

Texto I

A quantidade de crimes digitais no Brasil cresce sem precedentes, de acordo com dados de empresas especializadas em segurança na internet. Especialistas (...) separaram cinco tipos de crimes digitais, também chamados de crimes cibernéticos, com grande possibilidade de dominar a rede de computadores e celulares do Brasil neste ano. Em primeiro lugar aparece o crime mais comum praticado na internet brasileira: o roubo de dados pessoais, com destaque para criminosos focados em grandes empresas, e-commerce e governo. (...) O segundo crime será o avanço no uso de robôs com inteligência artificial. Eles fingem ser pessoas em uma rede social para roubar dados e depois invadir dispositivos das vítimas. O terceiro será o fim das senhas e o uso cada vez mais frequente de sistemas de dupla identificação, uso de digital e reconhecimento facial, principalmente em softwares de bancos, provedores de e-mail e redes sociais. O quarto é um crime crescente no país: o sextorsão, baseado em narrativas de intimidades de uma pessoa para ser usado como extorsão. Por exemplo, quando uma pessoa usa uma foto íntima para pedir dinheiro em troca da não publicação na internet. E o quinto será a sofisticação de golpes, com uso de checagem de dados pessoais das vítimas para criar uma falsa sensação de credibilidade aos sites falsos, onde cliente de bancos são vítimas em potencial. (...).

<https://www.jornalopcao.com.br/reportagens/cinco-tipos-de-crimes-digitais-devem-dominar-a-internet-brasileira-em-2019-212858/>

Texto II



Disponível em: <http://www.portaldailha.com.br/noticias/lernoticia.php?id=47237>
Acesso em 9 jun. 2023.

"Crime e terrorismo cibernéticos, em princípio, não fazem parte dos debates sobre cibersegurança no contexto da paz e segurança internacional que se desenvolvem na ONU atualmente, os quais têm mais a ver com a relação entre estados, prevenção e mitigação de conflitos interestatais.", explica o embaixador Guilherme Patriota, presidente do Group of Governmental Experts (GGE). Patriota afirma, porém, que determinados tipos de crimes e atos terroristas, de difícil atribuição de autoria e com elevado impacto, podem ser mal interpretados, provocando escaladas de tensão e conflitos entre países.

<https://www.uol.com.br/tilt/noticias/redacao/2019/12/30/longe-de-consenso-mundo-retoma-discussoes-para-evitar-guerra-cibernetica.htm>

PROPOSTA DE REDAÇÃO: A partir da leitura dos textos motivadores seguintes e com base nos conhecimentos construídos ao longo de sua formação, redija texto dissertativo-argumentativo em norma padrão da língua portuguesa sobre o tema: "Caminhos para coibir os crimes cibernéticos". Apresente proposta de intervenção, que respeite os direitos humanos. Selecione, organize e relacione, de forma coerente e coesa, argumentos e fatos para defesa de seu ponto de vista.

Texto III

Os crimes virtuais são atos ilícitos praticados por meios digitais de comunicação e acesso à informação. Eles são ataques ao computador, tanto ao hardware quanto ao software. Os mais comuns são fraudes, estelionato e vazamento de informações. Segundo o Relatório de Ameaças à Segurança na Internet de 2019, entre os 157 países analisados, o Brasil foi classificado como o quarto país com mais invasões de hackers e crimes virtuais, contabilizando 4,11% dos ataques globais.

<https://www.uol.com.br/tilt/noticias/redacao/2019/12/30/longe-de-consenso-mundo-retoma-discussoes-para-evitar-guerra-cibernetica.htm>
Acesso em 9 jun. 2023.

Texto IV

Ataque hacker é um ato de guerra?

Países buscam resposta a passos lentos

(...) ataques cibernéticos são um risco gigantesco à segurança nacional de países inteiros. O problema é que não há consenso entre países sobre qual tipo de ciberataque deve qualificado como um ato de guerra (...). Apesar de digital, uma ofensiva cibernética (...) é capaz de graves danos materiais, como desligar a energia ou a distribuição de água de uma cidade. (...)

Anarquia digital

Como o ciberespaço não respeita fronteiras nacionais, especialistas creem que é muito difícil estabelecer os limites de uma convenção internacional que poderia dizer, por exemplo, que uma grande invasão hacker vinda do exterior é, na verdade, um ato orquestrado pelo governo de um país. (...)