1820

Carolina Santos

A Nova Geopolítica da Cibersegurança: Impactos, Desafios e Estratégias de Defesa

Discente da Licenciatura em Estudos Europeus, Estudos Lusófonos e Relações Internacionais na Faculdade de Direito e Ciência Política da Universidade Lusófona – Centro Universitário do Porto

Resumo

A cibersegurança tornou-se um elemento essencial na geopolítica, pois reflete a crescente interdependência digital entre as nações. Este artigo investiga a cibersegurança como uma ferramenta estratégica usada pela União Europeia e outras potências no sistema internacional, para proteger os seus interesses nacionais e moldar as suas relações internacionais. A análise foca-se em como a cibersegurança é utilizada para alcançar certos objetivos e influências políticas e económicas, em especial no contexto da crescente ameaça de ataques cibernéticos, espionagem digital e manipulação de dados. A figura de Edward Snowden, cujas revelações sobre vigilância em massa desafiaram o entendimento sobre a privacidade, é abordada como um caso fundamental. Além disto, explora-se o papel de figuras influentes como Elon Musk e Mark Zuckerberg, cujas empresas e tecnologias têm implicações diretas nas questões de segurança digital e controlo da informação. O artigo demonstra como a cibersegurança está cada vez mais interligada com o equilíbrio de poder internacional, onde as decisões em torno de normas e políticas digitais têm um impacto profundo nas dinâmicas geopolíticas globais.

A cibersegurança não é apenas uma questão técnica, mas um campo estratégico que define a posição das nações no cenário internacional.

Palavras-chave: ciberespaço; cibersegurança; geopolítica; impactos digitais

Introdução

Durante a última década temos, enquanto humanidade, testemunhado uma revolução digital que transformou radicalmente as interações sociais, económicas e políticas. O ciberespaço, que inicialmente servia como meio de comunicação e de partilha de informações, evoluiu para um campo de batalha estratégico, nos últimos anos, sendo até considerado como um novo espaço de conflito entre as nações. De acordo com Singer e Friedman (2014), "a vulnerabilidade dos sistemas digitais expõe os Estados a ameaças que ultrapassam os métodos tradicionais de guerra" (p. 28).

No seguimento do tema apresentado, segue-se a questão orientadora – De que forma é que a cibersegurança é utilizada como elemento estratégico no âmbito das relações entre os Estados no sistema internacional atual?

Este artigo visa, como seu objetivo geral, aprofundar a nova geopolítica da cibersegurança, e compreender de que forma as ameaças digitais moldam as políticas globais. A análise inclui, nos seus objetivos específicos, a descrição de ataques cibernéticos e as suas implicações reais, a análise dos impactos da cibersegurança em particulares, a nível nacional e, em última instância, a nível global, bem como uma discussão sobre a atuação cada vez mais presente de figuras influentes atuais, como Edward Snowden, Elon Musk e Mark Zuckerberg, e as suas influências na geopolítica e, ao mesmo tempo, descreve-se a atuação dos líderes mundiais nestas matérias.

Consta ainda nos objetivos específicos a delimitação da posição da União Europeia (UE) no âmbito do ciberespaço e das questões que envolvem a segurança digital da União como um todo. De forma comparativa, descreve-se o ciberespaço chinês, utilizando a Firewall chinesa como exemplo, e o que esta implica para as restantes nações. Concomitantemente,

este artigo adota a lente concetual realista das Relações Internacionais para analisar a cibersegurança como uma nova ferramenta na estratégia global.

A teoria realista destaca a procura por poder e segurança, como elementos fundamentais para os Estados e que justificam os seus comportamentos no cenário internacional. Assim, a cibersegurança é vista como um meio de proteger interesses nacionais e influenciar a comunidade internacional. Este artigo é elaborado através do método qualitativo, focado na revisão da literatura e em estudos de caso, como Edward Snowden e a influência de Elon Musk, tendo em consideração as interações dos diferentes atores mencionados.

