CIEMTECH
I CONGRESSO INTERNACIONAL DE EMPREENDEDORISMO, INOVAÇÃO E GESTÃO DA TECNOLOGIA

Determinantes Dos Crimes Cibernéticos: Evidências De Um Estudo Cross-Country

Jennifer Jeane Carvalho de Araújo, UFAM, Brasil
Ana Cláudia de Araújo Moxotó, UFAM, Brasil

RESUMO

Este estudo investiga os fatores determinantes que acentuam a vulnerabilidade de países a ataques cibernéticos. Os crimes cibernéticos consistem em ações ilícitas de indivíduos denominados de hackers ou grupos de pessoas que visam invadir sistemas de computador, redes e dispositivos digitais com o objetivo de causar danos, roubar informações privadas ou obter algum tipo de vantagem. Nesse sentido, o presente estudo tem como objetivo investigar os fatores determinantes que intensificam a vulnerabilidade de países a ataques cibernéticos, Foram analisados dados de 50 países, listados no ranking de Bruce et al. (2024), utilizando regressão linear para investigar a relação entre crimes cibernéticos e variáveis relativas a dimensão da qualidade da governança, da política e de indicadores econômicos. O programa estatístico Gretl foi utilizado para realizar a regressão linear, com base no método dos mínimos quadrados ordinários (OLS). Os resultados indicam que a qualidade da regulação exerce um papel significativo na redução da vulnerabilidade, ou seja, países com maior segurança jurídica tendem a apresentar menores taxas de cibercrimes. Além disso, o estudo encontrou uma correlação entre desenvolvimento econômico dos países e a incidência de cibercrimes. No entanto, não foram encontradas relações significativas entre corrupção, instabilidade política e a ocorrência de ataques cibernéticos. Este estudo indica que melhorias na segurança cibernética exigem não apenas medidas tecnológicas, mas um fortalecimento das estruturas regulatórias e também abordagens mais amplas que abordem as questões socioeconômicas subjacentes que também influenciam o crime cibernético.

Palavras-chave: Ataques cibernéticos; Crimes cibernéticos; Segurança cibernética; Segurança jurídica; Países.

1. INTRODUÇÃO

O mundo globalizado abriu fronteiras e encurtou distâncias, contudo, possibilitou a atuação de cibercriminosos sem limite geográfico. Os ataques cibernéticos se tornaram uma realidade cada vez mais presente em nosso mundo digitalmente conectado.

A crescente dependência de sistemas e redes online expõe empresas, governos e indivíduos a uma variedade de ameaças. Os *cyberattacks* consistem em uma atividade ilícita utilizada com frequência por *hackers* (Aslan et al.,2023). As consequências desses ataques ultrapassam o prejuízo financeiro e chegam a comprometer a segurança nacional, a confiança pública sobre seus dados e o desenvolvimento econômico dos países quando atacados (Hathaway et al., 2012).

Os crimes cibernéticos são prejudiciais pois representam uma grave ameaça, onde é imprescindível que os governos, as empresas e os indivíduos invistam em medidas de segurança cibernética para proteger suas informações e infraestruturas críticas como forma de evitar os ataques. Estes crimes não apenas causam danos financeiros significativos a indivíduos e empresas, mas também comprometem dados sensíveis, afetam a infraestrutura crítica e podem até mesmo comprometer a segurança nacional. Além disso, a natureza anônima e transnacional da internet facilita a operação de criminosos cibernéticos, tornando a aplicação da lei e a responsabilização um desafio constante (Guo, 2018).

Para Riggs et al., (2023), a previsão é que o custo global do cibercrime alcance os $23.84 trilhões até 2027, um aumento significativo em relação aos $8.44 trilhões em 2022, o que coloca a cibersegurança como uma prioridade estratégica para líderes globais. A prevenção e a resposta a esses crimes exigem uma abordagem colaborativa, envolvendo a partilha de informações entre agências, setores e fronteiras, bem como a educação contínua do público sobre práticas seguras de internet.

Este trabalho busca analisar empiricamente os fatores que viabilizam os ataques cibernéticos globalmente.

Portanto, o estudo tem como objetivo investigar os fatores determinantes que intensificam a vulnerabilidade de países a ataques cibernéticos. A presente pesquisa foi guiada pela questão central: Quais fatores tornam os países mais vulneráveis a ataques cibernéticos?

Para responder a esta pergunta, serão analisados cinquenta países que aparecem no ranking *World Cybercrime Index* (Bruce et al., 2024) e visa responder quais os fatores relacionados a dimensão política, da qualidade da governança e de indicadores econômicos dos países corroboram a propagação de *cyberattacks* nos países ranqueados pelo estudo supracitado. Assim, presente pesquisa tem como objetivo investigar os fatores que tornam os países mais vulneráveis a ataques cibernéticos. Este estudo buscou analisar a questão da segurança cibernética não apenas de uma abordagem tecnológica, mas numa dimensão de fortalecimento das estruturas regulatórias e também abordagens mais amplas que abordem as questões socioeconômicas subjacentes que também influenciam o crime cibernético. A crescente

dependência da tecnologia digital e a complexidade das infraestruturas críticas tornam os ataques cibernéticos uma ameaça global, com sérias consequências econômicas, sociais e políticas. Embora diversos estudos tenham explorado essa temática, ainda há lacunas no conhecimento sobre os fatores que influenciam a vulnerabilidade de diferentes países. Portanto, é imperativo que as organizações invistam em treinamento e desenvolvimento de capacidades técnicas para resistir a essas ameaças e garantir a resiliência cibernética.

Este trabalho divide-se em outras quatro seções além desta introdução. A próxima seção traz à luz a revisão da literatura sobre ataques cibernéticos e os países atacados, o que leva a considerar a relação entre ambos para que seja possível formular as hipóteses deste estudo. Na terceira seção descreve-se a metodologia da pesquisa com detalhes da amostra das variáveis que foram utilizadas, a quarta seção abrange o modelo e método de estimação aplicado para testar as hipóteses apresentadas. A quinta seção traz a apresentação e análise empírica dos resultados, seguido pela próxima seção referente às discussões dos resultados encontrados e por fim, a sétima e última seção apresenta as considerações finais.

