cliente, palavras-passe e outra informação de segurança), que são depois utilizados para aceder ilegalmente às suas contas e retirar fundos.

A investigação inicial conduz os indícios do IP a Rohan e parece que os remetentes estão a utilizar um fluxo rápido para facilitar ataques de *phishing* e ocultar as origens dos nomes de domínio, bem como os endereços de e-mail do remetente. Suspeita-se que o governo de Rohan possa estar por trás destes ataques de cibercrime. As autoridades policiais de Rohan recusaram-se a cooperar em resposta a pedidos de assistência jurídica mútua invocando soberania e segurança. No entanto, a única forma de determinar a origem efetiva dos e-mails é solicitar assistência aos fornecedores de serviços de Internet de Rohan e às empresas de registo dos nomes de domínio em causa.

As investigações e discussões com outras autoridades policiais e reguladoras estrangeiras sugerem que esses e-mails são enviados por criminosos sofisticados, que podem ser intervenientes estatais ou membros de uma organização de crime organizado. Por vezes, os produtos desse tipo de crime são utilizados para facilitar as transmissões ilegais de moeda estrangeira e realizar transferências transfronteiras, ajudando assim as operações de branqueamento de capitais e outros crimes graves.

Gondor não dispõe de legislação em matéria de cibercriminalidade que preveja infrações informáticas ou poderes processuais específicos e, para realizar a investigação, recorre ao seu código penal no tocante a infrações tradicionais em matéria de fraude e criminalidade financeira.

Gondor tem um regulador de telecomunicações independente que não responde perante o governo, mas a governação e a política da Internet estão excluídas da sua alçada. O Ministério da Política da Internet trata das questões relacionadas com a Internet. O Ministério da Justiça ocupa-se da aplicação da lei. A regulamentação bancária é tratada exclusivamente pelo, forte e independente, Banco Nacional de Gondor.

É consultor jurídico/político do governo de Gondor em matéria de governação e cibercrime na Internet.

O governo de Gondor solicitou-lhe que sugerisse opções para abordar este problema. Algumas das opções que o governo solicitou que considerasse:

* Bloquear nomes de domínio e/ou endereços IP
* Bloquear todos os e-mails e sites de Rohan
* Contactar diretamente os fornecedores de serviços de Internet de Rohan para obter assistência
* Contactar a Interpol
* Recusar a ligação de Rohan ao cabo submarino de Gondor
* Declarar os ataques de ciberterrorismo como uma agressão por Rohan e apresentar a questão à ONU
* Aplicar uma vigilância e controlo em tempo real não só dos dados de tráfego, mas também dos dados de conteúdo

**Questões a debater no contexto das melhores práticas**

***Cibercrime***

* Que tipos de infrações foram cometidas neste caso?
* Seria útil se a definição das infrações em Gondor, Rohan e outros países cooperantes fosse semelhante e criminalizada?
* A que modelos pode Gondor recorrer para a introdução de legislação em matéria de cibercriminalidade?
* Como pode Gondor garantir que Rohan é obrigado, por força do direito internacional, a responder aos seus pedidos de cooperação?
* Deve Gondor poder contactar diretamente e receber informações e assistência dos fornecedores de serviços de Internet de Rohan?
* Pode Gondor solicitar assistência à Interpol?
* Que papel pode as Nações Unidas desempenhar no que diz respeito ao cibercrime associado ao branqueamento de capitais?
* Que ajuda pode a UIT prestar?
* Que soluções pode a Commonwealth fornecer, em especial neste caso?
* Que soluções pode a Convenção de Budapeste fornecer, em especial neste caso?