Cibersegurança e ciberespaço – Os novos domínios estratégicos

Segundo a definição da agência norte-americana CISA (2023), a cibersegurança consiste num conjunto de práticas que pretendem proteger redes, dispositivos, contas e dados, pessoais, empresariais e até governamentais, de acesso indevido e de práticas criminosas como ataques cibernéticos. A cibersegurança só é verdadeiramente conseguida quando respeitada a tríade da agência CIA, que consiste em assegurar a confidencialidade, integridade e disponibilidade da informação aos seus comuns usuários, num mundo cada vez mais depende das redes digitais. Para Singer e Friedman (2014), o ciberespaço resume-se a uma rede globalizada de redes, que interliga eletrodomésticos, telemóveis, computadores, relógios, carros, dispositivos médicos, até às estruturas críticas que sustentam a sociedade atual, como redes de eletricidade, à Internet.

Inicialmente concebido como um espaço para troca de informações, o ciberespaço evoluiu para um ambiente em que a tecnologia é concebida, cada vez mais, como um instrumento de poder. Singer e Friedman (2014) ressaltam que "os ataques cibernéticos permitem operações globais sem a necessidade de mobilização física de tropas" (p. 35), afirmação esta que constitui uma mudança no paradigma dos espaços de conflito, remontando à ideia da obra Arte da Guerra de Sun Tzu de que a suprema arte da guerra é conseguir subjugar o inimigo sem usar um soldado, sem lutar.

De facto, a segurança dos sistemas digitais torna-se cada vez mais complexa, mas, simultaneamente, essencial. Torna-se importante reafirmar um conceito importante de uma das mais importantes agências norte-americanas. A *CIA Triad*, ou Triângulo da Confidencialidade, Integridade e Disponibilidade, é um dos pilares fundamentais da cibersegurança e fornece a base para a construção de políticas eficazes de proteção e gestão de dados. Conforme afirmam Singer e Friedman (2014), "a segurança da informação está ancorada nas três dimensões da Triad, cada uma delas representando um objetivo crucial: manter a confidencialidade dos dados, garantir sua integridade e assegurá-los contra acessos não autorizados, e, finalmente, garantir a disponibilidade dos dados quando necessário" (p. 76).

A confidencialidade refere-se à proteção de dados sensíveis contra acesso não autorizado, garantindo que apenas indivíduos ou sistemas autorizados tenham acesso. Isto é particularmente relevante para proteger informações pessoais, dados financeiros e matérias comerciais estritamente confidenciais.

A integridade, por sua vez, assegura que os dados sejam precisos e não sejam alterados de forma imprópria durante o armazenamento ou transmissão. A falta de integridade pode resultar no comprometimento de decisões empresariais e governamentais baseadas em informações erradas, não exatas. A disponibilidade, o terceiro componente da *Triad*, trata da garantia de que os sistemas e dados estejam acessíveis e utilizáveis por usuários autorizados quando necessário.

Num cenário de crescente dependência de sistemas digitais, cada um desses elementos precisa de ser cuidadosamente equilibrado para garantir a proteção e a continuidade das operações críticas. Segundo Carr (2011), "sem um foco equilibrado nas três dimensões da CIA, as organizações correm o risco de comprometer a confiança e a eficácia dos seus sistemas de segurança digital" (p. 45). Esta situação demonstra a importância da *CIA Triad* como um modelo estratégico fundamental na gestão de riscos cibernéticos, permitindo que os líderes, técnicos e especialistas colaborem para criar um ambiente digital seguro e resiliente. Esta tríade não orienta apenas a implementação de medidas técnicas, mas também serve como

base para auditorias e avaliações de risco, permitindo que as organizações em questão desenvolvam defesas eficazes contra uma vasta diversidade de ameaças cibernéticas.

Neste contexto e remontando ao ataque do vírus worm *Stuxnet*, que foi direcionado aos sistemas industriais do programa nuclear iraniano, exemplifica como um ataque digital pode causar danos físicos reais, remota e anonimamente, sem aviso prévio, se a segurança digital dos sistemas não for salvaguardada seriamente, tendo sempre por base a tríade anteriormente descrita. Este ataque é, ainda, um exemplo do quão impactante, em termos reais, um ciberataque pode ser para uma empresa, para um setor económico e, em última instância, para a economia nacional, dependendo da dimensão do ataque.