1. REVISÃO BIBLIOGRÁFICA E HIPÓTESES

2.1. Ataques cibernéticos

O advento da globalização no mundo, ocasionou vítimas como empresas, pessoas físicas, países e órgãos governamentais de ataques cibernéticos. Hathaway et al., (2012), definem os ataques cibernéticos como qualquer ação tomada para prejudicar as funções de uma rede de computadores para fins políticos ou de segurança nacional. De acordo com Aslan et al., (2023), o crime cibernético é cometido por indivíduos ou grupos organizados conhecidos como *hackers*. Os *hackers* têm conhecimento profundo de sistemas operacionais, podem escrever programas de computador rapidamente e detectar vulnerabilidades de programas e sistemas em um curto período. O desenvolvimento de novas ferramentas de ataque, bem como o enorme benefício econômico, motiva os *cyberattack*ss. Miao *et al.*, (2022), apontam que o roubo e ataques contra informações controladas, juntamente com o número crescente de incidentes de vazamento de informações, tornou-se uma ameaça emergente à segurança cibernética nos últimos anos.

A pesquisa de Lee et al. (2023) evidencia a natureza dinâmica e complexa dos ataques de *ransomware*. Os criminosos cibernéticos demonstram uma variedade de motivações, que vão além do simples ganho financeiro. A busca por reconhecimento social, vingança e a exploração de vulnerabilidades específicas contribuem para a sofisticação e a adaptabilidade

das ameaças cibernéticas. Compreender essas motivações é fundamental para desenvolver estratégias de segurança proativas e eficazes. Neste sentido, o estudo de Huang et al., (2018), oferece uma visão detalhada sobre como os ataques cibernéticos se tornaram um negócio lucrativo, enfatizando a eficiência e a rentabilidade dessas operações ilícitas. Isso inclui seleção de alvo e organização de *hackers*.

A cibersegurança engloba um conjunto de medidas e práticas destinadas a garantir a confidencialidade, integridade e disponibilidade da informação no ambiente digital. Isso inclui o uso de tecnologias, políticas e procedimentos para prevenir, detectar e responder a incidentes de segurança cibernética (Von Solms, 2013). A evolução das ameaças cibernéticas, como evidenciado por Li et al. (2021), inclui uma variedade de táticas, desde ataques de negação de serviço até a proliferação de *botnets*. A presença de ameaças como cavalos de Tróia, conforme destacado por Kanaker (2022), compromete a integridade e a disponibilidade de infraestruturas críticas, especialmente em ambientes de nuvem.

Segundo Agrawal et al. (2014), a rápida disseminação de *malwares* agrava os desafios enfrentados pelas forças policiais no combate ao cibercrime. A combinação da complexidade técnica das investigações digitais, da escassez de recursos e da dinâmica em constante mudança do cenário cibernético, segundo Harkin et al. (2018), resulta em uma baixa taxa de resolução de casos e compromete a efetividade das ações de combate à criminalidade digital. Segundo Kaminska (2021), a política cibernética dos EUA é guiada pela 'gestão de riscos', o que resulta em uma postura mais tolerante frente a ataques cibernéticos. A evolução dos ataques cibernéticos, caracterizada pela automação e pela complexidade crescente, como descrito por Sharif & Mohammed (2022), exige uma resposta cada vez mais sofisticada. No entanto, a análise de Erkan-Barlow & Wells-Dietel (2023) indica que a alocação de recursos para segurança cibernética é insuficiente, e a dependência de seguros pode incentivar comportamentos de risco. A vulnerabilidade inerente dos sistemas, como destacado por Sharif & Mohammed (2022), agrava essa situação.

O âmbito das finanças, é um foco em potencial para as ameaças cibernéticas, devido ao armazenamento de informações que envolvem o sistema bancário e financeiro. Bouveret (2018), aponta que, os ataques cibernéticos também podem atingir múltiplas instituições financeiras para causar colapso no financeiro. Darem et al., (2023), reforçam que o setor bancário serve como a espinha dorsal da economia de um país, interligado com vários outros setores como o petróleo, a mineração, a saúde e a indústria. Arcuri et al., (2017), concluíram que as entidades financeiras sofrem frequentemente efeitos negativos maiores do que outras empresas. Diante dos efeitos negativos dos *cyberattack*ss, a segurança cibernética tornou-se

objeto que agrega valor às corporações. Os autores Smith et al., (2018), afirmam que o cibercrime não só resulta no roubo de bens e na perda de negócios, como também prejudica a reputação de uma empresa, o que, por sua vez, pode afetar o valor da empresa no mercado de ações.

2.2. A expansão global dos crimes cibernéticos

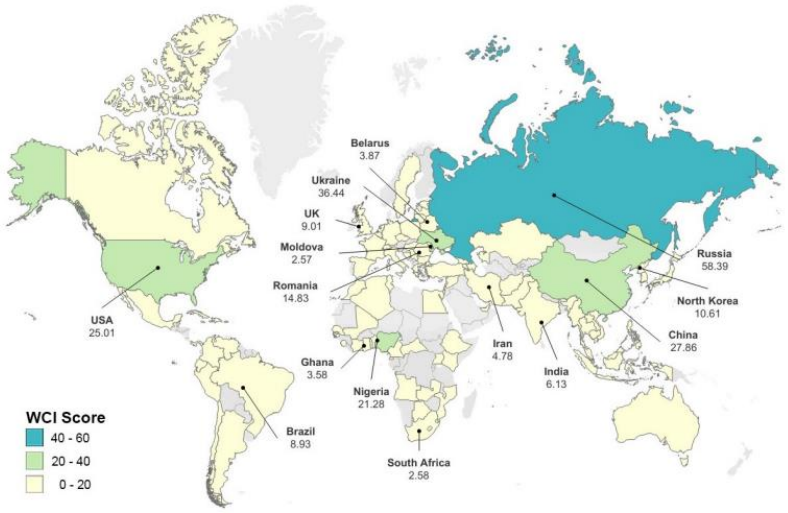

Fig 1. World map of the $WCI_{overall}$ index–top 15 countries labelled. Base map and data from OpenStreetMap and OpenStreetMap Foundation.