Ora, as ameaças emergentes são as mesmas para este mundo globalizado, no entanto a resposta das potências pode divergir. Para isto, vejamos o modus operandi chinês e o modelo europeu.

A Firewall chinesa, conhecida como "Grande Firewall da China", é uma das implementações mais sofisticadas de censura e controlo da Internet. Esta integra tecnologias como bloqueio de IP, filtragem de DNS, inspeção profunda de pacotes e deteção de palavras-chave para monitorizar e restringir o acesso a conteúdos considerados subversivos ou inapropriados pelo Estado chinês. King, Pan e Roberts (2013) afirmam que "a censura digital na China é projetada para evitar a disseminação de opiniões contrárias à narrativa estatal, utilizando tanto a tecnologia quanto diretrizes legais" (p. 330).

A Firewall não só impede o acesso a plataformas estrangeiras como Google e Facebook, mas também molda o comportamento dos seus usuários, promovendo uma autolimitação e reforçando o controlo do Estado sobre toda a informação consumida. Este mecanismo tem profundas implicações políticas e económicas, a níveis nacionais, mas também internacionais. Politicamente, a Firewall permite ao governo chinês manter o controlo rigoroso sobre a narrativa interna e prevenir a propagação de ideias que possam incitar descontentamento ou resistência ao regime.

Economicamente, as restrições impostas afetam essencialmente as empresas estrangeiras que desejam trabalhar na China, exigindo adaptações custosas e impactando a transparência do mercado. Conforme Singer e Friedman (2014) observam, "o controlo do fluxo de informação na Internet pode ser convertido numa forma de poder que transcende o militar" (p. 40). Desta forma, a Firewall chinesa não é apenas uma ferramenta de censura, mas um verdadeiro componente estratégico que contribui para a soberania digital da China e influencia a governança global do ciberespaço, no seu contexto geopolítico.

Já no Ocidente, e no contexto da União Europeia, a cibersegurança constitui um pilar essencial na soberania digital, pois reflete esforços para mitigar vulnerabilidades tecnológicas e a tentativa de assegurar autonomia estratégica face a outras potências, como a China e os EUA. Neste sentido, McMahon (2024) acredita que a aplicação da Inteligência Artificial (IA) na cibersegurança pode fortalecer a capacidade de identificação de ameaças pela União Europeia.

No entanto, o autor também alerta para a urgência na criação de padrões que garantam que esta aplicação da IA possa ser confiável, ética e transparente, fatores estes que constituem desafios atuais da segurança digital da UE. A Estratégia de Cibersegurança da UE, de acordo com a Diretiva NIS2, reflete a preocupação com esta situação e demonstra que pretende fomentar a resiliência digital dos Estados-membros através da harmonização de políticas com a cooperação internacional.

Além disto, as estratégias da União Europeia assentam, essencialmente, no reforço da autonomia estratégica, na promoção de parcerias globais e no estabelecimento de normas internacionais.

Em primeiro lugar, a UE assume uma abordagem de quase mercantilismo regulatório (Farrand e Carrapico, 2024), com o objetivo de reduzir a sua dependência externa, especialmente no setor digital. Esta posição reflete a preocupação com o controlo sobre as suas tecnologias críticas, alinhada com os esforços previstos na estratégia da UE, para integrar a segurança e a sustentabilidade nas políticas digitais.

Assim, a colaboração com organizações internacionais, nomeadamente focadas na defesa, como a NATO, seria vital para o desenvolvimento de uma segurança mais ampla e eficaz no ramo da segurança digital, e, simultaneamente, auxilia na pretensão europeia de liderar este campo.

Por outro lado, e no que refere às normas internacionais, a União Europeia garante esforços para criar regulamentações em matérias de cibersegurança, pois declara como necessária a uniformidade no uso de ferramentas para este fim, como é o caso do uso militar de inteligência artificial.

Assim, de modo comparativo, enquanto o modelo chinês preza pela soberania digital, pela privacidade dos usuários e garante o controlo dos fluxos de informação, chegando mesmo a bloquear sinais de IP indesejados, para assegurar a coesão política e social dos cidadãos, o modelo europeu pretende regulamentar, especialmente, o uso de Inteligência Artificial, por via da cooperação internacional. O objetivo europeu passa pela segurança dos seus sistemas digitais perante as cada vez mais frequentes e mais complexas ameaças digitais.