A figura 1: *World Cybercrime Index,* extraída de Bruce et al. (2024), apresenta em mapa, os países por índice de criminalidade cibernética. A proliferação de ataques cibernéticos no cenário digital contemporâneo impõe desafios complexos à segurança global. A atribuição precisa da origem geográfica desses ataques é dificultada pela natureza descentralizada do ciberespaço e pelo uso de infraestruturas intermediárias (Bruce et al., 2024). Nesse contexto, a cooperação entre governos e setores privados se revela crucial para mitigar os riscos e ameaças emergentes. É imprescindível a união entre o governo e organizações no combate às ameaças e riscos de ataques nas nações do mundo.

Neste sentindo, Holt et al., (2018), mostrou que países com alta infraestrutura tecnológica, amplas liberdades políticas e baixo impacto do crime organizado apresentaram maior incidência de infecções por *malware*. Srivastava et al. (2020) destacam que o capital econômico e tecnológico pode tanto impulsionar a origem de ataques cibernéticos quanto facilitar a implementação de medidas de defesa. Para os autores, o capital econômico e tecnológico de um país, são aspectos que potenciam a origem dos ataques cibernéticos, entretanto, salientam que onde há melhor preparação voltada à cibersegurança. Makridis et al.

(2019) complementam essa análise, argumentando que a prontidão cibernética envolve um conjunto mais amplo de fatores além do desenvolvimento econômico. A segurança cibernética exige uma preparação abrangente, que contempla aspectos jurídicos, técnicos, de organização, capacidade e cooperação (Bruggemann et al., 2022).

Países desenvolvidos como os Estados Unidos possuem um número elevado de casos registrados de *cyberattacks*, de acordo com o mapeamento geográfico global do crime cibernético (Bruce et al., 2024). O Brasil encontra-se em nono lugar no ranking do *World Cybercrime Index* overall–top 15 countries.

Estudos buscam investigar a relação entre os crimes cibernéticos e o grau de desenvolvimento econômico dos países. Chen et al. (2023), mostram que os fatores tecnológicos constituídos pela infraestrutura da internet e pelas condições de comunicação são necessários para a produção de crimes cibernéticos, tornando áreas mais ricas mais convenientes para a prática de crimes cibernéticos. Países mais desenvolvidos possuem mais desenvolvimento em tecnologias digitais e também possuem mais ativos digitais de alto valor agregado, no entanto, os países desenvolvidos geralmente possuem maiores recursos financeiros para investir em infraestrutura de segurança cibernética, pesquisa e desenvolvimento, e contratação de profissionais especializados. Esses países também têm acesso mais rápido às tecnologias mais recentes em segurança cibernética e podem implementá-las de forma mais eficiente.

Diante da revisão bibliográfica, considera-se a seguinte hipótese para avaliar a dimensão econômica dos crimes cibernéticos:

H1: *Em países desenvolvidos há mais crimes e ataques cibernéticos.*

Países em contextos de instabilidade política podem se mostrar particularmente vulneráveis a ataques cibernéticos. Ataques cibernéticos, quando utilizados como arma, podem causar danos devastadores à infraestrutura crítica, desestabilizar governos e economias, e, consequentemente, comprometer a soberania e a segurança nacional.

O conflito Russo-Ucraniano serve como um exemplo emblemático, onde Aviv e Ferri (2023) evidenciam a estratégia de combinar ataques físicos e cibernéticos. Na Ucrânia, a sobrecarga das defesas cibernéticas, as vulnerabilidades sistêmicas e a falta de conscientização da população, conforme apontado por Holovkin et al. (2023), criam um ambiente propício à proliferação de cibercrimes. A intangibilidade dos ataques cibernéticos exige a implementação

de medidas proativas e robustas de defesa cibernética. Portanto, a instabilidade política pode propiciar os crimes cibernéticos.

Em linha com a literatura, formula-se a seguinte hipótese para avaliar a dimensão política dos crimes cibernéticos:

H2: *Os países que enfrentam instabilidade política, são mais vulneráveis aos crimes cibernéticos.*

A pesquisa de Bruce et al. (2024) e Jackson (2024) sinaliza uma forte correlação entre altos níveis de corrupção e a prevalência de atividades cibercriminosas. De acordo com o mapeamento geográfico global do crime cibernético, a Rússia caracteriza-se como o maior centro de cibercriminalidade no mundo, seguidos da Ucrânia, da China e dos Estados Unidos, segundo Bruce et al., (2024).

Jackson (2024), destaca que a Rússia emergiu como um dos principais centros globais de cibercrime, graças a um ambiente legal permissivo e à estreita relação entre o Estado e o crime organizado. As leis russas contra o cibercrime são notoriamente fracas e a aplicação da justiça é seletiva, privilegiando os interesses do Estado. Essa dinâmica permite que cibercriminosos operem com relativa impunidade, enriquecendo-se financeiramente enquanto, ao mesmo tempo, oferecem seus serviços ao Estado para a realização de operações de ciberespionagem, golpes e sabotagens. A existência de redes criminosas que atuam tanto no mundo físico quanto no digital pode facilitar a ocorrência de diversos tipos de crimes, incluindo crimes cibernéticos. Portanto, em regiões com alta taxa de desemprego e poucas oportunidades legítimas, o crime cibernético surge como uma alternativa ilícita para obter renda, impulsionado por fatores como a prevalência de subculturas criminosas, a falta de leis eficazes e a corrupção. Em contrapartida, em países com alto índice de Gini e alto nível educacional, o crime cibernético pode ser impulsionado por um sentimento de injustiça, onde indivíduos altamente qualificados buscam compensar a disparidade salarial e alcançar um padrão de vida mais elevado (Chen et al. 2024).

Tendo em vista o exposto, estabelece-se a seguinte hipótese para avaliar a dimensão de governança dos crimes cibernéticos:

H3: *Há relação positiva entre os crimes cibernéticos e corrupção*

Zwilling et al. (2022) descobriram que os usuários da internet estão cientes das ameaças cibernéticas, mas não tomam medidas de proteção fortes. Pessoas com mais conhecimento em segurança cibernética estão mais cientes das ameaças, independentemente da localização ou gênero. O estudo também descobriu que há fatores específicos de cada país que influenciam como a conscientização, o conhecimento e o comportamento interagem.

No cenário global de crimes cibernéticos, a China se destaca como um alvo preferencial para ataques de *spam*, conforme os dados apresentados por Sufi (2023). Essa realidade sublinha a magnitude das ameaças digitais que o país enfrenta e a necessidade de fortalecer suas defesas cibernéticas. Guo (2018) destaca que a cibersegurança na China enfrenta desafios significativos, como a defasagem da legislação e a crescente sofisticação das ameaças cibernéticas. Embora a legislação chinesa reconheça a necessidade de uma resposta proporcional aos crimes cibernéticos, como apontam Khadam et al. (2023), e busque garantir a segurança de sistemas computacionais e a proteção de dados, conforme Lu (2010), a complexidade das ameaças contemporâneas exige uma adaptação constante do arcabouço legal.

Muitos países em desenvolvimento estão enfrentando dificuldades no combate ao crime cibernético devido à falta de recursos financeiros e humanos adequados, estruturas legais e regulatórias e capacidades técnicas e institucionais, fornecendo um terreno fértil para atividades de crime cibernético (Chen et al. 2023). A Nigéria, por sua vez, também enfrenta desafios consideráveis em sua busca por uma cibersegurança robusta. Conforme o mapeamento de Bruce et al. (2024), o país emerge como um novo polo de atenção no cenário global de cibercrimes, impulsionado pelo crescimento da economia digital. Ukwuoma et al. (2022) destacam que, apesar dos esforços para fortalecer a segurança cibernética, a Nigéria ainda apresenta lacunas em suas leis e políticas. Nte et al. (2022), corroboram essa análise, identificando que a legislação nigeriana, embora abrangente em alguns aspectos, não consegue acompanhar a evolução das ameaças cibernéticas. Familoni & Shoetan (2024) argumentam que o fortalecimento da infraestrutura de cibersegurança da Nigéria requer uma abordagem ampla, que inclua a reforma legislativa, o investimento em tecnologias de ponta, a cooperação internacional e a implementação de programas de educação e conscientização em larga escala.

Com base na revisão de literatura, aborda-se a hipótese:

H4: *Os países onde têm maior segurança jurídica há menos crimes cibernéticos.*

2. METODOLOGIA E ANÁLISE DE DADOS

Essa investigação busca verificar as hipóteses específicas estabelecidas na seção anterior. O estudo tem como objetivo investigar os fatores determinantes que intensificam a vulnerabilidade de países a ataques cibernéticos. Neste estudo, a variável dependente são os *cyberattacks*, que buscam investigar, através dos índices de PIB, controle da corrupção, estabilidade política e ausência de violência/terrorismo, qualidade regulatória, e o estado de direito dos países, a correlação entre estes indicadores e a quantidade de *cyberattacks* nos países. Esta pesquisa possui natureza aplicada, com objetivo explicativo, utilizando a abordagem quantitativa através do método de modelagem e simulação.

3.1. Variáveis e Estatísticas descritivas

Com base no mapeamento global de crime cibernético elaborado por Bruce et al. (2024), este estudo selecionou 50 países para analisar os fatores que influenciam a ocorrência de *cyberattacks*. A pesquisa considerou os *cyberattacks* como a variável dependente e, como variáveis explicativas, foram incluídos indicadores da dimensão econômica (PIB e PIB per capta), da dimensão política e de governança (controle da corrupção, estabilidade política, qualidade regulatória e estado de direito). As variáveis foram transformadas em log (base 10) para melhorar a normalidade para variáveis com distribuições distorcidas.

O estudo Bruce et al. (2024), resultado de uma parceria entre a Universidade de Oxford e a UNSW Canberra Cyber, forneceu os dados do Índice Mundial de Cibercrime (WCI). Este índice classifica as principais ameaças cibernéticas em cinco segmentos: produtos/serviços técnicos, ataques e extorsão, roubo de dados/identidade, golpes e saque/lavagem de dinheiro. Foi a partir desses segmentos que a variável dependente utilizada neste estudo.

Os dados das variáveis política, de governança e variáveis econômicas, referem-se ao ano de 2022. Por sua vez, os dados das variáveis de outros crimes associados presentes na pesquisa realizada por Bruce et al. (2024).

O trabalho de Bruce et al. (2024) já serviu como base para outras pesquisas. Hall e Ziemer (2024) analisaram o desvio online entre jovens armênios, situando o problema no contexto pós-soviético. Rasyid et al. (2024), investigaram os desafios legais da inteligência artificial na cibercriminalidade, enquanto Ufnal e Longuevergne (2024) se concentraram na detecção de *malwares* em arquivos tipo SVG. Por sua vez, Imam (2024) examinou o impacto do cibercrime nas relações internacionais da Nigéria.

O método *stepwise* foi utilizado para otimizar o modelo escolhido, iniciando o estudo

com todo o conjunto de variáveis explicativas. Eliminamos sequencialmente as variáveis sem significância estatística após realizar um teste para encontrar a significância conjunta dos parâmetros testados.

Assim, chegamos a um modelo inicial que inclui as seguintes variáveis explicativas mais relevantes, relatadas na Tabela 1.

Tabela 1: Tabela de variáveis.