Influência de atores individuais, atores não estatais e de grandes empresas

Além dos Estados, as grandes empresas e líderes tecnológicos desempenham papéis cruciais na delimitação do ciberespaço. Elon Musk, por meio do projeto Starlink, expande a conectividade global ao fornecer serviços de rede e Internet, especialmente em regiões de conflito, mas também a regiões mais isoladas, como a Gronelândia. Em 2022, a SpaceX atingiu uma avaliação superior a 100 mil milhões de dólares (InvestClub, 2022), valores que evidenciam o seu impacto estratégico no cenário internacional. Paralelamente, Mark Zuckerberg e a Meta têm sido objeto de debates intensos sobre questões de privacidade e de manipulação de dados, com as ações da empresa a cair aproximadamente 15% após denúncias de práticas inadequadas nestas matérias (Bloomberg, 2021). Estes exemplos demonstram como a atuação de atores não estatais pode influenciar a geopolítica digital e impõe desafios à ordem internacional.

Paralelamente ao contexto das relações internacionais, Elon Musk e Mark Zuckerberg ilustram como o setor privado influencia a dinâmica do ciberespaço entre as nações. Musk, com o projeto Starlink, posiciona a SpaceX como um ator estratégico, com uma avaliação de mercado superior a 100 mil milhões de dólares (InvestClub, 2022). De facto, e tendo em conta o contexto atual, a posição estratégica e os serviços que a Starlink proporciona, por exemplo, à Gronelândia, torna a questão da vontade de ter posse do território da Gronelândia, do atual Presidente Donald Trump ainda mais complexa para as relações internacionais. Os serviços Starlink podem, de facto, ser usados para influenciar as decisões dos líderes de ambas as nações, exemplo claro de como o ciberespaço pode ser não só influente nas políticas dos Estados, mas também como pode ser um novo espaço de conflitos. Em contrapartida, as controvérsias mais recentes que relacionam Zuckerberg e a Meta, com uma queda de 15% no valor das ações após denúncias de falhas na proteção de dados (Bloomberg, 2021), demonstram como práticas de gestão de dados afetam diretamente a estabilidade do mercado financeiro global.

Paralelamente e voltando a referir o multimilionário Elon Musk, é cada vez mais evidente, nos últimos anos, que, alegadamente, utiliza a sua rede social X (antigo Twitter) como uma verdadeira máquina de propaganda política. Além de todas as publicações que fez durante o período eleitoral dos EUA, Elon Musk também tem sido acusado de interferir com os processos democráticos europeus, nomeadamente o alemão, apoiando publicamente o partido de extrema-direita alemão, AfD, com várias publicações, servindo como exemplo uma publicação no dia das eleições, 23 de fevereiro de 2025, com 3 bandeiras da Alemanha, seguido de "AfD" e outras 3 bandeiras alemãs. De facto, após a aquisição da plataforma, de acordo com reportagens publicadas pela Bloomberg (2025), há indícios de que houve alterações nos algoritmos, que possam ter favorecido determinadas narrativas políticas, influenciando o debate público e, possivelmente, o comportamento dos eleitores. Embora estas acusações estejam sob investigação e ainda não tenham sido confirmadas de forma definitiva, diversos especialistas alertam que a interferência de plataformas digitais em processos eleitorais representa um risco à integridade dos processos

democráticos e reforça a necessidade de maior transparência e regulação no ambiente online (Bloomberg, 2024).

Não obstante, não são só apenas grandes empresas e pessoas influentes que têm poder de voto e de ação nestas matérias, com repercussões globais. Se voltarmos atrás no tempo e recorrermos ao ano de 2013, Edward Snowden é o nome mais emblemático desse ano no domínio digital. As revelações deste caso expuseram a verdadeira extensão dos programas de vigilância dos EUA, que causaram uma profunda reavaliação das políticas de segurança norte-americanas. "As revelações de Snowden abalaram a confiança dos cidadãos e impulsionaram reformas que obrigaram a investimentos milionários para restabelecer a privacidade digital" (Singer & Friedman, 2014, p. 44). Os custos indiretos dessas mudanças, embora difíceis de quantificar, têm impacto duradouro na política interna e nas relações internacionais.