Natureza	Variável	Descrição	Escala	Fonte
Cybercrimes (Variável dependente)	Geral **(CAT_T)**	Índice geral de crimes cibernéticos	0-100	Bruce et al., (2024)
Dimensão Política	Estabilidade política e ausência de violência/terrorismo **(S_POL)**	Mede as percepções da probabilidade de instabilidade política e/ou violência com motivação política, incluindo o terrorismo.	0-100	World Bank (2022)
Dimensão Governança	Controle de corrupção **(C_CORR)**	Captura percepções da extensão em que o poder público é exercido para ganho privado.	0-100	World Bank (2022)
	Qualidade regulatória **(R_QUA)**	Capta percepções da capacidade do governo para formular e implementar políticas e regulamentos sólidos que permitam e promovam o desenvolvimento do setor privado.	0-100	World Bank (2022)
	Estado de Direito **(R_LAW)**	Capta percepções sobre até que ponto os agentes confiam e cumprem as regras da sociedade.	0-100	World Bank (2022)
Dimensão Econômica	Produto Interno Bruto **(GDP_PCAP)**	Soma do valor bruto adicionado por todos os produtores residentes na economia, mais quaisquer impostos sobre produtos (menos subsídios) não incluídos na avaliação da produção, dividido pela população no meio do ano.	Dólar	World Bank (2022)
	Produto Interno Bruto **(GDP_MKTP)**	Taxa de crescimento percentual anual do PIB a preços de mercado com base na moeda local constante.	Dólar	World Bank (2022)

Fonte: Elaboração própria (2024)

3.1.1 Estatística Descritivas

A tabela 2 apresenta estatísticas descritivas sobre as variáveis utilizadas na análise empírica. Os dados permitem destacar alguns aspectos relevantes.

A variável dependente Cybercrimes (CAT_T) representa o índice geral de crimes cibernéticos. O índice corresponde a 50 países e apresenta um valor médio de 5,47. A mediana de 1,34 e possui um desvio padrão de 10,83, apresentando uma grande heterogeneidade. O país que possui um nível mais alto no índice é a Rússia, com 58,39, enquanto Belize apresenta a menor classificação com 0,44.

A variável explicativa Controle de corrupção (C_CORR) captura percepções da extensão em que o poder público é exercido para ganho privado. O índice apresenta um valor médio de 50,79. A mediana de 45,99 e possui um desvio padrão de 27,68, apresentando uma grande heterogeneidade. O país que possui um nível mais alto no índice é a Suíça, com 97,17, enquanto a Coreia do Norte apresenta a menor classificação, com 2,36.

A variável explicativa Estabilidade política e ausência de violência/terrorismo (S_POL) mede as percepções da probabilidade de instabilidade política e/ou violência com motivação política, incluindo o terrorismo. Apresenta um valor médio de 41,40. A mediana de 43,40 e possui um desvio padrão de 24,11, apresentando uma grande heterogeneidade. O país que possui um nível mais alto no índice é a Suíça, com 92,45, enquanto Mianmar (antiga Birmânia) apresenta a menor classificação com 2,83.

A variável explicativa Qualidade regulatória (R_QUA) capta percepções da capacidade do governo para formular e implementar políticas e regulamentos sólidos que permitam e promovam o desenvolvimento do setor privado. O índice apresenta um valor médio de 53,97. A mediana de 54,25 e possui um desvio padrão de 29,79, apresentando uma grande heterogeneidade. O país que possui um nível mais alto no índice é a Austrália, com 99,53, enquanto a Coreia do Norte apresenta a menor classificação, com 0,00.

A variável explicativa Estado de Direito (R_LAW) capta percepções sobre até que ponto os agentes confiam e cumprem as regras da sociedade. O índice corresponde a 50 países e apresenta um valor médio de 50,88. A mediana de 48,58 e possui um desvio padrão de 28,23, apresentando uma grande heterogeneidade. O país que possui um nível mais alto no índice é a Suíça, com 97,64, enquanto a Coreia do Norte apresenta a menor classificação, com 4,72.

A variável explicativa Produto Interno Bruto per capita (GDP_PCAP) representa a soma do valor bruto adicionado por todos os produtores residentes na economia, mais quaisquer impostos sobre produtos (menos subsídios) não incluídos na avaliação da produção, dividido

pela população no meio do ano. Apresenta um valor médio de 20.391,03 dólares. A mediana de 11.476,68 dólares e possui um desvio padrão de 22.683,92 dólares, apresentando uma grande heterogeneidade. O país que possui um nível mais alto no índice é a Suíça, com 93.260 dólares, enquanto Serra Leoa apresenta a menor classificação com 476 dólares.

A variável explicativa Produto Interno Bruto (GDP_MKTP) representa a taxa de crescimento percentual anual do PIB a preços de mercado com base na moeda local constante. Este indicador apresenta um valor médio de 1.661.358.452.155,45 dólares. A mediana é de 407.027.451.714,62 dólares e desvio padrão de 4.390.501.444.744,46 dólares. O país que possui um nível mais alto no índice é os Estados Unidos, com 25.744.108.000,00 dólares, enquanto a Gâmbia apresenta a menor classificação com 2.175.099.790 dólares.

Levando em consideração a variável dependente e as variáveis explicativas presentes no estudo, chegamos à descrição estatísticas descritas na tabela 2, a seguir:

Tabela 2: Descrição Estatística das variáveis

Variável	Média	Mediana	Desvio Padrão	Mínimo	Máximo
CAT_T	5,47	1,34	10,83	0,44	58,39
C_CORR	50,79	45,99	27,68	2,36	97,17
S_POL	41,40	43,40	24,11	2,83	92,45
R_QUA	53,97	54,25	29,79	0,00	99,53
R_LAW	50,88	48,58	28,23	4,72	97,64
GDP_PCAP (Dólares)	20.391,03	11.476,78	22.683,92	476	93.260
GDP_MKTP (Milhões de dólares)	1.661.358.452.155,45	407.027.451.714,62	4.390.501.444.744,46	25.744.108.000,00	2.175.099.790

Fonte: Elaboração própria (2024)

3. MODELO E MÉTODO DE ESTIMAÇÃO

Em caso das premissas de linearidade e a especificação correta dos modelos forem atendidas, a abordagem de estimação (regressão estatística) OLS (*Ordinary Least Squares)* conhecido como o método dos mínimos quadrados ordinários pode ser usado para estimar os modelos, a seguir indicado. No entanto, caso sejam detectadas violações de hipóteses, métodos alternativos de estimação como o estimador GLS (*Generalized Least Squares*), conhecido como mínimos quadrados generalizados devem ser aplicados, pois são mais eficientes na ocorrência de heterocedasticidade. Para proceder à regressão linear, utilizou-se o Gretl, plataforma

desenvolvida para análise e interpretação de diversos dados, bastante utilizado em pesquisas econômicas com o intuito de auxiliar nos estudos estatísticos. Assumiu-se uma especificação do modelo log-log para apresentar melhores resultados. Segue as especificações do modelo (1).

Modelo (1):

$$lnCAT\_T_i = \alpha_o + \alpha_1 lnC\_CORR_i + \alpha_2 lnS\_POL_i + \alpha_3 lnR\_QUA_i + \alpha_4 lnR\_LAW_i + \alpha_5 lnGDP\_PCAP_i + \alpha_6 lnGDP\_MKTP_i + u_i \ (Eq.1)$$

Onde a variável dependente do modelo (1), CAT_T (Eq. 1), é definida pelo índice geral de crimes cibernéticos. Tratando-se de um tema cada dia mais presente nos mais diversos meios, tanto corporativo como também no pessoal. As demais variáveis explicativas tais estão especificadas na Tabela 1.

4. ANÁLISE EMPÍRICA

A Tabela 3 apresenta resultados das regressões considerando crimes cibernéticos (CAT_T) como variável dependente. Em termos gerais, os resultados são bons do ponto de vista da qualidade do ajuste. O R-quadrado do modelo é razoável, correspondendo a 31%. Adicionalmente, o teste RESET não rejeita a hipótese nula de que o modelo possui uma especificação adequada. A estimativa modelo é eficiente pois os distúrbios se mostram homocedásticos, conforme indicado pelo teste de White, além disso, a hipótese nula de variância constante do erro não é rejeitada.

Os resultados das estimativas dos modelos utilizados estão descritos na Tabela 3.

Tabela 3: Resultados

Dependent variable **L_CAT_T**	**Model (1)** **(OLS)**
Const	−7,29387 (***) <0,0001
l_R_QUA	−0,487261 (**) 0,0299
l_GDP_MKTP	0,368541 (***) <0,0001
R-squared (R^2)	0,310643
F-Stat Joint significance	F(5, 15)=908,3732 p-value <0,0001
Heteroscedasticity (White test)	x^2 (10) = 5,32054 p-value 0,37
Specification (RESET test)	F(2, 13) = 0, 19 p-value 0,82
Observations (#)	49

Nota: ***, **, * indica que o coeficiente é estatisticamente significante nos níveis 1%, 5% e 10%, respectivamente; os p-valores dos coeficientes de significância estão logo abaixo das estimativas; (#) devido à falta de dados, a lista inicial de países foi reduzida.

De acordo com a Tabela 3 e interpretando os impactos marginais das variáveis explicativas, podemos prever as seguintes situações:

A variável qualidade da regulação (l_R_QUA), mede a capacidade do governo de criar leis e regulamentos claros e eficientes que ajudem as empresas a se desenvolver. Com um aumento de 1% na variável l_R_QUA, estima-se uma queda de -0,48% nos crimes cibernéticos totais, com tudo mais constante. Os dados encontrados confirmam a hipótese 4 que trata da segurança jurídica dos países.

A variável l_GDP_MKTP está associada ao PIB total dos países. Com um aumento de 1% no PIB, estima-se um aumento de 0,36% nos crimes cibernéticos totais, com tudo mais constante. Os dados encontrados confirmam a hipótese 1 que afirma que, em países desenvolvidos, há mais crimes e ataques cibernéticos.

Os dados do estudo confirmam como as dimensões econômicas e de governança estão relacionadas ao crime cibernético. Para as demais variáveis que constam no estudo empírico não foi encontrada significância estatística.

5. DISCUSSÕES

Os dados do estudo empírico indicam que, de fato, há uma relação estatística significante entre a variável os crimes cibernéticos e a qualidade regulatória (R_QUA). Portanto, nos países onde têm maior segurança jurídica há menos crimes cibernéticos. Portanto, o estudo destaca a importância dos indicadores da dimensão de governança, com a qualidade da regulação, para garantir a segurança jurídica e para combater o avanço dos crimes cibernéticos. Este estudo empírico está em concordância com Bruggemann et al., (2022), que relata que a segurança cibernética exige uma preparação abrangente, que contempla aspectos jurídicos, técnicos, de organização, capacidade e cooperação. Smith et al., (2018), afirmam que o cibercrime não só resulta no roubo de bens e na perda de negócios, como também prejudica a reputação de uma empresa, o que, por sua vez, pode afetar o valor da empresa no mercado de ações.

A pesquisa evidencia a importância crucial de regulamentações eficazes para combater crimes cibernéticos, e como exemplo destaca-se os casos emblemáticos o da Rússia, China, Nigéria e EUA, da necessidade de melhorar a regulação. De acordo com o mapeamento geográfico global do crime cibernético, a Rússia caracteriza-se como o maior centro de cibercriminalidade no mundo (Bruce et al., 2024). Jackson (2024), destaca que a Rússia emergiu como um dos principais centros globais de cibercrime, graças a um ambiente legal permissivo e à estreita relação entre o Estado e o crime organizado. As leis russas contra o cibercrime são notoriamente fracas e a aplicação da justiça é seletiva, de acordo com o

autor. Da mesma forma, Kaminska (2021) afirma que a política cibernética dos EUA resulta em uma postura mais tolerante frente a ataques cibernéticos. A evolução dos ataques cibernéticos, caracterizada pela automação e pela complexidade crescente, como descrito por Sharif & Mohammed (2022), exige uma resposta cada vez mais sofisticada.