Edward Snowden é um ex-agente da NSA (Agência Nacional de Segurança dos EUA), tendo entrado nesta em 2006 e, desde aí, aprofundou a sua área de atuação no uso de tecnologias de supervisão em larga escala, um campo de preocupação constante muito devido à evolução das telecomunicações. Em 2013, Snowden começou a desconfiar dos programas de vigilância da NSA, pois estes acediam e usavam dados de milhões de pessoas, sem o seu conhecimento, muito menos consentimento, o que constituía uma violação jurídica (Snowden, 2019). Assim, e por acreditar na violação dos direitos civis por parte da NSA, começou por reunir documentos da agência e entregou-os a jornalistas do *The Guardian*, que começaram a publicar notícias de exposição dos documentos da agência e que revelavam o alcance da vigilância digital pelos EUA e pelos seus aliados, nomeadamente interceções às comunicações entre líderes mundiais (Greenwald, MacAskill, & Poitras, 2013). Logicamente, após estas publicações, Snowden tornou-se um alvo dos EUA, que o acusaram de espionagem e acesso indevido a propriedade governamental confidencial. De acordo com Snowden, a tecnologia, enquanto ferramenta de segurança, é facilmente desviada para outros fins dos governos, como a supervisão massiva dos cidadãos, o que constitui uma verdadeira violação das liberdades civis, e ainda argumenta a necessidade da privacidade digital para a democracia (Snowden, 2019).

O caso de Edward Snowden teve um impacto substancial e duradouro nas políticas e estratégias de cibersegurança, nomeadamente na União Europeia, quanto à necessidade de evoluções de segurança digital e de regulamentos claros e transparentes acerca do uso de tecnologias de vigilância.

Implicações de ciberataques e respostas dos líderes mundiais

Os ciberataques significam custos financeiros que vão além dos gastos imediatos de recuperação desse ataque. Singer e Friedman (2014) afirmam que "os impactos económicos de um ataque cibernético estendem-se à perda de receita, danos à reputação e interrupção das operações comerciais" (p. 56). Exemplos como o ataque à Target em 2013, com custos diretos superiores a 200 milhões de dólares, bem como o leak de dados da Equifax em 2017, com prejuízos estimados em 1,4 mil milhões de dólares (U.S. House of Representatives Committee on Oversight and Government Reform, 2018), evidenciam a gravidade destes incidentes em termos microeconómicos.

Os danos à reputação são custos incalculáveis, mas com impactos duradouros. O ataque à Sony Pictures em 2014, por exemplo, resultou em prejuízos superiores a 50 milhões de dólares, devido à perda de confiança dos investidores e parceiros comerciais (Singer & Friedman, 2014, p. 60). A restauração da imagem institucional obriga a investimentos avultosos e prolongados em comunicação e transparência, o que claramente afeta a competitividade das empresas. Ataques cibernéticos direcionados a infraestruturas críticas, como o incidente WannaCry que afetou o NHS no Reino Unido, demonstram que os prejuízos vão muito além dos financeiros. O custo de recuperação do NHS foi estimado em cerca de 92 milhões de libras (aproximadamente 120 milhões dólares) (National Health Executive, 2018), evidenciando o risco para a segurança e a qualidade dos serviços públicos.

Eventos como o leak da Equifax provocam volatilidade nos mercados financeiros. Após o incidente, o valor de mercado da empresa sofreu uma queda abrupta, com perdas superiores a 4 mil milhões de dólares (U.S. House of Representatives Committee on Oversight and Government

Reform, 2018), que declara a sensibilidade dos investidores e a importância da cibersegurança para a estabilidade económica.

A eficácia da defesa cibernética depende do quão contínuo é o investimento em tecnologias como firewalls, criptografia e sistemas de deteção de acessos indevidos. Carr (2011) afirma que "a atualização constante desses sistemas é crucial para enfrentar as ameaças emergentes" (p. 85). Concomitantemente, a natureza transnacional dos ciberataques torna indispensável a cooperação internacional. Singer e Friedman (2014) observam que "acordos bilaterais e multilaterais, como o entendimento entre os EUA e a China para limitar a ciberespionagem, são essenciais para a criação de um ambiente digital seguro" (p. 71). De facto, estes acordos facilitam a partilha de informações e a quase hegemonização de protocolos, contribuindo para uma resposta coordenada a incidentes.

Nesta via, a cooperação internacional torna-se cada vez mais urgente pois, como referido anteriormente, o espaço cibernético pode ser utilizado como um verdadeiro espaço de conflito, em que outras nações interferem nas matérias internas dos países. Assim, torna-se pertinente abordar a influência russa em processos eleitorais, pois tem constituído uma preocupação crescente, com evidências de tentativas de interferência em diversas democracias ao redor do mundo. Um exemplo notório ocorreu nas eleições presidenciais de 2018 no Brasil, onde se observou o uso de campanhas de desinformação através das redes sociais e de plataformas digitais para manipular a opinião pública (Gazeta do Povo, 2022).

A respeito deste caso, o estudo de Singer e Friedman (2014) aponta que "a manipulação de informações nas plataformas digitais é uma das formas mais eficazes de se exercer poder estratégico sem recorrer ao uso da força militar" (p. 69). Especialistas em cibersegurança também identificaram atividades de bots e notícias falsas associadas a atores russos, que tinham por objetivo amplificar e estimular a polarização política. Estes incidentes ilustram a crescente interseção entre cibersegurança, geopolítica e processos democráticos, exigindo uma abordagem mais coordenada e sensível à ameaça digital no campo político.

Assim, considera- se a integração dos setores público e privado fundamental para criar uma rede de defesa robusta. Carr (2011) destaca que "a sinergia entre governos e empresas privadas possibilita a implementação de soluções inovadoras e eficazes para combater ameaças cibernéticas" (p. 92). Esta colaboração promove a troca de informações estratégicas e otimiza os investimentos em tecnologias de segurança.

No contexto dos maiores ataques cibernéticos, o ataque do *worm* Stuxnet marcou uma mudança do que se pensava ser o paradigma da cibersegurança. Singer e Friedman (2014) descrevem o incidente como "um ponto de inflexão que demonstrou o potencial dos ciberataques de causar danos físicos e estratégicos" (p. 38).

Com tantas implicações e a tantos níveis que um ciberataque produz em empresas que, rapidamente, pode alastrar-se para impactos nacionais, espera-se uma resposta adequada dos líderes mundiais a estes desafios que podem colocar em causa, como já vimos, a sua própria democracia. No entanto, observamos que não é esta a realidade atual.

No contexto internacional, a falta de conhecimento dos líderes mundiais em relação às questões cibernéticas é um padrão bastante recorrente, quase como a norma geral. Contudo, esta falha revela-se como uma falha crítica na formulação de políticas de segurança digital, que tem gerado uma dependência excessiva de técnicos e especialistas na definição de estratégias nestas matérias.

A pouca compreensão e conhecimento por parte dos governantes sobre os desafios e as complexidades do ciberespaço frequentemente resulta numa visão bastante simplificada dos riscos associados ao espaço digital. Conforme Singer e Friedman (2014) afirmam, "a crescente digitalização e as ameaças cibernéticas tornaram-se tão complexas que muitos líderes estão a deixar vitalmente essa responsabilidade em mãos de técnicos ou especialistas, com pouca compreensão dos riscos e das oportunidades envolvidas" (p. 45). De facto, esta delegação de responsabilidade a especialistas técnicos pode ser perigosa, uma vez que os líderes políticos, ao não possuírem o nível necessário de conhecimento sobre como os sistemas digitais funcionam,

podem tomar decisões que não abordam a totalidade das ameaças ou que falham em antecipar os efeitos adversos de uma ciberameaça global.

Além disto, especialistas como Carr (2011) destacam que a abordagem passiva adotada por muitos governos em relação ao conhecimento sobre cibersegurança tem consequências significativas a vários níveis: "Sem uma liderança informada, os países geralmente falham na implementação de políticas eficazes, frequentemente reagindo no momento em vez de adotar medidas proativas" (p. 102). Isto ocorre porque as decisões políticas, em muitas situações, são fundamentadas em conselhos técnicos que podem não entender ou considerar a dimensão geopolítica ou económica de um ataque cibernético coordenado contra uma nação.