Neste sentido, a complexidade das ameaças cibernéticas contemporâneas coloca a legislação chinesa em um constante desafio, como apontado por Guo (2018). Embora a legislação tenha evoluído para reconhecer a necessidade de uma resposta proporcional aos crimes cibernéticos (Khadam et al., 2023). Ukwuoma et al. (2022) e Nte et al. (2022), o país ainda enfrenta lacunas em sua legislação e políticas. Conforme identificado por esses autores, a legislação nigeriana, embora abrangente em alguns aspectos, não consegue acompanhar a evolução das ameaças cibernética. Bruce et al. (2024), afirmam que o Brasil se encontra em nono lugar no ranking do *World Cybercrime Index overall*–top 15 countries.

A relação entre desenvolvimento econômico e vulnerabilidade a ataques cibernéticos foi confirmada por este estudo empírico. Por um lado, países com maior PIB per capita, como observado por Srivastava et al. (2020), dispõem de recursos mais robustos para investir em medidas de segurança cibernética. No entanto, essa mesma prosperidade econômica os torna alvos mais atrativos para cibercriminosos, devido ao valor de seus ativos digitais. Conforme destacado por Holt et al. (2018), a alta infraestrutura tecnológica, embora essencial para o desenvolvimento, também amplia a superfície de ataque, tornando esses países mais vulneráveis a incidentes cibernéticos. Países desenvolvidos como os Estados Unidos possuem um número elevado de casos registrados de *cyberattacks*, de acordo com o mapeamento geográfico global do crime cibernético (Bruce et al., 2024). Por outro lado, muitos países em desenvolvimento estão enfrentando dificuldades no combate ao crime cibernético devido à falta de recursos financeiros e humanos adequados, estruturas legais e regulatórias e capacidades técnicas e institucionais, fornecendo um terreno fértil para atividades de crime cibernético (Chen et al. 2023).

O crime cibernético é um fenômeno mais abrangente que apenas a questão tecnológica, e é enraizado em causas geográficas e socioeconômicas profundas e abrangentes (Chen et al., 2023). No entanto, os resultados na pesquisa empírica não encontraram uma relação estatisticamente significativa entre corrupção e o *cybercrime*. Não há também evidência estatística que relacione estabilidade política e crimes cibernéticos. Portanto as hipóteses 2 e 3 não foram comprovadas pelo estudo.

6. CONSIDERAÇÕES FINAIS

O estudo apresentou como objetivo de pesquisa a existência da relação positiva entre os fatores determinantes que intensificam a vulnerabilidade de países a ataques cibernéticos, através desta pesquisa de natureza aplicada, com objetivo explicativo, utilizando a abordagem quantitativa através do método de modelagem e simulação.

Usou-se o *software* Gretl para as análises estatísticas. Quanto aos métodos de estimação, foi utilizado o método dos mínimos quadrados ordinários (OLS). Foram analisados dados de 50 países, listados no ranking de Bruce et al. (2024), utilizando regressão linear para investigar a relação entre crimes cibernéticos e variáveis relativas a dimensão da qualidade da governança, da política e de indicadores econômicos.

Através da análise empírica, os resultados do estudo se confirmaram parcialmente as hipóteses da pesquisa, visto que não foram encontradas relações estatisticamente significativas entre a corrupção e os crimes cibernéticos, bem como em relação à estabilidade política e os crimes cibernéticos. No entanto, este estudo encontrou uma relação entre desenvolvimento econômico, qualidade regulatória e os crimes cibernéticos.

Em relação às limitações do estudo, houve certa complexidade na coleta de dados referente à ausência de informações dos países sobre as determinantes, ampliando a complexidade da análise e pode implicar na interpretação dos resultados. Além da quantidade pequena do total de países com informações acessíveis, resultando em uma amostra incompleta.

O crime cibernético é um fenômeno mais abrangente que apenas a questão tecnológica, e é enraizado em causas geográficas e socioeconômicas profundas e abrangentes (Chen et al., 2023). Este estudo oferece uma perspectiva alternativa na busca por mitigar os problemas de segurança cibernética, em vez de uma abordagem puramente técnica. Este estudo indica que melhorias na segurança cibernética exigem não apenas medidas tecnológicas, mas um fortalecimento das estruturas regulatórias e também abordagens mais amplas que abordem as questões socioeconômicas subjacentes que também influenciam o crime cibernético.

Indubitavelmente, para alcançar resultados mais precisos sobre a relação das determinantes dos crimes cibernéticos e países, indica-se a necessidade para pesquisas futuras, através de estudos com uma amostragem maior de países, além da amplitude dos dados referentes aos países, assim como acrescentar outras variáveis para a análise de novas pesquisas. Dessa forma, mais pesquisas sobre o assunto são necessárias, dado a importância

que o estudo possui para o avanço do conhecimento científico nos âmbitos da gestão tecnológica e risco.

REFERÊNCIAS

Agrawal, M., Singh, H., Gour, N., & Kumar, M. A. (2014). Evaluation on malware analysis. *International Journal of Computer Science and Information Technologies*, *5*(3), 3381-3383.

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017, January). How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns. In *ITASEC* (pp. 175-193).

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

Aviv, I., & Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection*, *43*, 100637

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research*, 1-19.

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *Plos one*, *19*(4), e0297312.

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., ... & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, 10(1), 1-10.

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access*, *11*, 125138-125158.

Erkan-Barlow, A., & Wells-Dietel, B. P. (2023). The Current State of Cyber Insurance and Regulation in the Context of Investment Efficiency and Moral Hazard: A Literature Review. *Journal of Insurance Regulation. https://content. naic. org/sites/default/files/cipr-jir-2023-4. pdf*.

Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. *Computer Science & IT Research Journal*, *5*(4), 850-877.

Guo, M. (2018). China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces. *International Journal of Critical Infrastructure*

Protection, *22*, 139-149.

Hall, T., & Ziemer, U. (2024). Online deviance in post-Soviet space: Victimisation, perceptions and social attitudes amongst young people, an Armenian case study. *Digital Geography and Society*, *7*, 100096.

Hathaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2012). The law of cyber-attack. *Calif. L. Rev.*, *100*, 817.

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research*, *19*(6), 519-536.

Hellvig, R. C. (2023). Cybersecurity And Macroeconomic Vulnerabilities. *Internal Auditing & Risk Management*, (Supplement), 20-27.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2018). Assessing the macro-level correlates of malware infections using a routine activities framework. *International journal of offender therapy and comparative criminology*, *62*(6), 1720-1741.

Holovkin, B., Cherniavskyi, S., & Tavolzhanskyi, O. (2023). Factors of cybercrime in Ukraine. *Relações Internacionais no Mundo Atual*, *3*(41), 464-488.

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR)*, *51*(4), 1-36.

Imam, A. (2024). Nigeria's Foreign Relations and Soft Power Diplomacy Amidst Cybercrime. *Available at SSRN 4896432*.

Jackson, A. (2024). How the Collapse of the Soviet Union Made Russia a Great CyberPower. *The Cyber Defense Review*, *9*(1), 99-112.

Kaminska, M. (2021). Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. *Journal of Cybersecurity*, *7*(1), tyab008.

Kanaker, H., Karim, N. A., Awwad, S. A., Ismail, N. H., & Zraqou, J. (2022). Trojan Horse Infection Detection in Cloud Based Environment Using Machine Learning. *International Journal of Interactive Mobile Technologies*, *16*(24).

Khadam, N., Anjum, N., Alam, A., Mirza, Q. A., Assam, M., Ismail, E. A., & Abonazel, M. R. (2023). How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan. *Heliyon*, *9*(12).

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Lee, S. H., Kang, I., & Kim, H. W. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes?. *Technology in Society*, *75*, 102361.

Lu, H., Liang, B., & Taylor, M. (2010). A comparative analysis of cybercrimes and

governmental law enforcement in China and the United States. *Asian journal of criminology*, *5*, 123-135.

Makridis, C. A., & Smeets, M. (2019). Determinants of cyber readiness. *Journal of Cyber Policy*, *4*(1), 72-89.

Miao, Y., Chen, C., Pan, L., Han, Q. L., Zhang, J., & Xiang, Y. (2021). Machine learning–based cyber attacks targeting on controlled information: A survey. *ACM Computing Surveys (CSUR)*, *54*(7), 1-36.

Nte , N. D., Enoke, B. K., & Teru, V. A. (2022). A comparative analysis of cyber security laws and policies in Nigeria and South Africa. *Law Research Review Quarterly*, *8*(2), 233-258.

Rasyid, M. F. F., SJ, M. A., Mamu, K. Z., Paminto, S. R., Hidaya, W. A., & Hamadi, A. (2024). Cybercrime Threats and Responsibilities: The utilization of artificial intelligence in online crime. *Jurnal Ilmiah Mizani: Wacana Hukum, Ekonomi Dan Keagamaan*, *11*(1, April), 49-63.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, *23*(8), 4060.

Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, *15*(1), 138-156.

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, *17*(1), 42-60

Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of cybercrime originating within a nation: a cross-country study. *Journal of Global Information Technology Management*, *23*(2), 112-137.

Sufi, F. (2023). Novel Application of Open-Source Cyber Intelligence. *Electronics*, *12*(17), 3610.

Ufnal, M., & Longuevergne, T. (2024). Detection and Prevention of Malware Smuggling in Scalable Vector Graphics (SVG).

Ukwuoma, H. C., Williams, I. S., & Choji, I. D. (2022). Digital economy and cybersecurity in Nigeria: policy implications for development. *International Journal of Innovation in the Digital Economy (IJIDE)*, *13*(1), 1-11.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of*

Computer Information Systems, *62*(1), 82-97.

DETERMINANTS OF CYBERCRIME: EVIDENCE FROM A CROSS-COUNTRY STUDY

ABSTRACT

This study investigates the determining factors that increase the vulnerability of countries to cyber attacks. Cybercrime consists of illicit actions by individuals known as hackers or groups of people who aim to break into computer systems, networks and digital devices in order to cause damage, steal private information or gain some kind of advantage. Data from 50 countries, listed in the Bruce et al. ranking (2024), was analyzed using linear regression to investigate the relationship between cybercrime and variables relating to the quality of governance, politics and economic indicators. The Gretl statistical program was used to perform the linear regression, based on the ordinary least squares (OLS) method. The results indicate that the quality of regulation plays a significant role in reducing vulnerability, i.e. countries with greater legal certainty tend to have lower cybercrime rates. In addition, the study found a correlation between countries' economic development and the incidence of cybercrime. However, no significant relationships were found between corruption, political instability and the occurrence of cyber attacks. This study indicates that improvements in cyber security require not only technological measures, but a strengthening of regulatory frameworks and also broader approaches that address the underlying socio-economic issues that also influence cyber crime.

DETERMINANTES DE LA CIBERDELINCUENCIA: DATOS DE UN ESTUDIO INTERNACIONAL

RESUMEN

Este estudio investiga los factores determinantes que acentúan la vulnerabilidad de los países ante los ciberataques. La ciberdelincuencia consiste en acciones ilícitas por parte de individuos conocidos como hackers o grupos de personas que pretenden irrumpir en sistemas informáticos, redes y dispositivos digitales con el fin de causar daños, robar información privada u obtener algún tipo de ventaja. Los datos de 50 países, incluidos en la clasificación de Bruce et al. (2024), se analizaron mediante regresión lineal para investigar la relación entre la ciberdelincuencia y las variables relativas a la calidad de la gobernanza, la política y los indicadores económicos. Para realizar la regresión lineal se utilizó el programa estadístico Gretl, basado en el método de mínimos cuadrados ordinarios (MCO). Los resultados indican que la calidad de la regulación desempeña un papel significativo en la reducción de la vulnerabilidad, es decir, que los países con mayor seguridad jurídica tienden a tener menores tasas de ciberdelincuencia. Además, el estudio encontró una correlación entre el desarrollo económico de los países y la incidencia de la ciberdelincuencia. Sin embargo, no se encontraron relaciones significativas entre la corrupción, la inestabilidad política y la aparición de ciberataques. Este estudio indica que las mejoras en la ciberseguridad no solo requieren medidas tecnológicas, sino un refuerzo de los marcos normativos y también planteamientos más amplios que aborden las cuestiones socioeconómicas subyacentes que también influyen en la ciberdelincuencia.