A complexidade das ameaças emergentes, muitas das quais superam sistemas existentes de defesa, exige que os líderes não dependam exclusivamente de técnicos, mas também desenvolvam uma compreensão profunda da infraestrutura cibernética e das implicações das ciberameaças para a estabilidade nacional e global. É neste contexto que a necessária convergência entre os conhecimentos técnicos e políticos surge como uma prioridade.

De acordo com King, G., Pan, J., & Roberts, M. E. (2013), "os líderes políticos que possuem pouca compreensão dos desafios cibernéticos correm o risco de subestimar ou até ignorar as verdadeiras implicações dos incidentes de cibersegurança, com consequências potencialmente devastadoras não apenas para suas economias, mas para a segurança nacional como um todo" (p. 339). Portanto, a falta de educação e envolvimento direto dos líderes nas matérias relacionadas à cibersegurança cria uma fragilidade estrutural que pode ser explorada adversariamente numa nova etapa, onde os ataques cibernéticos estão cada vez mais sofisticados. Noutras palavras, quando os líderes políticos não possuem a literacia cibernética necessária, as estratégias adotadas tendem a ser fragmentadas e reativas, insuficientes, deixando de incorporar a dimensão estratégica que os riscos digitais exigem atualmente.

Esta falta de conhecimento não só impede a criação de políticas integradas que considerem os impactos socioeconómicos e geopolíticos dos ataques cibernéticos, como também limita a capacidade dos Estados de

antecipar e mitigar ameaças emergentes, evidenciando a urgente necessidade de programas de capacitação e de uma colaboração mais estreita entre decisores e técnicos especializados.

De facto, em última análise, a falta de conhecimentos cibernéticos atuais pode ser comparada à altura da Guerra Fria. Durante esta altura, a nova tecnologia, sendo estas as armas nucleares, os líderes mundiais não entendiam como funcionavam nem que efeitos poderiam ter, pois deixaram isto para os especialistas, levando a que os líderes tivessem uma visão reduzida da realidade a ser negociada. Assim, houve uma corrida a este tipo de armamento, ignorante, que causou medo e confusão até eventualmente culminar numa verdadeira guerra de nervos com situações delicadas, como a Crise dos Mísseis de Cuba, e na posterior alteração da Ordem Mundial.

Comparando esta situação ao contexto atual, um Oficial americano, agora, responsável por negociações com a China em matéria de cibersegurança não saber o que é, nem como funciona, um ISP (Internet Service Provider), era o mesmo que, na Guerra Fria, um Oficial americano não saber o que era o Míssil Balístico Intercontinental durante as negociações com a URSS. Exemplo claro do que a falta de lucidez sobre uma temática que coloca em causa tantos domínios, desde a microeconomia setorial, à economia nacional, à própria defesa e soberania nacionais, digitais e democráticas, até ao seu posicionamento na hierarquia da sociedade internacional dos tempos de hoje.

Conclusão

A Era Digital transformou o ciberespaço num novo espaço de conflitos, onde o controlo da informação tornou-se uma real arma estratégica. Ataques como o ataque Stuxnet, as revelações de Edward Snowden, os desafios enfrentados por grandes empresas tecnológicas e a implementação da Firewall chinesa, evidenciam que os impactos dos ciberataques são amplos, abrangem diversas dimensões, como as dimensões financeiras, sociais e políticas.

Remontando à questão de partida - De que forma é que a cibersegurança é utilizada como elemento estratégico no âmbito das relações entre os Estados no sistema internacional atual? – considera-se que a cibersegurança consolida-se como um elemento estratégico, ao transformar o ciberespaço como um novo campo de disputa de poder entre as nações, podendo levar a conflitos cibernéticos, uma nova dinâmica nas relações internacionais.

Não obstante, a crescente frequência e especialização dos ciberataques, por vezes promovidos por Estados ou a partir de atores não estatais que estejam envolvidos em agendas políticas, demonstram que a segurança digital ultrapassa o domínio técnico e pode ter consequências nefastas para as economias e até para a soberania dos Estados, visto que a cibersegurança passa a ser considerada como um novo domínio de defesa nacional. O exemplo de Edward Snowden exemplifica como é que um Estado pode utilizar o ciberespaço para vigiar e manipular, não só as suas populações, bem como de outras nações, através da ciberespionagem. Neste contexto, a cibersegurança, que envolve defesa nacional, as economias e as soberanias das nações, torna-se um fator estratégico e basilar na projeção de poder dos Estados e, consequentemente, na definição mais assente da hierarquia do sistema internacional.

Quanto a limitações dos estudos, a natureza dinâmica do ciberespaço implica que as estratégias de defesa podem tornar-se obsoletas rapidamente. Assim sendo, entre os principais desafios estão a rápida evolução das técnicas de ataques cibernéticos e a necessidade de integrar as tecnologias emergentes, como a Inteligência Artificial, para a deteção precoce de ameaças. A cooperação internacional, embora essencial, enfrenta dificuldades políticas e culturais que tornam mais complexa a implementação de uma estratégia global eficaz.

Recomenda-se ainda que futuras pesquisas analisem possíveis implementações de sistemas de defesa proativos, que possam utilizar algoritmos de inteligência artificial e em estudos longitudinais integrados que acompanhem os impactos económicos e sociais dos ciberataques ao longo do tempo.

Referências Bibliográficas

Associação Portuguesa para o Desenvolvimento das Comunicações. (2021, novembro 19). *Programa Europa Digital tem 102 milhões para cibersegurança e digital*. https://www.apdc.pt/noticias/atualidade-internacional/programa-europa-digital-tem-102-milhoes-para-ciberseguranca-e-digital

Bloomberg. (2021). Meta Nears Bear Market After $224 Billion Value Wipeout. *Bloomberg News*. https://www.bloomberg.com/news/articles/2021-12-03/meta-set-to-enter-bear-market-after-230-billion-value-wipeout

Bloomberg. (2024). *Musk Berated by German Leaders Over Backing for Far-Right Party*. Bloomberg News. https://www.bloomberg.com/news/articles/2024-12-30/musk-berated-by-german-leaders-over-backing-for-far-right-party

Bloomberg. (2025). *Musk's Election Interference Is Rattling German Political Class*. Bloomberg News. https://www.bloomberg.com/news/articles/2025-01-29/musk-s-election-interference-is-rattling-german-political-class

Carr, J. (2011). *Inside cyber warfare: Mapping the cyber underworld* (2ª ed.). O'Reilly Media.

Cybersecurity and Infrastructure Security Agency. (2023, fevereiro 14). *What is cybersecurity?* https://www.cisa.gov/news-events/news/what-cybersecurity

Farrand, B., & Carrapito, H. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs, 100*(6), 2379-2383.

Gazeta do Povo. (2022, setembro 27). *Hackers russos tentam interferir nas eleições brasileiras*. https://www.gazetadopovo.com.br/mundo/hackers-russos-tentam-interferir-nas-eleicoes-brasileiras-4iml3wa244ku7n011menqwsil/

Greenwald, G., MacAskill, E., & Poitras, L. (2013, junho 6). *NSA Prism program taps in to user data of Apple, Google and others*. The Guardian. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

InvestClub. (2022, agosto 12). *SpaceX raises $250 million at $125 billion valuation*. https://investclub.sv/pt/2022/08/12/spacex-raises-250-million-at-125-billion-valuation/

King, G., Pan, J., & Roberts, M. E. (2013). *How censorship in China allows government to control the news*. *American Political Science Review, 107*(2), 326-343.

McMahon, G. (2024). *Analytic tradecraft standards in an age of AI*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/research-analysis/analytic-tradecraft-standards-age-ai

National Health Executive. (2018, janeiro 15). *WannaCry cyber attack cost NHS £92m after 19,000 appointments were cancelled*. https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Snowden, E. (2019). *Permanent record*. Macmillan.

União Europeia. (2022). *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à segurança das redes e sistemas de informação em toda a União e que altera a Diretiva (UE) 2016/1148*. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555

U.S. House of Representatives Committee on Oversight and Government Reform. (2018). *The Equifax Data Breach*. https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf