RELAÇÕES INTERNACIONAIS
20 anos
R:I
82
€12,50
JUN:2024:TRIMESTRAL

Geopolítica contemporânea e os desafios para a segurança e a defesa cibernéticas

Danielle Jacon Ayres Pinto
Marcos Aurélio Guedes de Oliveira
Natália Diniz Schwether
[Coordenadores]

€ 12,50

RELAÇÕES INTERNACIONAIS 20 anos R:I

82 JUNHO : 2024 TRIMESTRAL

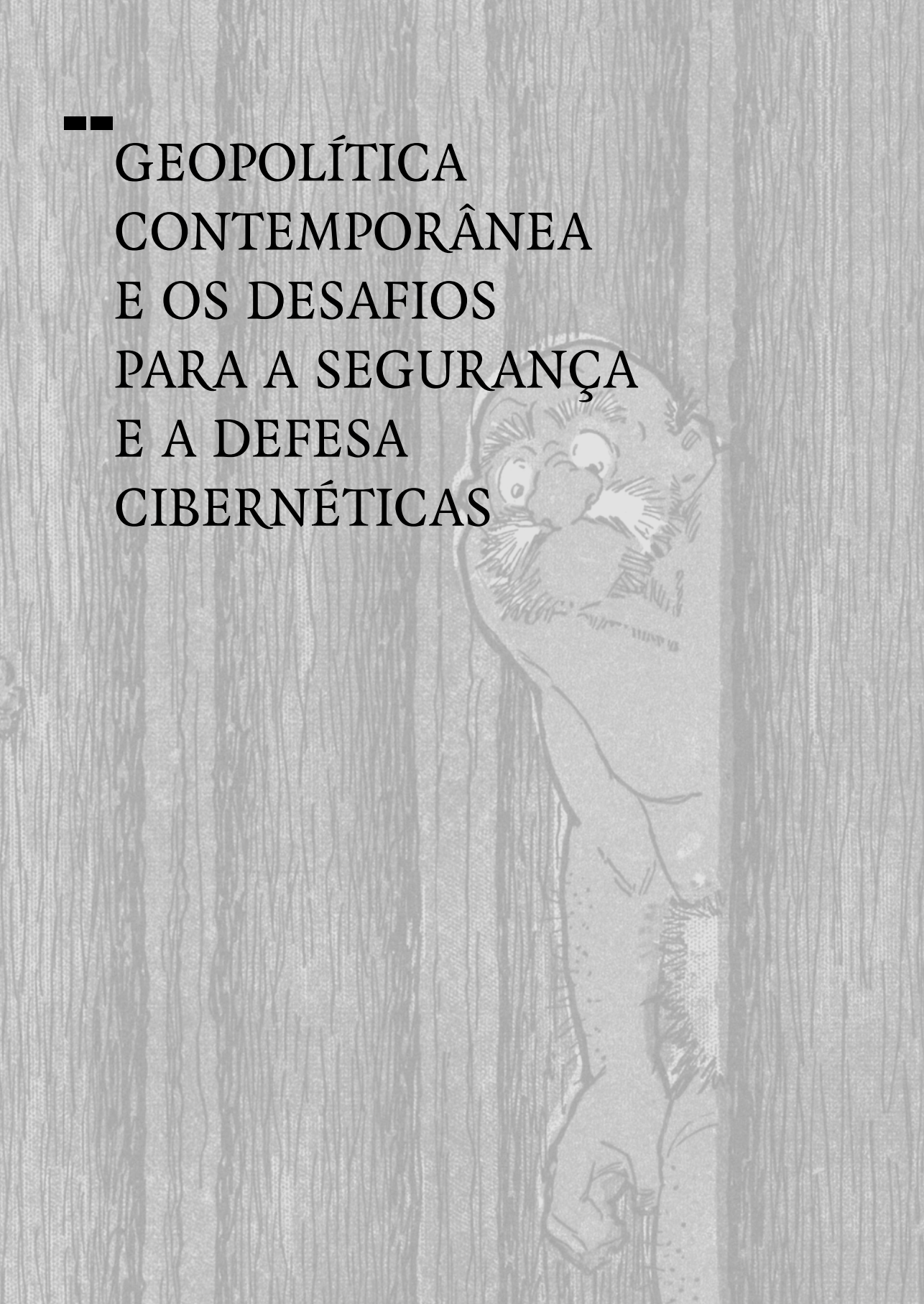
PROPRIETÁRIO, EDITOR E REDAÇÃO
IPRI-NOVA
Rua de D. Estefânia, 195, 5.º Dt.º
1000-155 Lisboa
Tel.: +351 21 314 1176
Fax: +351 21 314 1228
E-mail: ipri@ipri.pt
Website: www.ipri.pt
NIF: 506346064
DESIGN
José Brandão [Atelier B2]
REVISÃO António Alves Martins
IMPRESSÃO
Edições Húmus Lda
Apartado 7081, 4764-908 Ribeirão
Vila Nova de Famalicão
TIRAGEM 400 exemplares
INSCRIÇÃO NA ERC 124442
ISSN 1645-9199
DOI https://doi.org/10.23906/ri2024.82
DEPÓSITO LEGAL 207 795/04
Os sumários da R:I são indexados pela CSA PAIS, IBSS, IPSA, LATINDEX, SciELO Citation Index da Thomson Reuters, EBSCO e EHRI PLUS.
O estatuto editorial encontra-se disponível *online* na página http://www.ipri.pt/images/publicacoes/revista_ri/assinaturas_ri/EstatutoEditorial_RI2016.pdf

Índice

CAPA
Design de José Brandão
baseado numa ilustração
de A. Braun.

Financiado por fundos nacionais através da FCT - Fundação para a Ciência e a Tecnologia, I.P., no âmbito do projeto UIDB/04627/2020.
DOI 10.54499/UIDB/04627/2020

GEOPOLÍTICA CONTEMPORÂNEA E OS DESAFIOS PARA A SEGURANÇA E A DEFESA CIBERNÉTICAS



Nota introdutória
Geopolítica contemporânea e os desafios para a segurança e a defesa cibernéticas

Danielle Jacon Ayres Pinto | *Marcos Aurélio Guedes de Oliveira* | *Natália Diniz Schwether*

A geopolítica contemporânea é marcada por rápidas mudanças, e as principais delas que podemos destacar são os avanços tecnológicos e a crescente interconexão global. Nesse cenário, um dos desafios mais significativos é garantir um espaço cibernético seguro e estável para a sociedade e para o Estado. As ameaças cibernéticas não apenas afetam indivíduos e organizações, mas também têm implicações profundas para a segurança nacional e a estabilidade internacional. Assim, esse dossiê aqui desenvolvido tem por intuito explorar as interseções entre geopolítica, segurança cibernética e defesa cibernética, analisando os principais atores, tipos de ameaças, desafios e estratégias de mitigação.

O rápido desenvolvimento tecnológico em um mundo hiperconectado traz consequências pouco previsíveis e de grande impacto. De maneira que cada vez mais casos envolvendo o uso do poder cibernético em conflitos interestatais são registrados, seja para realizar campanhas de reconhecimento e informação, seja para otimizar ou comprometer sistemas operacionais militares e/ou civis de infraestruturas físicas e impactar de modo significativo a moral doméstica dos alvos atingidos – foi possível ver tal situação ocorrer de forma efetiva na guerra que a Rússia trava contra a Ucrânia. Outro impacto que a revolução nas tecnologias de informação e comunicação produziu traduziu-se nos graves problemas globais que têm desafiado a ordem legal e social dos Estados, ao ponto de redefinir os laços da comunicação humana e pôr em xeque a ordem democrática – as manipulações digitais no pleito do Brexit, nas eleições americanas de 2016 e nas eleições brasileiras de 2018 são um claro exemplo desse cenário ameaçador em crescimento.

Dessa forma, a relação tecnológica, cultural e de poder tem levado à construção de um novo sistema internacional que acelera a ascensão de potências emergentes e redefine as relações Norte-Sul. Todas as áreas da ciência, inclusive as humanidades, estão incorporando essa questão em suas preocupações. Mas é no estudo da política internacional que se sobressai o tema de maneira mais contundente. Os ganhadores nesse processo

 https://doi.org/10.23906/ri2024.82a01

serão aquelas nações que melhor entendam os sinais dessas transformações e procurem incorporar esse aprendizado ao seu processo decisório.

Todavia, como podemos identificar as principais potências na área digital e quais seriam seus maiores recursos?

Antes de desenvolvermos essa questão, vale entender que o espaço cibernético se tornou o quinto domínio da guerra e os Estados-Nação utilizam ataques cibernéticos como ferramentas de coerção, poder e influência. A espionagem cibernética, a sabotagem e as campanhas de desinformação são algumas das estratégias empregadas por países para alcançar objetivos geopolíticos, e tudo isso ocorre frente a uma incipiente governança global nessa seara que resiste a se desenvolver por força e vontade dos Estados no sistema internacional. Quanto menos regras, menos governança e maiores recursos, mais a esfera cibernética passa a ser o espaço onde tudo se pode fazer e pouco se pode limitar ou punir. Vejamos: quem foi culpabilizado pelos ataques com o Stuxnet? Quais reais punições sofreu a Cambridge Analytica por manipular dados no pleito do Brexit? Qual punição receberam os *hackers* «patriotas» russos por usar de forma desvirtuada os algoritmos das mídias sociais, em especial do Facebook, na eleição dos Estados Unidos em 2016? Nenhuma punição relevante que evitasse que esse cenário não só se repetisse, como, principalmente, passasse a fazer parte das estratégias de ação de diversos atores no sistema internacional para conseguirem satisfazer suas demandas de poder e influência. A reação muitas vezes foi punir indivíduos, fazer algum tipo de legislação interna e aumentar o investimento no desenvolvimento de tecnologia com fins securitários. Nenhuma outra ação ao nível global avançou no sentido de evitar ataques, pelo contrário, o que se viu foi o aumento do uso indiscriminado e descontrolado de meios digitais para ataques de todos os tipos e uma clara deterioração da segurança cibernética e da defesa cibernética no mundo.

Mas vejamos quem são os principais atores estatais que dominam as tecnologias cibernéticas no mundo.

Os Estados Unidos, que emergem como um dos principais atores na arena da segurança cibernética, investindo significativamente em infraestrutura cibernética e em capacidades ofensivas e defensivas. Agências como a National Security Agency e o Cyber Command desempenham papéis críticos na proteção de ativos nacionais e na condução de operações cibernéticas no exterior. A doutrina cibernética dos Estados Unidos enfatiza tanto a defesa quanto a dissuasão ativa.

A Rússia também é amplamente reconhecida por suas capacidades avançadas em ciberespionagem e ciberataques. Incidentes como o hackeamento do Comitê Nacional Democrata dos Estados Unidos em 2016 e os ataques à infraestrutura ucraniana demonstram a eficácia e a ambição das operações cibernéticas russas. A Rússia utiliza ciberoperações como extensão de suas estratégias de guerra híbrida, visando desestabilizar adversários e influenciar processos políticos.

A China é outro jogador chave, com extensas atividades de ciberespionagem econômica e militar. O país tem sido acusado de roubar propriedade intelectual e segredos industriais de empresas ocidentais, além de realizar operações de influência política. As capacidades cibernéticas da China são vistas como parte integrante de sua estratégia de modernização militar e de sua ambição de se tornar uma superpotência tecnológica. O Estado de Israel é amplamente reconhecido por suas capacidades cibernéticas avançadas e por ser um dos líderes mundiais em segurança cibernética. O país tem investido significativamente em tecnologia cibernética, tanto para fins defensivos quanto ofensivos. Unidades militares especializadas, como a Unidade 8200, são conhecidas por suas operações sofisticadas de ciberespionagem e guerra cibernética. Esse país também é um centro de inovação cibernética, com um ecossistema robusto de *startups* e empresas de tecnologia que desenvolvem soluções avançadas de segurança cibernética. A colaboração entre o setor militar, governo e indústria privada tem sido um fator chave no fortalecimento das capacidades cibernéticas de Israel.

Todavia, existem também outros países com menor capacidade, mas que já entenderam que os recursos cibernéticos são fulcrais para o novo embate geopolítico mundial. Estados como o Irã e a Coreia do Norte têm investido em capacidades cibernéticas para compensar suas desvantagens em termos de poder militar convencional. Além disso, grupos não estatais, como *hackers* independentes e organizações terroristas, representam ameaças adicionais. A proliferação de ferramentas cibernéticas acessíveis aumentou o risco de ataques provindos de diversos atores e por diversos motivos. Assim, o espaço cibernético é um espaço inseguro por essência, mas também, e muitas vezes, por escolha e necessidade dos Estados que mais controlam essas tecnologias.

Mas como mudar esse cenário e tornar o mundo digital mais seguro para cidadãos, empresas, organizações não governamentais e Estados?

Podemos pensar em algumas alternativas.

A primeira alternativa seria o incremento da cooperação internacional para combater ameaças cibernéticas. Todavia, como já dissemos acima, essa é dificultada por questões de soberania, confiança mútua e interesses divergentes. A criação de normas e padrões globais para a segurança cibernética é um desafio contínuo. Iniciativas como o Grupo de Peritos Governamentais da Organização das Nações Unidas sobre Avanços na Informação e na Tecnologia de Comunicação são passos importantes, mas a implementação e a adesão permanecem complexas.

Melhorias nas regulamentações e políticas nacionais na área são uma questão urgente. Desenvolver e implementar políticas eficazes de segurança cibernética é crucial e isso inclui legislações que exijam padrões de segurança para empresas e infraestrutura crítica, bem como estratégias nacionais de defesa cibernética. A regulação deve equilibrar a proteção contra ameaças e a promoção da inovação tecnológica.

Investir pesado em educação tecnológica e capacitação é a forma mais eficaz de fazer perdurar no tempo medidas de segurança e de defesa cibernéticas. A formação de

profissionais qualificados em segurança cibernética é vital. A demanda por especialistas excede a oferta, e há uma necessidade urgente de programas educacionais e de treinamento para preencher essa lacuna. Todavia, mais importante que formar profissionais especializados na área é dar ao cidadão comum, principalmente aos mais vulneráveis que são os idosos e as crianças, formação para utilizarem as tecnologias sem que se tornem presas fáceis para a criminalidade digital. Um processo efetivo de higiene cibernética, como o realizado no continente europeu, deveria ser um exemplo para o mundo todo de como agir nessa esfera.

Assim, a geopolítica contemporânea e a segurança cibernética estão indissociavelmente ligadas. Os desafios para a defesa cibernética são complexos e multifacetados, exigindo uma abordagem coordenada e inovadora. À medida que a tecnologia continua a evoluir, a importância da segurança cibernética na geopolítica global só tende a aumentar, tornando-se uma área crucial para a segurança nacional e a estabilidade internacional. A colaboração internacional, a inovação tecnológica, a educação e a formulação de políticas eficazes são essenciais para enfrentar os desafios presentes e futuros.

Para promover o debate nesse sentido, esse dossiê especial sobre «Geopolítica contemporânea e os desafios para a segurança e a defesa cibernéticas» vai trazer sete artigos que debaterão diferentes temas.

O artigo «Cooperação em segurança e defesa cibernética e a proteção das democracias sul-americanas», das autoras Jéssica Maria Grassi, Danielle Jacon Ayres Pinto e Graciela de Conti Pagliari, vai problematizar como a proteção das democracias na região sul-americana está intrinsecamente conectada com o aprimoramento do conceito de segurança e defesa cibernéticas.

No artigo seguinte, com o título «A cibernética na grande estratégia: um estudo comparado de Reino Unido, França e Portugal», a proposta dos autores Natália Diniz Schwether e Marcos Aurélio Guedes de Oliveira é promover uma comparação das grandes estratégias de países centrais na política internacional e perceber como esses documentos tratam a questão cibernética.

No terceiro artigo, com o título «Proteção de dados: experiência internacional e o caso brasileiro – relação com a segurança da informação e a governança cibernética», os autores Constança Maria Maia Arruda e Pedro Arthur Linhares Lima trazem um debate muito atual sobre como proteger os dados no ciberespaço e como criar uma governança para aprimorar esses processos.

No próximo artigo, intitulado «Defesa cibernética na guerra russo-ucraniana: um mapeamento dos ataques cibernéticos às infraestruturas críticas da Ucrânia», os autores Thays Felipe David de Oliveira, Renato Victor Lira Brito e Priscylla Cristina de Souza Lippo identificam os principais ataques cibernéticos russos às infraestruturas ucranianas, quais foram os principais alvos e o porquê da sua escolha.

No artigo seguinte, o tema tratado foi «Marco zero: as origens da guerra cibernética orquestrada pelos Estados Unidos da América para atingir a República Islâmica do Irã

(2007-2010)»; escrito pelos autores Fernando H. Casalunga, Eduardo Munhoz Svartman e Bruno Cardoso Reis, o artigo vai debater as estratégias de ataques cibernéticos dos Estados Unidos frente ao Irã e quais foram os ganhos auferidos nessa ação.

No sexto artigo, com o título «Ordem e progresso? Analisando as respostas brasileiras aos cibercrimes», os autores Mariana Grilli Belinotte, Luiz Rogério Franco Goldoni, Joe Devanny e Carlos Frederico Coelho debatem os avanços do Brasil na resposta normativa e prática aos crimes cibernéticos que a sociedade desse país vem enfrentando.

No sétimo artigo, com o título «Consciência situacional como ferramenta estratégica da defesa cibernética», os autores André Lucas Alcântara da Silva e Gills Vilar-Lopes promovem o debate da importância da consciência situacional para promoção da defesa cibernética dos Estados frente às novas ameaças que enfrentam atualmente.

Por fim, esperamos que os artigos desenvolvidos nesse dossiê possam servir de base para aprimorar o debate em torno do tema e produzir processos securitários mais efetivos e que busquem a segurança da sociedade, do indivíduo, dos atores privados e do Estado de forma efetiva e numa lógica colaborativa e nunca belicosa. R:I

Danielle Jacon Ayres Pinto Investigadora sénior do Núcleo de Pesquisa em Política Internacional, Segurança e Defesa (NPSeD). Doutora em Ciência Política pela Universidade Estadual de Campinas (UNICAMP). Professora no Curso de Relações Internacionais e coordenadora do Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina (UFSC). > Centro Socioeconômico – CSE UFSC, R. Roberto Sampaio Gonzaga-Trindade, Florianópolis, Brasil | danielle.ayres@ufsc.br

Marcos Aurélio Guedes de Oliveira Professor titular do Departamento de Ciência Política da Universidade Federal de Pernambuco. > Centro de Filosofia e Ciências Humanas (CFCH) – UFPE, Rua Acadêmico Hélio Ramos, s/n, 6.º andar, Cidade Universitária – Recife, PE, Brasil | marcosaurelioguedes@gmail.com

Natália Diniz Schwether Doutora e pós-doutora em Ciência Política pela Universidade Federal de Pernambuco. > Centro de Filosofia e Ciências Humanas (CFCH) – UFPE, Rua Acadêmico Hélio Ramos, s/n, 6.º andar, Cidade Universitária – Recife, PE, Brasil | n.schwether@unesp.br

Cooperação em segurança e defesa cibernética e a proteção das democracias sul-americanas

Jéssica Maria Grassi | Danielle Jacon Ayres Pinto | Graciela de Conti Pagliari

INTRODUÇÃO

A internet, que já foi compreendida como uma força para liberdade e para democracia, tem se tornado um espaço para amplificação da desinformação, incitação da violência e de contestação da confiabilidade da mídia e das instituições democráticas, configurando-se um local favorável para a ascensão e difusão dos radicalismos de extrema-direita[1]. Sobre isso, a última década mostrou à sociedade mundial – em especial à sul-americana – os grandes desafios aos quais as democracias estarão submetidas no século XXI. Com processos cada vez mais deturpados sobre o conteúdo verídico das informações sobre política, economia, política externa, cultura, segurança e defesa, é possível observar um movimento de crescente descrença da sociedade no conteúdo da informação que recebe dos tradicionais canais de notícias. O resultado desse movimento tem sido um exponencial aumento da crença dos indivíduos em informações de conteúdo falso, transmitida por agentes de espectro ideológico próximo ao do cidadão.

Como consequência, o novo meio digital de sociabilidade da informação tem provocado sérios danos aos pilares democráticos dos Estados, pois a desinformação e as informações falsas têm virado recurso do debate político oficial. Nessa perspectiva, entre as diversas ameaças obser-

RESUMO

A última década mostrou à sociedade mundial – em especial a sociedade sul-americana – os grandes desafios aos quais as democracias estarão submetidas no século XXI. Entre as diversas ameaças observadas no ciberespaço estão as denominadas campanhas de desinformação e as interferências híbridas. Diante disso, esse novo meio digital de sociabilidade da informação tem provocado sérios danos aos pilares democráticos dos Estados, pois a desinformação e as informações falsas têm virado recurso no debate político. Isso posto, o artigo buscará analisar a construção de processos cooperativos na área de segurança e defesa cibernética entre os países sul-americanos entre 2012 e 2020 e seus efeitos na proteção da democracia e do Estado de direito. Defende-se que, devido à dinâmica transfronteiriça do mundo digital e do disseminado alcance de suas ações e consequências, a busca por uma solução a essas demandas perpassa um processo de aprofundamento da cooperação estatal no qual as estratégias de política externa dos Estados são fundamentais para a construção de uma resposta efetiva a esse tipo de ameaça à democracia em âmbito internacional. Nessa perspectiva, com-

→

 https://doi.org/10.23906/ri2024.82a02

preende-se a interdependência entre os Estados nessa esfera e adota-se uma concepção cooperativa para refletir sobre os obstáculos enfrentados pelos países sul-americanos.

Palavras-chave: segurança cibernética, interferências híbridas, democracia, cooperação cibernética.

ABSTRACT

Cooperation in cyber security and cyber defense and the protection of South American democracies

The last decade has shown the global society, especially South American society, the great challenges that democracies will face in the 21st century. Among the various threats observed in cyberspace are the so-called disinformation campaigns and hybrid interference. As a result, this new digital means of information socialization has caused serious damage to the democratic pillars of states, as disinformation and false information have become a feature of political debate. Based on this, the article seeks to analyze how South American countries are building cooperation in cybersecurity and cyber defense between 2012 and 2020, and what the implications are for the protection of democracy and the rule of law. It is argued that, due to the transnational dynamics of the digital world and the wide reach of its actions and consequences, the search for a solution to these demands goes through a process of deepening state cooperation, in which the foreign policy strategies of states are fundamental for building an effective response to this type of threat to democracy at the international level. From this perspective, we understand the interdependence between States in this sphere and adopt a cooperative conception to reflect on the obstacles South American countries face.

Keywords: cybersecurity, hybrid interference, democracy, cyber cooperation.

vadas nesse novo espaço estão as denominadas interferências híbridas, campanhas de desinformação, *fake news*[2], propaganda computacional e outras formas de manipulação da informação por meio do ciberespaço. Tais ferramentas possuem o potencial de comprometer valores democráticos e desestabilizar instituições políticas. Também podem pressionar organizações econômicas e financeiras de um país, afetar seu moral e moldar o cenário interno, conforme as preferências de determinado grupo ou país. Isso tudo com a vantagem do anonimato, já que é extremamente difícil a identificação da origem exata desse tipo de campanha cibernética.

Os países sul-americanos enfrentam uma série de fragilidades políticas e institucionais que se somam a desafios econômicos e geopolíticos enfrentados pela região. Especificamente, no âmbito cibernético, tais países carecem de capacidades cibernéticas[3] e suas debilidades estruturais se originam desde frágeis bases educacionais, especificamente, da falta de incentivos à educação cibernética da sua população, da falta de políticas públicas para a ciência nacional e para a conscientização, até a formação e capacitação de recursos humanos. Sendo a educação, a formação de talentos e o desenvolvimento científico e tecnológico um pilar estratégico para a construção de capacidades cibernéticas, que é a base da qual as demais dimensões da construção de capacidades se sustentarão e, da mesma forma, entendendo a camada *peopleware*[4] como a mais importante para a segurança cibernética de uma nação, essa carência acaba por se refletir nos atuais desafios cibernéticos e democráticos dos países da região. Essa situação deixa esse grupo de países, em sua maioria considerados subdesenvolvidos ou em desenvolvimento, vulneráveis diante das inúmeras ameaças advindas do ciberespaço. Além disso, esse contexto resulta em vantagens e oportunidades de intervenções de atores estatais mais desenvolvidos em países do Sul Geopolítico[5][6].

Diante do exposto, e devido à dinâmica transfronteiriça do mundo digital e do disseminado alcance de suas ações e consequências, entende-se que a busca por uma solução para essas demandas perpassa pelo processo de aprofun-

damento da cooperação interestatal, no qual as estratégias de política externa dos Estados são fundamentais para a construção de uma resposta efetiva a esse tipo de ameaça que traz riscos, inclusive, aos seus processos democráticos. Desse modo, o artigo pretende trabalhar a seguinte questão: os países sul-americanos estão construindo processos cooperativos regionais na área de segurança e defesa cibernética de modo a protegerem suas democracias frente aos desafios da era digital? Acredita-se que, apesar de iniciativas de cooperação cibernética terem tomado forma na região e mesmo com o potencial regional para avançar em processos cooperativos, pouco se evoluiu no sentido de implementar agendas de cooperação multilateral que auxiliem na proteção dos sistemas democráticos regionais.

Esta pesquisa parte de uma perspectiva que evidencia a interdependência entre os Estados e adota-se uma concepção cooperativa para refletir sobre os obstáculos enfrentados pelos países sul-americanos, atentando para as dinâmicas geopolíticas próprias da região. Neste sentido, pelo fato de haver dinâmicas geopolíticas e securitárias a América do Sul justifica-se como um objeto de análise por si só na medida em que este trabalho analisa os elementos de cooperação desenvolvidos a partir dos mecanismos regionais sul-americanos. Embora a analogia trazida da economia de que o Brasil seja um rinoceronte em uma loja de cristais se comparado aos demais países da América do Sul[7], a mesma não retira a capacidade analítica da região como espaço específico de análise.

Para alcançar o objetivo proposto, adota-se a técnica de pesquisa bibliográfica, utilizando, eventualmente, documentos oficiais e notícias para auxiliar na discussão dos tópicos mais atuais. Ademais, ressalta-se que, para analisar a cooperação cibernética na América do Sul, tem-se o ano de 2012 como marco temporal, visto que neste ano os membros da União das Nações Sul-Americanas (Unasul) iniciaram um plano de trabalho para cooperação multilateral na área cibernética no âmbito do seu Conselho de Defesa.

Para desenvolver essa pesquisa o artigo está dividido em três seções. Iniciamos apresentando as principais ameaças à segurança e defesa dos Estados, inclusive no que diz respeito à proteção dos sistemas democráticos. Em seguida, trazemos a discussão sobre processos de cooperação estatal no setor cibernético, destacando estudos que apontam para as vantagens de estratégias cooperativas principalmente para os países do Sul Geopolítico e para países que não possuem nítidos rivais no âmbito militar. Por fim, analisamos o processo de cooperação cibernética que tomou forma na América do Sul, os percalços ao longo dos últimos anos e os efeitos de tais processos cooperativos para a construção de capacidades e proteção das democracias dos países da região.

AMEAÇAS CIBERNÉTICAS E OS RISCOS À DEMOCRACIA NO SÉCULO XXI

As ferramentas do ciberespaço vêm sendo aperfeiçoadas de maneira a revolucionar o modo de se fazer a guerra no século XXI e esse cenário tornou a ciberguerra uma das

grandes preocupações das defesas nacionais hoje em dia[8]. Isso se deve às características que tornam esse espaço diferenciado dos demais[9], à crescente digitalização dos processos e das infraestruturas críticas dos Estados e às consequentes vulnerabilidades inerentes dessas infraestruturas que dependem dos sistemas computacionais[10]. Com isso, constroem-se cenários potencialmente catastróficos, no qual o poder cibernético se traduz em diversas vantagens em conflitos.

AS FERRAMENTAS DO CIBERESPAÇO VÊM SENDO APERFEIÇOADAS DE MANEIRA A REVOLUCIONAR O MODO DE SE FAZER A GUERRA NO SÉCULO XXI: CONSTROEM-SE CENÁRIOS POTENCIALMENTE CATASTRÓFICOS, NO QUAL O PODER CIBERNÉTICO SE TRADUZ EM DIVERSAS VANTAGENS EM CONFLITOS.

Entretanto, segundo Thomas Rid, a probabilidade de uma guerra autônoma no ciberespaço é baixa, quando se conceitua corretamente o termo e se observa as formas mais comuns de atuação dos atores nesse espaço. Para o autor, os atores têm utilizado ferramentas digitais para sabotagem, espionagem e subversão, as quais podem acompanhar operações militares tradicionais, mas não a guerra como a conhecemos desde a teorização clausewitzina[11]. Contudo, tendo em vista as oportunidades que os recursos cibernéticos apresentam para os atores, é necessário entender o crescimento das campanhas de desinformação, propaganda computacional ou manipulação da informação como um elemento promotor do conflito na esfera cibernética[12]. Sobre isso, é importante apresentar o que se tem denominado por interferências híbridas. Interferências híbridas podem ser definidas como ataques sutis, como manipulação da informação, uso de campanhas de desinformação e uma série de recursos não militares, utilizados como meios indiretos para influenciar o debate público, acelerar polarizações políticas, ideológicas, econômicas e sociais de um país e minar sua coesão interna[13].

Elemento central das interferências híbridas é a subversão, citada por Rid, na qual o alvo é a mente humana e sua consciência identitária dentro da sociedade. A subversão pode ser entendida como tentativas de desestabilizar ou minar a integridade ou autoridade do Estado alvo através de atores locais, usando como ferramentas as campanhas de desinformação[14]. Nesse sentido, tais interferências podem ser utilizadas como estratégias complementares (em situações de conflito ou não) para desestabilizar um país e fazê-lo adotar determinada postura. Isso tudo com a vantagem do anonimato e sem ultrapassar o limiar do conflito. Somando-se a isso, essas ações possuem um custo financeiro baixo e menor aporte tecnológico e intelectual. Ao mesmo tempo, são altamente prejudiciais, podendo resultar em importantes danos no «mundo físico», além de serem de difícil contenção e resiliência por parte do ator atacado.

As campanhas de desinformação têm como elemento central a distorção da verdade, de modo que se torna cada vez mais difícil distinguir fato de ficção. Tais ferramentas digitais tornaram-se fundamentais para obter vantagens em períodos eleitorais e têm sido utilizadas para promover artificialmente ou manipular pontos de vista que favorecem líderes políticos, para abafar opiniões divergentes ou para atacar ou desacreditar

opositores. Desse modo, têm potencial de acelerar a polarização, interferir ou alterar resultados políticos e, de forma efetiva, desestabilizar os pilares das democracias liberais, pondo em risco as liberdades civis[15].

Apontou-se, em estudo publicado em 2019, que 68% dos países utilizaram *trolls*, patrocinados pelo Estado, para atingir opositores e/ou jornalistas; 89% usaram de propaganda computacional para atacar a oposição política; e 75% dos países usaram desinformação e manipulação da mídia para enganar os usuários. Constatou-se que, pelo menos, 70 países vêm realizando campanhas cibernéticas com fins políticos[16]. De forma similar, em investigações realizadas entre 2016 e 2019, as quais analisaram 97 eleições nacionais em países livres ou parcialmente livres, identificou que em 20 países[17] houve claras evidências de interferências estrangeiras. Entre os 20 países citados neste estudo estão Brasil e Colômbia[18].

As eleições presidenciais do Brasil, em 2018 e 2022, são importantes exemplos na região sul-americana do potencial desestabilizador das ferramentas digitais, uma vez que o processo foi caracterizado pelo uso das redes sociais para disseminar notícias falsas, contestar a confiabilidade da mídia e das instituições democráticas, acirrando a polarização, aumentando a violência política e minando a coesão interna[19]. Na Colômbia, o referendo para a paz em 2016 e as eleições presidenciais em 2018 e em 2022 também envolveram «mentiras estratégicas, falácias, propaganda, fortes apelos à emoção, conspirações ou narrativas de polarização»[20]. Ainda, as eleições na Argentina em 2023 e outros tantos cenários de desinformação e manipulação através das plataformas digitais marcaram a política latino-americana nos últimos anos[21]. Cabe reiterar a complexidade de definir a origem exata dessas campanhas cibernéticas, as quais podem se originar ou serem financiadas por atores externos.

As manipulações que podem surgir como ação de atores externos nesse pleito fazem com que a democracia seja o alvo direto dos recursos cibernéticos utilizados numa lógica não violenta. Logo, a clivagem ideológica que tal ação pode causar promove ruptura social e pode, como afirmam Oliveira e Izycki,

> «ser interpretad[a] como evidência de um ambiente democrático em deterioração ou, pelo menos, de um ecossistema político no qual a violação da privacidade dos cidadãos com o objetivo de direcionar sua assimilação cognitiva da realidade é uma forma aceitável de conduzir os assuntos governamentais»[22].

O fato é que, como já antevê o relatório do Fórum Econômico Mundial de Davos de 2024, a informação falsa e a desinformação serão as principais ameaças securitárias do mundo no curto prazo. Isso porque nos próximos dois anos mais de 97 países, incluindo o mais populoso do mundo – a Índia – e o mais rico do mundo – os Estados Unidos – terão eleições importantes[23].

Todavia, quando se trata de recursos cibernéticos, há a necessidade de se ajustar o foco da segurança e da defesa, abarcando toda a complexidade e sinuosidade dos desafios

que advêm do ciberespaço, já que medidas tradicionais de defesa não são suficientes para esses novos tipos de ameaças. Além disso, Wigell reitera que os meios para se proteger desses novos métodos devem considerar também a defesa dos valores democráticos. Para o autor,

> «os valores democráticos liberais não têm de ser vulnerabilidades em matéria de segurança, mas podem ser transformados em pontos fortes e instrumentos para dissuadir de forma credível os agressores híbridos, tornando simultaneamente as nossas democracias ocidentais mais robustas e resilientes»[24].

Nesse sentido, as estratégias de segurança, defesa e construção de capacidades cibernéticas amplas devem considerar abordagens que envolvam toda a sociedade, abordagens cooperativas entre autoridades do setor público, do setor privado, da academia e demais organizações da sociedade civil[25]. Ou, como alguns autores denominam, uma abordagem em tríplice hélice[26]. Como pondera Wigell, «nesta nova era de política subversiva, em que a dicotomia clássica vestefaliana entre assuntos internos e externos do Estado se esbateu, a dissuasão é mais difícil de alcançar apenas através da ação do Estado»[27].

Nessa direção, tendo em vista a dinâmica transfronteiriça do mundo digital e o disseminado alcance de suas ações, medidas de cooperação interestatais também são fundamentais para promover segurança, bem como para a promoção de um processo de governança cibernética internacional que deve ser consolidado de forma ampla. Nesse sentido, analisando os diversos desafios enfrentados pelos países sul-americanos na construção de suas capacidades cibernéticas, conforme mencionado anteriormente, entendemos que o processo de aprofundamento da cooperação estatal é fundamental para a construção de uma resposta efetiva a essas ameaças na região. Essa é a discussão que pretendemos ressaltar na seção seguinte.

COOPERAÇÃO PARA A CONSTRUÇÃO DE CAPACIDADES CIBERNÉTICAS: BUSCANDO SUPERAR DESAFIOS PROVENIENTES DO CIBERESPAÇO

Apesar de iniciativas cooperativas estarem tomando forma, estudos que discutam profundamente a cooperação internacional ainda não estão no centro da discussão quando o assunto é segurança e defesa cibernética, sobretudo por tratar de temas sensíveis e que envolvem a construção da confiança entre os atores[28]. A lógica dominante dá ênfase à securitização e, mesmo, militarização do ciberespaço, abordando-o como um novo domínio para realização de guerras; discute-se, portanto, conflitos, armas cibernéticas, dissuasão militar cibernética e possibilidade de uma corrida armamentista cibernética se desenvolver[29]. Esse contexto deixaria pouco espaço para medidas cooperativas, já que ressalta um ambiente de competição onde a construção da confiança torna-se uma missão quase impossível.

Entretanto, novas perspectivas sobre a temática vêm tomando forma, ressaltando a necessidade de propor alternativas para a construção de capacidades cibernéticas que ultrapassem a lógica militarizada, atentando para o fato que a era digital demanda respostas diferenciadas[30]. Essas visões apontam para dinâmicas cooperativas, o desenvolvimento da diplomacia cibernética e de ações coordenadas entre atores estatais, não estatais e os diversos setores da sociedade. Justifica-se o caráter transnacional dessa esfera, a interligação dos sistemas, a interdependência entre os atores e as características intrínsecas desse ambiente para fortalecer temáticas relacionadas à governança da internet, a construção da confiança entre os atores e o estabelecimento de acordos bilaterais e multilaterais no setor[31].

Conforme Mikser[32], pensar a construção de capacidades cibernéticas desde uma perspectiva cooperativa regional pode melhorar a condição dos países se desenvolverem neste setor, construindo capacidades mais sólidas, aumentando sua consciência sobre as ameaças emergentes e propondo mecanismos mais efetivos para enfrentá-las. Isso propiciaria um espaço mais estável, principalmente levando em consideração a interconexão entre os Estados no ciberespaço.

Diante disso, pode-se observar iniciativas cooperativas tomando forma em organizações internacionais, como na Organização do Tratado do Atlântico Norte, na União Europeia, na Associação das Nações do Sudeste Asiático, na Organização dos Estados Americanos, no Mercosul e nos fóruns existentes no âmbito das Nações Unidas e na União Internacional de Telecomunicações, como as reuniões do Group of Governmental Experts e do Open-Ended Working Group[33].

Perspectivas cooperativas são particularmente importantes para os países sul-americanos, os quais enfrentam dificuldades econômicas, carecem de recursos humanos qualificados, de habilidades e conhecimento, de desenvolvimento tecnológico e investimento em ciência nacional. Consequentemente, permanecem dependentes dos países desenvolvidos, importando suas soluções para o setor[34]. Ademais, de modo geral, possuem fragilidades institucionais e fraca estrutura de governança cibernética interna[35].

PAÍSES DO SUL GEOPOLÍTICO, COMO OS PAÍSES SUL-AMERICANOS, ENCONTRAM-SE À MARGEM DA CONSTRUÇÃO DE UMA GOVERNANÇA CIBERNÉTICA INTERNACIONAL.

Adicionalmente, conforme destacam Ceballos, Maisonnave e Londoño:

> «As *fake news* e o *lawfare*, fenômenos plenamente presentes nas disputas latino-americanas, são apenas exemplos do potencial antidemocrático das ferramentas digitais se não houver uma visão estratégica em torno delas. A colonialidade do poder e do saber faz com que, enquanto as grandes potências priorizam sua autonomia digital na América Latina, os avanços neoliberais desfazem as políticas estatais de desenvolvimento nacional. Desta forma, a formação de profissionais em tecnologia é negligenciada, estes são flexíveis à estrangeirização dos nossos sistemas tecnológicos e de gestão da informação e, do ponto de vista de uma integração tecnológica regional essencial, carecem de projetos sustentáveis»[36].

Cabe ressaltar que a interconectividade dos sistemas e a carência de regulamentação no ciberespaço facilitam ataques que possam promover rupturas políticas e militares. Assim, em um contexto de acirramento da competição geopolítica internacional, para esse grupo de países torna-se particularmente fundamental a construção de capacidades cibernéticas para que sejam capazes de proteger suas instituições políticas, econômicas e militares, inclusive frente às interferências híbridas mencionadas[37].

Ainda, países do Sul Geopolítico, como os países sul-americanos, encontram-se à margem da construção de uma governança cibernética internacional, sendo insuficientemente representados nas instâncias internacionais de tomada de decisão, de formulação de políticas e de desenvolvimento de mecanismos para o futuro do ciberespaço. Analisando por essa perspectiva, constata-se, portanto, que a estrutura global do ciberespaço perpetua a divisão Norte-Sul[38].

Desse modo, reitera-se a importância de processos de cooperação Sul-Sul para que esses países possam articular ações para a promoção de medidas de segurança, defesa e resiliência no espaço cibernético, desenvolvendo mecanismos de compartilhamento de informações, conhecimentos e experiências, iniciativas conjuntas para treinamento, capacitação e resolução de desafios comuns, trabalhando conjuntamente para a construção de suas capacidades cibernéticas, diminuindo os custos envolvidos, e buscando romper com sua dependência em relação aos países desenvolvidos. Ademais, processos cooperativos são fundamentais para que esses países possam coordenar posições visando aumentar seu poder de decisão e de barganha, para que tenham seus interesses atendidos nos espaços de governança internacional[39].

Como aponta Herz:

> «o debate público sobre segurança cibernética precisa ser promovido em base local, nacional, regional e internacional. Diferentes órgãos e setores do aparato estatal, organizações da sociedade civil, comunidade técnica, setor privado, academia e entidades internacionais precisam ser ouvidos e precisam ter participação nas formas de coordenação. Este processo diz respeito à saúde das instituições democráticas, mas também à necessidade de informação da população sobre as regras e processos relativos à Quarta Revolução Industrial»[40].

Assim, refletindo sobre o histórico das iniciativas de cooperação e integração na América do Sul – principalmente considerando a criação do Conselho de Defesa Sul-Americano (CDS) da Unasul e as novas agendas postas no Mercosul nas últimas duas décadas –, bem como os avanços que tais processos proporcionaram no auge de seus funcionamentos[41], percebe-se o potencial para medidas cooperativas na região também para o âmbito cibernético. Ainda, observando o cenário regional, não há percepções sobre disputas de poder no domínio cibernético entre os países sul-americanos e os países que já projetaram e desenvolveram iniciativas de cooperação cibernética[42]. Desse

modo, a próxima seção buscará compreender como foi e está sendo encaminhada uma agenda de cooperação multilateral na área cibernética.

COOPERAÇÃO CIBERNÉTICA NA AMÉRICA DO SUL: AVANÇOS E RETROCESSOS

A América do Sul é uma região consideravelmente heterogênea, onde se observam notáveis assimetrias em questões econômicas, políticas, sociais e securitárias. Apesar das inúmeras diferenças entre os Estados da região, o contexto geopolítico internacional os une, já que, por um ângulo distinto, tais países também enfrentam inúmeros desafios políticos, econômicos, sociais e securitários que os aproximam para além do aspecto meramente geográfico. Da mesma forma, se observarmos as capacidades cibernéticas desses Estados, encontraremos situações substancialmente diferenciadas e, por outro lado, desafios que têm o potencial de os aproximar, já que os diferentes estágios em que os países se encontram nessa área podem ser analisados a partir de uma perspectiva de complementaridade, na qual os países podem cooperar e contribuir para a construção de capacidades regionais a partir de suas experiências e avanços individuais[43].

Do ponto de vista da cooperação multilateral, os países sul-americanos iniciaram um importante diálogo no âmbito do CDS da Unasul. Em 2012, os Estados-Membros criaram um plano de trabalho buscando oportunidades de coordenar posições e de estabelecer políticas e mecanismos regionais para combater as ameaças cibernéticas e informáticas. Os Estados estabeleceram a criação de um Grupo de Trabalho em Ciberdefesa e entenderam, como um primeiro passo, a necessidade de definir conceitos comuns na área. A partir disso, seriam avaliadas as possibilidades de avanços com a criação de políticas e mecanismos para lidar com tais ameaças cibernéticas. Entre outras coisas, também previram que buscariam diagnosticar as situações enfrentadas pelos países, identificar os principais atores, instituições e protocolos de cada país, propor programas de educação e exercícios de capacitação conjuntos[44].

Após os escândalos de espionagem norte-americana, houve um fortalecimento das iniciativas no âmbito da Unasul, com ênfase à defesa cibernética. Em 2013, em declaração conjunta, os países estabeleceram, inclusive, a intenção de promover o desenvolvimento de tecnologias regionais e de instituir iniciativas conjuntas entre Mercosul e Unasul[45]. Ainda, nesse período, chegaram a propor a construção e conexão das redes de fibra ótica dos países, visando tornar as telecomunicações mais seguras[46].

APÓS OS ESCÂNDALOS DE ESPIONAGEM NORTE-AMERICANA, HOUVE UM FORTALECIMENTO DAS INICIATIVAS NO ÂMBITO DA UNASUL, COM ÊNFASE À DEFESA CIBERNÉTICA.

Da mesma forma, após esses vazamentos, algumas conversações no âmbito do Mercosul também tomaram forma, essas mais voltadas à segurança da informação e das comunicações. Cria-se, a partir disso, um grupo de trabalho com especialistas sobre o tema, os quais chegaram a esboçar linhas de ação que perpassavam discussões sobre regulamentações, desenvolvimento de *softwares*, intercâmbio de informação, capacitação

e desenvolvimento tecnológico. O grupo, no entanto, não obteve resultados concretos e deixou de se reunir após 2015[47].

Já no âmbito da Unasul, em 2014, na X Reunião da Instância Executiva do Conselho de Defesa Sul-Americano, os países-membros estabeleceram, entre seus objetivos: produzir e sistematizar uma ampla reflexão sobre as definições conceituais da defesa e segurança cibernética, de modo a unificá-las no nível regional; criar um grupo de trabalho e uma rede de contatos entre as autoridades competentes para troca de conhecimentos, de procedimentos e de soluções no âmbito da defesa cibernética[48]. Os planos de ação de 2015, 2016 e 2017 previram a continuação das atividades do Grupo de Trabalho de Ciberdefesa, a coordenação de ações com o Conselho de Infraestrutura e Planejamento (Cosiplan) e a realização de um seminário sobre o tema, além da necessidade de repensar o cronograma do plano de trabalho da instituição[49].

No âmbito do Mercosul, também foi criado o Grupo Agenda Digital em 2017. Este se voltou, principalmente, ao tema da economia digital. Os planos do Grupo discutem, entre outros tópicos, aspectos técnicos e regulatórios sobre governo eletrônico, infraestrutura digital e conectividade, segurança e confiança do ambiente digital, bem como habilidades digitais[50].

Desafortunadamente, não se constatou significativos progressos nas discussões. Observa-se que os países não conseguiram avançar nem no sentido de homogeneizar os termos e desenvolver conceitualizações comuns, muito menos avançaram na proposição de políticas e estratégias conjuntas para o setor[51]. Entre os principais agravantes para esse cenário estão a polarização política, as crises internas enfrentadas pelos países e as interferências externas à região, as quais resultaram no processo de desmantelamento da Unasul a partir de 2016 e a consequente paralização dos direcionamentos que vinham sendo dados no âmbito do CDS, bem como a relativa estagnação nas conversações no âmbito do Mercosul[52].

Ainda, o cenário da cooperação e da integração na região já enfrentava diversos problemas estruturais, que perpassam, por exemplo, a fraca institucionalidade dos processos de integração, a falta de recursos e as debilidades internas dos Estados que travam o prosseguimento de vários projetos. Ademais, diante da polarização e das heterogeneidades regionais, seja em termos políticos, econômicos, sociais ou securitários, as decisões por consenso tornam-se complexas[53].

Assim, conforme pondera Justribó, os países sul-americanos apresentam marcos legislativos, políticos e doutrinários diferentes, o que resulta em avanços heterogêneos[54]. Isso tudo dificulta posicionamentos e avanços conjuntos em processos cooperativos na América do Sul, além de deixar a região em mais um cenário de dependência dos atores hegemônicos do sistema e vulnerável diante das inúmeras ameaças cibernéticas mencionadas na primeira seção deste artigo. Para Herz, o desmantelamento da Unasul, especificamente do CDS, representou uma oportunidade perdida, diante da viabilidade de, regionalmente, harmonizar as legislações, criar

regras e articular políticas, criar mecanismos de gestão de crises e coordenar posições em fóruns internacionais[55].

Diante do enfraquecimento dos processos cooperativos no âmbito sul-americano, ampliou-se o espaço para a atuação em mecanismos no nível continental, já que os países alargaram o diálogo sobre tais temas na Junta Interamericana de Defesa OEA. A OEA adotou ainda em 2004 uma estratégia conjunta para segurança cibernética e vem avançando com a proposição de medidas de confiança, realizando investigações nos países-membros, desenvolvendo informes e propondo treinamentos, simulações e capacitações conjuntas[56]. Cabe mencionar, entretanto, que a instituição é sediada nos Estados Unidos – sendo este também seu principal financiador – e tem sido, historicamente, um espaço para a propagação da agenda securitária da potência do Norte, sendo, portanto, um símbolo da ordem norte-americana na América Latina. Para mais, essa situação deixa a América do Sul novamente dependente de mecanismos externos para a resolução de problemáticas regionais[57].

Não obstante, alguns consensos parecem persistir na região. Entre eles estão a defensa da necessidade de normas mais específicas e vinculativas no nível internacional, a construção de confiança entre os atores e o estabelecimento da Organização das Nações Unidas como plataforma para diálogos sobre a paz, a segurança e a estabilidade internacional do ciberespaço[58]. Partindo de consensos já estabelecidos e buscando novas agendas, os Estados podem unir forças para fazer frente em processos de governança internacional, aumentar seus níveis de segurança cibernética e combater os desafios que ameaçam as democracias sul-americanas.

Por fim, apesar dos desafios para a consolidação de uma agenda de cooperação cibernética na América do Sul, o período de auge dos processos de cooperação e integração regional demonstra o potencial da região em avançar na proposição de medidas conjuntas em diversas áreas, inclusive em segurança e defesa, e solucionar controvérsias regionalmente de forma autônoma. Tais iniciativas possibilitaram a maior coesão regional e demonstraram a capacidade de mobilização da região em prol de uma inserção internacional menos dependente[59], processo que, principalmente na esfera cibernética, será fator estratégico em um futuro próximo tanto para o desenvolvimento da região como para sua segurança em âmbito coletivo.

CONSIDERAÇÕES FINAIS

Esta pesquisa visou, em um primeiro momento, analisar as ameaças cibernéticas e os desafios que estas oferecem à estabilidade democrática. A partir disso, discutiu-se as abordagens cooperativas no setor cibernético e a construção de processos de cooperação na América do Sul, observando o cenário geopolítico sul-americano e ponderando sobre os efeitos dessas medidas para a proteção dos pilares democráticos. Defendemos que a busca por uma solução para as demandas dos países perpassa pelo processo de aprofundamento da cooperação regional, uma vez que estratégias de política externa

são fundamentais para construção de uma resposta efetiva a essas novas ameaças à segurança e defesa dos Estados. Além disso, argumentamos que as ameaças cibernéticas demandam abordagens diferenciadas e mais abrangentes que abarquem toda a complexidade e sinuosidade dos desafios estabelecidos com o espaço cibernético.

Partindo dessa perspectiva, retomando as discussões propostas, além de todas as ameaças originadas no ciberespaço já amplamente discutidas, esse ambiente traz novas ferramentas que atuam também de forma mais sutil e que possuem a capacidade de acelerar polarizações, minar a coesão interna e, principalmente, desestruturar os sistemas democráticos. Essas ferramentas estão sendo empregadas em interferências híbridas em diversos Estados, utilizando, frequentemente, atores locais para tais ações. Diante disso, abordagens que ultrapassem a lógica militarizada, que abranjam medidas cooperativas multissetoriais, envolvendo os setores público e privado bem como a sociedade civil, e medidas de cooperação interestatais estão sendo discutidas pela academia. Compreende-se que tais ameaças necessitam de respostas mais abrangentes, que melhorem as condições dos países se desenvolverem no setor e auxiliem no desenvolvimento de mecanismos mais eficientes para enfrentar os desafios emergentes. Essas discussões têm especial relevância para os países do Sul Geopolítico, que enfrentam desafios econômicos, tecnológicos, fragilidades institucionais e grande dependência em relação às potências do Norte.

Muito embora os desafios à cooperação entre os países da região apontados neste trabalho permaneçam, a percepção desses acerca da importância de normas multilaterais internacionais construtoras da confiança demonstra que há consenso no que diz respeito à necessidade de criação de normas de governança cibernética. Este é um ponto fundamental para sustentar o argumento de que os países devem buscar respostas que ultrapassem as tradicionais reações securitárias, voltando seus esforços também para ações multilaterais centradas no nível regional, desenvolvendo estratégias conjuntas na região. Como apontado, isso configuraria um caminho promissor, de modo a fazer frente às ameaças digitais que vêm desestabilizando suas democracias nos últimos anos.

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Jéssica Maria Grassi Investigadora associada do Núcleo de Pesquisa em Política Internacional, Segurança e Defesa (NPSeD). Doutora em Relações Internacionais pela Universidade Federal de Santa Catarina (UFSC).

> Centro Socioeconômico – CSE UFSC, R. Roberto Sampaio Gonzaga-Trindade, Florianópolis, Brasil | jessicamgrassi@gmail.com

Danielle Jacon Ayres Pinto Investigadora sénior do Núcleo de Pesquisa em Política Internacional, Segurança e Defesa (NPSeD). Doutora em Ciência Política pela Universidade Estadual de Campinas (UNICAMP). Professora no Curso de Relações Internacionais e coordenadora do Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina (UFSC).
> Centro Socioeconômico – CSE UFSC, R. Roberto Sampaio Gonzaga-Trindade, Florianópolis, Brasil | danielle.ayres@ufsc.br

Graciela de Conti Pagliari Professora no Departamento de Economia e Relações Internacionais da Universidade Federal de Santa Catarina (UFSC). Coordenadora e investigadora sénior do Núcleo de Pesquisa em Política Internacional, Segurança e Defesa (NPSeD).Doutora em Relações Internacionais pela Universidade de Brasília (UNB).
> Centro Socioeconômico – CSE UFSC. R. Roberto Sampaio Gonzaga-Trindade, Florianópolis, Brasil | graciela.pagliari@gmail.com

NOTAS

1 BRADSHAW, Samantha; HOWARD, Philip N. – *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. University of Oxford, Computational Propaganda Research Project, working paper, report n.º 19, 2019; AYRES PINTO, Danielle Jacon; MORAES, Isabela – «As mídias digitais como ferramentas de manipulação de processos eleitorais democráticos: uma análise do caso Brexit». In *Revista de Estudios Sociales*. Bogotá. N.º 74, outubro-dezembro de 2020, pp. 71-82.

2 As *fake news* são compreendidas como uma das formas que apresentam as campanhas de desinformação. Se caracterizam por informações falsas, inventadas ou distorcidas, visando enganar ou manipular a opinião pública e distorcer o debate político. Ver: CURI JÚNIOR, Aribelco; ALFAYA, Natalia Maria Ventura da Silva – «O impacto das fake news nas eleições presidenciais de 2018 e 2022: prejuízos para a democracia e a sociedade». In *Revista do Instituto de Direito Constitucional e Cidadania*. Paraná. Vol. 8, N.º 1, janeiro-junho de 2023, pp. 1-11.

3 O conceito de capacidade cibernética é particularmente difícil de ser mensurado, não havendo consenso na literatura sobre seus componentes, indicadores ou como efetivamente devem ser avaliadas as capacidades dos Estados. Para uma compreensão mais aprofundada sobre elementos que sustentam a construção de capacidades cibernéticas, ver GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas e os Processos Cooperativos no Contexto Geopolítico Sul-Americano». Universidade Federal de Santa Catarina, Florianópolis, Brasil, 2023. Tese de doutorado em Relações Internacionais.

4 Conforme Ferreira Neto, o ciberespaço pode ser entendido a partir de três camadas: o *hardware*, que seriam os componentes do sistema; o *software*, que diz respeito aos sistemas e à programação; e a *peopleware*, que se refere às pessoas que atuam nesse ambiente. Ver: FERREIRA NETO, Walfredo Bento – «Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder». In *Revista das Ciências Militares, Coleção Meira Mattos*. Rio de Janeiro. Vol. 1, janeiro-abril de 2014, pp. 7-18. A *peopleware* seria a camada mais importante ou a base de sustentação do ciberespaço, conforme Grassi, já que «diferente dos demais espaços geográficos – terrestre, marítimo, aéreo e extra-atmosférico – que existem independentes da vontade humana, o ciberespaço é produto da ação humana, sua evolução ou transformação ao longo do tempo é devida à atuação do ser humano, que desenvolve e interage com o elemento físico e que, a partir dele, põe em funcionamento todos os seus sistemas» (GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...»).

5 O termo passou a ser utilizado como um substituto de Sul Global por autores que defendem a insuficiência analítica, a imprecisão semântica e a generalização do conceito e compreendem que este reforça as assimetrias e desigualdades da clivagem Norte-Sul. Nesse sentido, o uso do termo «Sul Geopolítico» busca «reforçar a agência dos atores do Sul, na medida em que traz uma imagem autoconstruída, a partir das leituras que eles têm das relações internacionais e de suas inserções». Ainda, «o conceito apresentado busca colocar essas disputas e tensões no centro da análise, convidando a uma leitura histórica das assimetrias, das relações de dominação, da exploração e da humilhação como fatores constitutivos das relações internacionais» (ver COSTA, Hugo Bras Martins da; DUARTE, Rubens de Siqueira – «Sul Global versus Sul Geopolítico: um debate quanto à pertinência analítica dos conceitos». In *Austral: Brazilian Journal of Strategy and International Relation*. Porto Alegre. Vol. 12, N.º 24, 2023, p. 24-25).

6 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

7 OLIVEIRA, Marcos Aurelio Guedes, et al. – *Guia de Defesa Cibernética da América do Sul*. Recife: Ed. UFPE, 2017.

8 AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria – «Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil». In *Revista Brasileira de Estudos de Defesa*. Vol. 7, N.º 2, julho-dezembro de 2020, pp. 103-131.

9 NYE JR, Joseph S. – *The Future of Power*. Nova Iorque: Public Affairs, 2011; PORTELA, Lucas Soares – «Movimentos Centrais e Subjacentes no Espaço Cibernético do Século XXI». Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2016. Dissertação de mestrado em Ciências Militares; FERREIRA NETO, Walfredo Bento – «Territorializando o "novo" e (re)territorializando os tradicionais...».

10 AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria – «Guerra cibernética...».

11 RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies*. Vol. 35, N.º 1, 2012, pp. 5-32.

12 OLIVEIRA, Raquel Jorge de; IZYCKI, Eduardo – «Propaganda computacional na prática: os casos de Estados Unidos,

França, Colômbia e Venezuela». In *XI Encontro Nacional Da Associação Brasileira de Estudos de Defesa* [online]. 2021, pp. 1-18.

13 WIGELL, Mikael – «Democratic deterrence: "how to dissuade hybrid interference». In *Washington Quarterly*. Vol. 44, N.º 1, 2021, pp. 49-67.

14 RID, Thomas – «Cyber war will not take place».

15 BRADSHAW, Samantha; HOWARD, Philip N. – *The Global Disinformation Order…*; AYRES PINTO, Danielle Jacon; MORAES, Isabela – «As mídias digitais como ferramentas de manipulação…».

16 BRADSHAW, Samantha; HOWARD, Philip N. – *The Global Disinformation Order…*.

17 Os atores citam os seguintes países: Austrália, Brasil, Colômbia, República Checa, Finlândia, França, Alemanha, Indonésia, Israel, Itália, Malta, Montenegro, Países Baixos, Macedónia do Norte, Noruega, Singapura, Espanha, Taiwan, Ucrânia e Estados Unidos da América.

18 HANSON, Fergus, et al. – *Hacking Democracies: Cataloguing Cyber-enabled Attacks on Elections*. Australian Strategic Policy Institute, policy brief, report n.º 16, 2019.

19 CURI JÚNIOR, Aribelco; ALFAYA, Natalia Maria Ventura da Silva – «O impacto das fake news nas eleições presidenciais de 2018 e 2022…».

20 GUTIÉRREZ-COBA, Liliana; RODRÍGUEZ-PÉREZ, Carlos – «Estrategias de posverdad y desinformación en las elecciones presidenciales colombianas 2022». In *Revista de Comunicación*. Vol. 22, N.º 2, 2023, pp. 225-242. Tradução livre dos autores.

21 RAULS, Leonie – «How Latin American governments are fighting fake news». In *Americas Quartely*. 19 de outubro de 2021. Consultado em: 12 de outubro de 2023. Disponível em: https://americasquarterly.org/article/how-latin-american-governments-are-fighting-fake-news/; CRIALES, José Pablo – «La inseguridad irrumpe en la campaña electoral argentina aupada por las noticias falsas en redes sociales». In *El País*. Buenos Aires, 11 de agosto de 2023. Consultado em: 12 de outubro de 2023. Disponível em: https://elpais.com/argentina/2023-08-11/la-inseguridad-irrumpe-en-la-campana-electoral-argentina-aupada-por-las-noticias-falsas-en-redes-sociales.html.

22 OLIVEIRA, Marcos Aurelio Guedes, et al. – *Guia de Defesa Cibernética da América do Sul*, p. 4.

23 FÓRUM ECONÔMICO MUNDIAL – *Global Risks Report 2024*. Genebra: Fórum Econômico Mundial, 2024. Consultado em: 28 de fevereiro de 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

24 WIGELL, Mikael – «Democratic deterrence…», p. 50. Tradução livre a partir do original.

25 WIGELL, Mikael – «Democratic deterrence…»; OLIVEIRA, Raquel Jorge de; IZYCKI, Eduardo – «Propaganda computacional na prática…»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

26 PAGLIARI, Graciela de Conti; AYRES PINTO, Danielle Jacon; VIGGIANO, Juliana – «Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratégica: um estudo prospectivo». In *Defesa Cibernética e Mobilização Nacional*. Recife: Ed. UFPE, 2020, pp. 153-174.

27 WIGELL, Mikael – «Democratic deterrence…», p. 53. Tradução livre a partir do original.

28 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

29 LIBICKI, Martin – *Cyberdeterrence and Cyberwar*. Pittsburgh: RAND Corporation, 2009; LIFF, Adam P. – «Cyberwar: a new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war». In *Journal of Strategic Studies*. Vol. 35, N.º 3, 2012, pp. 401-428; STONE, John – «Cyber war will take place!». In *Journal of Strategic Studies*. Vol. 36, N.º 1, 2013, pp. 101-108; RID, Thomas – «Cyber war will not take place»; AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria – «Guerra cibernética…».

30 SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South». In *Third World Quarterly*. Vol. 39, N.º 5, 2018, pp. 821-837; CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges and global inequalities in cyber capacity building». In *Third World Quarterly*. Vol. 41, N.º 6, 2020, pp. 917-938.

31 MULLER, Lilly Pijnenburg – *Cyber Security Capacity Building in Developing Countries*. Norwegian Institute for International Affairs (NUPI), Policy brief n.º 15, 2015, pp. 1-5; PAWLAK, Patryk – «Capacity building in cyberspace as an instrument of foreign policy». In *Global Policy*. Vol. 7, N.º 1, 2016, pp. 83-92; PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building: conundrum and opportunity». In *Journal of Cyber Policy*. Vol. 2, N.º 1, 2017, pp. 123-144; BARRINHA, André; RENARD, Thomas – «Cyber-diplomacy: the making of an international society in the digital age». In *Global Affairs*. Vol. 3, N.º 4-5, 2017, pp. 353-364; HERZ, Monica – «Cibersegurança na América Latina». In *Conferência de Segurança Internacional do Forte de Copacabana – A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global*. Fundação Konrad Adenauer; Centro Brasileiro de Relações Internacionais. Coleção de Policy Papers, 2019, pp. 9-19; SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South»; CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges…».

32 MIKSER, Sven – «La necesidad de una respuesta armonizada a las amenazas de ciberseguridad: el camino a seguir». In *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe*. Observatorio de la Ciberseguridad en América Latina y el Caribe, Report Ciberseguridad 2020, pp. 34-37.

33 PAWLAK, Patryk – «Capacity building in cyberspace as an instrument of foreign policy»; PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building…»; HERZ, Monica – «Cibersegurança na América Latina».

34 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

35 MULLER, Lilly Pijnenburg – *Cyber Security Capacity Building in Developing Countries*; SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South»; CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges…»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

36 CEBALLOS, Luis Dario; MAISONNAVE, Marcelo Andrés; LONDOÑO, Carlos Rafael Britto – «Soberanía tecnológica digital en Latinoamérica». In *Revista Propuestas para el Desarrollo*. México. Ano IV, N.º IV, outubro de 2020, p. 152. Tradução livre a partir do original.

37 MULLER, Lilly Pijnenburg – *Cyber Security Capacity Building in Developing Countries*; SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South»; PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building…»; CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges…».

38 CHENOU, Jean-Marie; FUERTE, Juan Sebastián Rojas – «The difficult path to the insertion of the Global South in Internet governance». In *Internet Governance in the Global South: History, Theory, and Contemporary Debates*. São Paulo: NUPRI/USP, 2018, pp. 42-73.

39 *Ibidem*; PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building…»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas…».

40 HERZ, Monica – «Cibersegurança na América Latina», p. 17.

41 Para aprofundamento sobre as iniciativas de cooperação e integração sul-americanas, recomenda-se: FUCCILLE, Alexandre – «O Brasil e a América do Sul: (re)pensando a segurança e a defesa na região». In *Revista Brasileira de Estudos de Defesa*. Vol. 1, N.º 1, 2014, pp. 112-146; PAGLIARI, Graciela de Conti – «Conselho de Defesa Sul-Americano e a adoção de

medidas de fortalecimento da confiança». In *Carta Internacional*. Belo Horizonte. Vol. 10, N.º 3, 2015, p. 23; TEIXEIRA JÚNIOR, Augusto Wagner Menezes – «Contribuições do Conselho de Defesa Sul-Americano para a Cooperação Militar». In *Revista Política Hoje*. Vol. 24, N.º 1, 2015, pp. 57-70; BRICEÑO-RUIZ, José – «Da crise da pós-hegemonia ao impacto da covid-19: o impasse do regionalismo latino-americano». In *Revista Cadernos de Campo*. Araraquara. N.º 29, julho-dezembro de 2020, pp. 21-39; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria; KERR OLIVEIRA, Lucas – «A cooperação em segurança e defesa na América do Sul a partir de 2016: desafios e perspectivas». In *Revista Brasileira de Estudos Estratégicos*. Niterói. Vol. 16, N.º 26, 2021, pp. 25-49; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global: desestabilização e (des)integração sul-americana». In *Conjuntura Austral*. Porto Alegre. Vol. 12, N.º 61, 2022, pp. 33-46.

42 JUSTRIBÓ, Candela – «Ciberdefensa: una visión desde la UNASUR». In *VII Congreso del Instituto de Relaciones Internacionales*. La Plata, 2014, pp. 1-24; GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano: (in) conformação de políticas de segurança e defesa cibernética?». In *Austral: Revista Brasileira de Estratégia e Relações Internacionais*. Porto Alegre. Vol. 7, N.º 14, julho-dezembro de 2018, pp. 217-241.

43 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

44 JUSTRIBÓ, Candela – «Ciberdefensa...»; OLIVEIRA, Marcos Aurelio Guedes, et al. – *Guia de Defesa Cibernética da América do Sul*; GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano...»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

45 JUSTRIBÓ, Candela – «Ciberdefensa...».

46 VAN RAEMDONCK, Nathalie – *Cyber Diplomacy in Latin America*. UE Cyber Direct, Digital Dialogue, 26 de junho de 2020, pp. 4-37. Consultado em: 6 de agosto de 2023. Disponível em: https://eucyberdirect.eu/research/cyber-diplomacy-in-latin-america.

47 SFORZIN, Verónica Elena – «El rol de los organismos regionales: Celac, Mercosur y Alianza del Pacifico, frente a las Tecnologías de la Información y la Comunicación en el periodo del 2005 al 2015». Universidad Nacional de La Plata, Provincia de Buenos Aires, 2020. Tese de doutorado em Comunicação.

48 GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano...».

49 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

50 MERCOSUL – Agenda Digital. Consultado em: 6 de agosto de 2023. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/.

51 JUSTRIBÓ, Candela – «Ciberdefensa...»; GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano...»; GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

52 NEVES, Bárbara Carvalho; HONÓRIO, Karen – «Latin American regionalism under the new right». In *E-International Relations*. 27 de setembro de 2019, pp. 1-6. Disponível em: https://www.e-ir.info/pdf/80118; BRICEÑO-RUIZ, José – «Da crise da pós-hegemonia ao impacto da covid-19...»; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global...».

53 SOUZA, Tamires Aparecida Ferreira – «Cooperação em Defesa e a Região Sul-americana: O Papel do Conselho de Defesa Sul-Americano da UNASUL». Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015. Dissertação de mestrado em Estudos Estratégicos Internacionais; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global...».

54 JUSTRIBÓ, Candela – «Ciberdefensa...».

55 HERZ, Monica – «Cibersegurança na América Latina», p. 17.

56 ORGANIZAÇÃO DOS ESTADOS AMERICANOS – «Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética" Aprobada en la Cuarta Sesión Plenaria, celebrada el 8 de junio de 2004». Washington DC, Estados Unidos de América, 2004. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp; ORGANIZAÇÃO DOS ESTADOS AMERICANOS – Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio, 2023. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oascybercbms.org/es; ORGANIZAÇÃO DOS ESTADOS AMERICANOS – *Programa de Ciberseguridad*. 2023. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp.

57 NEVES, Bárbara Carvalho; HONÓRIO, Karen – «Latin American regionalism under the new right»; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global...».

58 GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas...».

59 TEIXEIRA JÚNIOR, Augusto Wagner Menezes – «Contribuições do Conselho de Defesa Sul-Americano para a Cooperação Militar»; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria; KERR OLIVEIRA, Lucas – «A cooperação em segurança e defesa na América do Sul...»; MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global...».

BIBLIOGRAFIA

AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria – «Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil». In *Revista Brasileira de Estudos de Defesa*. Vol. 7, N.º 2, julho-dezembro de 2020, pp. 103-131. DOI: https://doi.org/10.26792/rbed.v7n2.2020.75178.

AYRES PINTO, Danielle Jacon; MORAES, Isabela – «As mídias digitais como ferramentas de manipulação de processos eleitorais democráticos: uma análise do caso Brexit». In *Revista de Estudios Sociales*. Bogotá. N.º 74, outubro-dezembro de 2020, pp. 71-82. DOI: https://doi.org/10.7440/res74.2020.06.

BARRINHA, André; RENARD, Thomas – «Cyber-diplomacy: the making of an international society in the digital age». In *Global Affairs*. Vol. 3, N.º 4-5, 2017, pp. 353-364. DOI: https://doi.org/10.1080/23340460.2017.1414924.

BRADSHAW, Samantha; HOWARD, Philip N. – *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. University of Oxford, Computational Propaganda Research Project, working paper, report n.º 19, 2019.

BRICEÑO-RUIZ, José – «Da crise da pós-

-hegemonia ao impacto da covid-19: o impasse do regionalismo latino-americano». In *Revista Cadernos de Campo*. Araraquara. N.º 29, julho-dezembro de 2020, pp. 21-39. DOI: https://doi.org/10.47284/2359-2419.2020.29.2139.

CALDERARO, Andrea; CRAIG, Anthony J. S. – «Transnational governance of cybersecurity policy challenges and global inequalities in cyber capacity building». In *Third World Quarterly*. Vol. 41, N.º 6, 2020, pp. 917-938. DOI: https://doi.org/10.1080/01436597.2020.1729729.

CEBALLOS, Luis Dario; MAISONNAVE, Marcelo Andrés; LONDOÑO, Carlos Rafael Britto – «Soberanía tecnológica digital en Latinoamérica». In *Revista Propuestas para el Desarrollo*. México. Ano IV, N.º IV, outubro de 2020, pp. 151-167.

CHENOU, Jean-Marie; FUERTE, Juan Sebastián Rojas – «The difficult path to the insertion of the Global South in Internet governance». In *Internet Governance in the Global South: History, Theory, and Contemporary Debates*. São Paulo: NUPRI/USP, 2018, pp. 42-73.

COSTA, Hugo Bras Martins da; DUARTE, Rubens de Siqueira – «Sul Global versus Sul Geopolítico: um debate quanto à pertinência analítica dos conceitos». In *Austral: Brazilian Journal of Strategy and International Relation*. Porto Alegre. Vol. 12, N.º 24, 2023, pp. 13-35. DOI: https://doi.org/10.22456/2238-6912.132863.

CRIALES, José Pablo – «La inseguridad irrumpe en la campaña electoral argentina aupada por las noticias falsas en redes sociales». In *El País*. Buenos Aires, 11 de agosto de 2023. Consultado em: 12 de outubro de 2023. Disponível em: https://elpais.com/argentina/2023-08-11/la-inseguridad-irrumpe-en-la-campana-electoral-argentina-aupada-por-las-noticias-falsas-en-redes-sociales.html.

CURI JÚNIOR, Aribelco; ALFAYA, Natalia Maria Ventura da Silva – «O impacto das fake news nas eleições presidenciais de 2018 e 2022: prejuízos para a democracia e a sociedade». In *Revista do Instituto de Direito Constitucional e Cidadania*. Paraná. Vol. 8, N.º 1, janeiro-junho de 2023, pp. 1-11. DOI: https://doi.org/10.48159/revistadoidcc.v8n1.e079.

FERREIRA NETO, Walfredo Bento – «Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder». In *Revista das Ciências Militares, Coleção Meira Mattos*. Rio de Janeiro. Vol. 1, janeiro-abril de 2014, pp. 7-18.

FÓRUM ECONÔMICO MUNDIAL – *Global Risks Report 2024*. Genebra: Fórum Econômico Mundial, 2024. Consultado em: 28 de fevereiro de 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

FUCCILLE, Alexandre – «O Brasil e a América do Sul: (re)pensando a segurança e a defesa na região». In *Revista Brasileira de Estudos de Defesa*. Vol. 1, N.º 1, 2014. pp. 112-146.

GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares – «A geopolítica do espaço cibernético sul-americano: (in) conformação de políticas de segurança e defesa cibernética?». In *Austral: Revista Brasileira de Estratégia e Relações Internacionais*. Porto Alegre. Vol. 7, N.º 14, julho-dezembro de 2018, pp. 217-241. DOI: https://doi.org/10.22456/2238-6912.87994.

GRASSI, Jéssica Maria – «A Construção de Capacidades Cibernéticas e os Processos Cooperativos no Contexto Geopolítico Sul-Americano». Universidade Federal de Santa Catarina, Florianópolis, Brasil, 2023. Tese de doutorado em Relações Internacionais.

GUTIÉRREZ-COBA, Liliana; RODRÍGUEZ-PÉREZ, Carlos – «Estrategias de posverdad y desinformación en las elecciones presidenciales colombianas 2022». In *Revista de Comunicación*. Vol. 22, N.º 2, 2023, pp. 225-242. DOI: https://doi.org/10.26441/RC22.2-2023-3270.

HANSON, Fergus; O'CONNOR, Sara; WALKER, Mali; COURTOIS, Luke – *Hacking Democracies: Cataloguing Cyber-enabled Attacks on Elections*. Australian Strategic Policy Institute, policy brief, report n.º 16, 2019, pp. 3-30.

HERZ, Monica – «Cibersegurança na América Latina». In *Conferência de Segurança Internacional do Forte de Copacabana – A Quarta Revolução Industrial: Impactos na Segurança Internacional e a Reformulação da Ordem Global*. Fundação Konrad Adenauer; Centro Brasileiro de Relações Internacionais. Coleção de Policy Papers, 2019, pp. 9-19.

JUSTRIBÓ, Candela – «Ciberdefensa: una visión desde la UNASUR». In *VII Congreso del Instituto de Relaciones Internacionales*. La Plata, 2014, pp. 1-24.

LIBICKI, Martin – *Cyberdeterrence and Cyberwar*. Pittsburgh: RAND Corporation, 2009.

LIFF, Adam P. – «Cyberwar: a new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war». In *Journal of Strategic Studies*. Vol. 35, N.º 3, 2012, pp. 401-428. DOI: https://doi.org/10.1080/01402390.2012.663252.

MERCOSUL – Agenda Digital. Consultado em: 6 de agosto de 2023. Disponível em: https://www.mercosur.int/pt-br/temas/agenda-digital/.

MIKSER, Sven – «La necesidad de una respuesta armonizada a las amenazas de ciberseguridad: el camino a seguir». In *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe*. Observatorio de la Ciberseguridad en América Latina y el Caribe, Report Ciberseguridad 2020, pp. 34-37.

MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria – «Impactos da disputa geopolítica entre as grandes potências no Sul Global: desestabilização e (des)integração sul-americana». In *Conjuntura Austral*. Porto Alegre. Vol. 12, N.º 61, 2022, pp. 33-46. DOI: https://doi.org/10.22456/2178-8839.113748.

MORAIS DA SILVA, Ana Karolina; GRASSI, Jéssica Maria; KERR OLIVEIRA, Lucas – «A cooperação em segurança e defesa na América do Sul a partir de 2016: desafios e perspectivas». In *Revista Brasileira de Estudos Estratégicos*. Niterói. Vol. 16, N.º 26, 2021, pp. 25-49. DOI: https://doi.org/10.29327/230731.13.26-2.

MULLER, Lilly Pijnenburg – *Cyber Security Capacity Building in Developing Countries*. Norwegian Institute for International Affairs (NUPI), Policy brief n.º 15, 2015, pp. 1-5.

NEVES, Bárbara Carvalho; HONÓRIO, Karen – «Latin American regionalism under the new right». In *E-International Relations*. 27 de setembro de 2019. Disponível em: https://www.e-ir.info/pdf/80118.

NYE JR, Joseph S. – *The Future of Power*. Nova Iorque: Public Affairs, 2011.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – «Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética" Aprobada en la Cuarta Sesión Plenaria, celebrada el 8 de junio de 2004». Washington DC, Estados Unidos de América, 2004. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio, 2023. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oascybercbms.org/es.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – *Programa de Ciberseguridad*. 2023. Consultado em: 6 de agosto de 2023. Disponível em: https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp.

OLIVEIRA, Marcos Aurélio Guedes; PAGLIARI, Graciela de Conti; MARQUES, Adriana A.; PORTELA, Lucas Soares; FERREIRA NETO, Walfredo Bento – *Guia de Defesa Cibernética da América do Sul*. Recife: Ed. UFPE, 2017.

OLIVEIRA, Raquel Jorge de; IZYCKI, Eduardo – «Propaganda computacional na prática: os casos de Estados Unidos, França, Colômbia e Venezuela». In *XI Encontro Nacional Da Associação Brasileira de Estudos de Defesa* [online]. 2021, pp. 1-18.

PAGLIARI, Graciela de Conti – «Conselho de Defesa Sul-Americano e a adoção de medidas de fortalecimento da confiança». In *Carta Internacional*. Belo Horizonte. Vol. 10, N.º 3, 2015, pp. 23-40. DOI: https://doi.org/10.21530/ci.v10n3.2015.307.

PAGLIARI, Graciela de Conti; AYRES PINTO, Danielle Jacon; VIGGIANO, Juliana – «Mobilização nacional, ameaças ciberné-

ticas e redes de interação num modelo de tríplice hélice estratégica: um estudo prospectivo». In *Defesa Cibernética e Mobilização Nacional*. Recife: Ed. UFPE, 2020, pp. 153-174.

PAWLAK, Patryk – «Capacity building in cyberspace as an instrument of foreign policy». In *Global Policy*. Vol. 7, N.º 1, 2016, pp. 83-92. DOI: https://doi.org/10.1111/1758-5899.12298.

PAWLAK, Patryk; BARMPALIOU, Panagiota-Nayia – «Politics of cybersecurity capacity building: conundrum and opportunity». In *Journal of Cyber Policy*. Vol. 2, N.º 1, 2017, pp. 123-144. DOI: https://doi.org/10.1080/23738871.2017.1294610.

PORTELA, Lucas Soares – «Movimentos Centrais e Subjacentes no Espaço Cibernético do Século XXI». Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2016. Dissertação de mestrado em Ciências Militares.

RAULS, Leonie – «How Latin American governments are fighting fake news». In *Americas Quartely*. 19 de outubro de 2021. Consultado em: 12 de outubro de 2023. Disponível em: https://americasquarterly.org/article/how-latin-american-governments-are-fighting-fake-news/.

RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies*. Vol. 35, N.º 1, 2012, pp. 5-32. DOI: https://doi.org/10.1080/01402390.2011.608939.

SCHIA, Niels Nagelhus – «The cyber frontier and digital pitfalls in the Global South». In *Third World Quarterly*. Vol. 39, N.º 5, 2018, pp. 821-837. DOI: https://doi.org/10.1080/01436597.2017.1408403.

SFORZIN, Verónica Elena – «El rol de los organismos regionales: Celac, Mercosur y Alianza del Pacifico, frente a las Tecnologías de la Información y la Comunicación en el periodo del 2005 al 2015». Universidad Nacional de La Plata, Provincia de Buenos Aires, 2020. Tese de doutorado em Comunicação.

SOUZA, Tamires Aparecida Ferreira – «Cooperação em Defesa e a Região Sul-americana: O Papel do Conselho de Defesa Sul-Americano da UNASUL». Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015. Dissertação de mestrado em Estudos Estratégicos Internacionais.

STONE, John – «Cyber war will take place!». In *Journal of Strategic Studies*. Vol. 36, N.º 1, 2013, pp. 101-108. DOI: https://doi.org/10.1080/01402390.2012.730485.

TEIXEIRA JÚNIOR, Augusto Wagner Menezes – «Contribuições do Conselho de Defesa Sul-Americano para a Cooperação Militar». In *Revista Política Hoje*. Vol. 24, N.º 1, 2015, pp. 57-70.

VAN RAEMDONCK, Nathalie – *Cyber Diplomacy in Latin America*. UE Cyber Direct, Digital Dialogue, 26 de junho de 2020, pp. 4-37. Consultado em: 6 de agosto de 2023. Disponível em: https://eucyberdirect.eu/research/cyber-diplomacy-in-latin-america.

WIGELL, Mikael – «Democratic deterrence: ¨how to dissuade hybrid interference». In *Washington Quarterly*. Vol. 44, N.º 1, 2021, pp. 49-67. DOI: https://doi.org/10.1080/0163660X.2021.1893027.

A cibernética na grande estratégia

Um estudo comparado de Reino Unido, França e Portugal[1]

Natália Diniz Schwether | *Marcos Aurélio Guedes de Oliveira*

INTRODUÇÃO

O presente artigo pretende, por meio da análise comparada de três casos e dos modelos adotados por cada um deles, contribuir para o esforço mundial de fortalecimento do espaço cibernético e para a formulação de políticas públicas em matéria de segurança e defesa cibernética, à medida que reconhece ser fundamental conhecer, apresentar e contrapor as iniciativas de diferentes países para o ambiente cibernético.

Nesse sentido, o objetivo geral do artigo é entender como Reino Unido, França e Portugal têm se preparado para a guerra do futuro, com foco nas ações adotadas para o novo domínio do ciberespaço. Os três casos da análise figuram entre as oito nações mais seguras no espaço cibernético, na Europa, sendo o Reino Unido o país europeu com maior comprometimento com a sua segurança cibernética[2].

Mais especificamente, objetiva: compreender teoricamente os conceitos de grande estratégia e poder cibernético, analisar as diferentes propostas dos três países e comparar os achados. Para atingir os objetivos foram escrutinadas as estratégias nacionais, as diretrizes e as doutrinas para o ciberespaço, bem como elencadas as instituições correspondentes, com base nos documentos emitidos pelos Estados e suas forças armadas.

Acresce-se a isso, a criação de um quadro comparativo, seguido de um descritivo de cada categoria analisada – grande estratégia, poder cibernético, instituições, inovação e parcerias –, apontando as semelhanças e as diferenças

RESUMO

O presente artigo elenca três Estados – Reino Unido, França e Portugal – entre os oito mais seguros no ambiente cibernético, com o intuito de responder ao seguinte questionamento: como eles têm se organizado para conter as ameaças advindas do ciberespaço?, e quais as semelhanças e as diferenças entre as estratégias adotadas? Para tanto, cinco categorias de análise guiam uma comparação sistemática e contextualizada, fundamentada, especialmente, em fontes primárias e documentos oficiais. De forma que, ao final, é possível depreender como os três países enfrentam o que hoje se considera uma das ameaças prioritárias às economias e à segurança nacional, além das estruturas criadas em cada um deles e dos setores e atores envolvidos na execução de suas estratégias.

Palavras-chave: cibernética, grande estratégia, poder, análise comparada.

ABSTRACT

Cybernetics in grand strategy: a comparative study of the United Kingdom, France, and Portugal

→

 https://doi.org/10.23906/ri2024.82a03

This article lists three states – the United Kingdom, France, and Portugal – among the eight most secure in the cyber environment, with the aim of answering the following question: How have they organized themselves to contain threats arising from cyberspace? And what are the similarities and differences between the strategies adopted? To this end, five categories of analysis guide a systematic and contextualized comparison, based mainly on primary sources and official documents. In the end, it is possible to understand how the three countries face what is today considered one of the priority threats to economies and national security, in addition to the structures created in each of them and the sectors and actors involved in the implementation of their strategies.

Keywords: cybernetics, grand strategy, power, comparative analysis.

entre os modelos. De forma que, ao final, são discutidos os achados, sendo possível depreender como o Reino Unido, a França e Portugal têm enfrentado o que hoje se considera uma das ameaças prioritárias às economias e à segurança nacional.

GRANDE ESTRATÉGIA E PODER CIBERNÉTICO

Os conceitos de grande estratégia e poder cibernético são polissêmicos; assim, desde logo, é fundamental apresentarmos o significado que iremos atribuir a cada um deles, bem como estabelecermos o elo que os une. Embora não haja um consenso, a noção de grande estratégia é pertinente devido a uma de suas características-chave, a qual compreende um planejamento de longo prazo.

O uso recorrente do termo e a sua popularidade aumentaram expressivamente com o fim da Guerra Fria, contudo, em sua maioria, ele aparecia em estudos que tinham como base a realidade estadunidense e estavam voltados, sobretudo, para a área da economia de defesa[3].

Antes disso, no entanto, no final da década de 1960, Liddell-Hart foi responsável por apresentar uma das definições mais referenciadas, desde então, em seu livro *Estratégia*. Para o autor, «o papel da Grande Estratégia – ou alta estratégia – é coordenar e direcionar todos os recursos da nação, ou de um grupo de nações, em direção à realização do objetivo político da guerra – o fim definido pela política fundamental»[4].

Soma-se a essa definição a contribuição de Paul Kennedy: para o estudioso, a grande estratégia está preocupada tanto com a paz quanto com a guerra, ou seja, trata-se de um continuum de ações e da integração de diversas políticas por décadas, em que cabe aos agentes (líderes políticos) «unir todos os elementos (militares e não militares), para a preservação e o desenvolvimento dos interesses da nação»[5].

Em ambas as definições fica evidente, portanto, que a grande estratégia é um plano proposital de longo prazo, semelhante a uma estratégia militar, com o diferencial de que para sua elaboração são levados em consideração todos os recursos do Estado[6]. Sob esse mesmo prisma, Murray[7] argumenta a respeito da importância do entrelaçamento de diferentes setores e reconhece que a política deve, na maioria das vezes, impulsionar a necessidade militar. Walt[8], por sua vez, reforça que o principal objetivo da grande estratégia é o de produzir segurança.

Para a estudiosa Silove há, ainda, outras duas frequentes aplicações do termo «grande estratégia», uma delas distingue os grandes princípios (orientações e coordenadas conceituais) e a outra os grandes comportamentos (padrões de comportamento, práticas e ideias)[9].

Nessa última interpretação estariam, por exemplo, Hal Brands[10] – o qual afirma que a grande estratégia se trata de ideias ou uma lógica para se planejar a longo prazo, a qual vincula interesses de um país com suas interações com o mundo –, além de Brooks e Wohlforth[11] – para quem a grande estratégia corresponde ao padrão de escolhas adotado ao longo do tempo.

Na interpretação desses pensadores, a grande estratégia advém de uma série de decisões, entre elas, também aquelas tomadas no âmbito externo. Para Thomas J. Christiensen, a grande estratégia pode ser entendida «como um pacote completo de políticas domésticas e internacionais desenhadas para aumentar o poder e a segurança nacional»[12]. De maneira análoga, Milani e Nery[13] concordam que uma grande estratégia pressupõe um alinhamento em termos de política externa, objetivos de defesa, cooperação internacional e parcerias com o mercado doméstico.

Em geral, as definições apresentam importantes pontos em comum. O primeiro deles diz respeito à origem do termo; tendo em vista o conceito de grande estratégia ser oriundo do conceito de estratégia, dois elementos são centrais: os fins e os meios. Uma grande estratégia faz parte, por conseguinte, de um processo decisório e de planejamento[14].

No entanto, diferentemente da estratégia, a grande estratégia possui, necessariamente, uma natureza de longo prazo, ou seja, é um caminho que orienta do presente para o futuro, sejam décadas ou séculos. Ao mesmo tempo que ela é holística, pois envolve todos os recursos de uma nação e todas as facetas do poder disponíveis para a consecução dos objetivos nacionais[15].

Destarte, em um contexto de ampla disponibilidade de informação e tecnologia, em que o ambiente virtual armazena inúmeras informações sensíveis, o poder cibernético – o uso estratégico do ciberespaço[16] – se tornou um meio para garantir a soberania, a segurança, a defesa, a resiliência e o desenvolvimento nacional[17].

Assim dizendo, o poder cibernético é uma prioridade transversal na estratégia dos Estados e uma componente, cada vez mais, importante do poder nacional, pelo que os países competem para adquirir e usar essa capacidade[18].

Frisa-se, no entanto, que o poder baseado em recursos de informação não é novo, a diferença reside no ambiente. O poder cibernético depende dos atributos que caracterizam o domínio do ciberespaço[19]. Na esteira desse pensamento, vale ressaltar a diferença entre ciberespaço e poder cibernético. Para Sheldon[20], o ciberespaço é o domínio em que ocorrem as operações cibernéticas. Já o poder cibernético é a soma dos efeitos estratégicos gerados pelas operações cibernéticas no ciberespaço.

Na concepção de Nye[21], o poder cibernético é a capacidade de obter resultados preferenciais no ciberespaço ou em outros domínios, ao criar vantagens ou influenciar eventos através do uso de recursos do domínio cibernético.

Assim sendo, o poder cibernético tem um propósito estratégico para alcançar fins

O PODER CIBERNÉTICO TEM UM PROPÓSITO ESTRATÉGICO PARA ALCANÇAR FINS POLÍTICOS.

políticos. Este propósito estratégico diz respeito a capacidade, na paz e na guerra, de manipular as percepções e, ao mesmo tempo, degradar a capacidade de um adversário de compreender o ambiente. As operações cibernéticas, portanto, não servem a seus próprios fins, mas aos fins da política: «A estratégia é a ponte entre a política e a exploração do instrumento cibernético»[22].

Nota-se, pois, que o ciberespaço em todos os seus aspectos – tecnológicos, psicológicos, políticos, militares – está sob a autoridade da estratégia[23]. De maneira que, pensar o ciberespaço, as novas possibilidades advindas desse espaço e a sua aplicação é parte fundamental da tarefa dos formuladores de políticas[24].

Frente a isso, diversos países têm percorrido um processo de atualização das suas grandes estratégias e inclusão de novos conceitos para enfrentar as complexidades do ciberespaço. «As operações cibernéticas aparecem repetidamente no sofisticado manual do Estado moderno.»[25]

Igualmente, o ciberespaço, sem fronteiras e transacional, se tornou um domínio[26] crucial, também, para o planejamento militar[27]. Os planejadores militares têm procurado incorporar a capacidade cibernética nos níveis tático, operacional e estratégico da guerra, o que contribui para que as operações cibernéticas tenham um papel cada vez mais decisivo[28].

De maneira estratégica, o emprego militar da capacidade cibernética é capaz de produzir importantes efeitos, seja devido a maior precisão e rapidez dos ataques, a viabilidade de extração e coleta de dados ou ao aperfeiçoar a comunicação e a tomada de decisão[29]. Ao utilizar a capacidade cibernética «o tomador de decisão aumenta a probabilidade de influenciar outrem e, por conseguinte, aumenta sua chance de êxito na consecução do objetivo»[30].

Outrossim, o emprego da capacidade cibernética na guerra reúne características que a tornam, particularmente, atraente aos Estados, a exemplo dos desafios de atribuição, da natureza multiuso das tecnologias que a ela estão associadas, da imprevisibilidade dos alvos, do potencial dos danos colaterais ou não intencionais e da possibilidade de ser combinada com as armas convencionais[31].

O dano de um ataque cibernético, em contraste a um agravo físico, é, em geral, extremamente difícil de se mensurar e capaz de ocasionar efeitos tanto diretos e imediatos quanto tardios e indiretos[32]. Em contrapartida, é inegável que os ataques são resultado da exposição e de possíveis falhas nos sistemas alvo, as quais são exploradas oportunamente por agentes maliciosos[33].

Logo, os esforços estatais estão concentrados em eliminar vulnerabilidades e na redução da suscetibilidade de ataques no ciberespaço; há, ainda, um crescente número de Estados que empregam o poder cibernético de modo ofensivo na consecução de seus interesses e objetivos nacionais[34].

Assim sendo, a próxima seção irá se concentrar na apresentação dos três casos eleitos para essa análise, observando em suas grandes estratégias qual o espaço dedicado ao poder cibernético, além de explicitar como os países têm se organizado em prol da segurança e resiliência estatal.

ANÁLISE COMPARADA DOS CASOS

A comparação sistemática e contextualizada de poucos casos foi a técnica empregada para responder às perguntas: como o Reino Unido, a França e Portugal têm se organizado para conter as ameaças advindas do ciberespaço?, e quais as semelhanças e as diferenças entre as estratégias adotadas?

Lipjhart[35] define a comparação como um método básico das ciências sociais, de grande utilidade para estabelecer proposições gerais empíricas e para descobrir o relacionamento empírico entre variáveis. Para orientar a análise, foram aqui adotadas cinco categorias passíveis de comparação. Além disso, para cada categoria, mais abstrata, foram eleitas algumas unidades específicas, de forma a permitir observar os mesmos itens nos três distintos casos. As categorias e unidades estão dispostas no quadro 1:

Quadro 1 > Categorias da análise

Categorias	Unidades de comparação
Grande estratégia	Documentos do governo nacional
Poder cibernético	Documentos da defesa nacional (Ministério/ Forças Armadas)
Instituições	Civis e militares Segurança / Defesa cibernética
Inovação	Pesquisa e desenvolvimento
Parcerias	Cooperação internacional Exercícios / Alianças

Fonte: Elaborado pelos autores, 2023.

A definição cuidadosa do que será analisado em cada categoria é o que dá sustentação e credibilidade para a presente análise. Nesse sentido, na primeira categoria – «grande estratégia» – reúnem-se as diretrizes do planejamento estratégico, as perspectivas futuras e os planos para se atingirem os interesses de cada um dos Estados.

Diante dessa apreensão do grande quadro, passa-se então à categoria «poder cibernético», na qual o uso estratégico do ciberespaço, seja para segurança ou defesa nacional, recebe enfoque. São mapeados os documentos orientadores do setor e os objetivos traçados em cada um deles, com atenção aos níveis tático, operacional e estratégico da guerra.

A seguir, busca-se de forma mais minuciosa, na categoria «instituições», entender como foram distribuídas as atividades e quais as estruturas criadas e os atores, civis e militares, envolvidos. Mais duas categorias completam a análise: «inovação», a qual lança um olhar sobre iniciativas no campo da pesquisa e do desenvolvimento, além de propostas singulares para o campo «parcerias», em que são observados os arranjos, as alianças e os exercícios realizados na área, principalmente, no âmbito externo.

O principal insumo da pesquisa são fontes primárias – documentos oficiais emitidos pelos governos e órgãos de defesa. No caso britânico destaca-se a «revisão integrada de segurança», «defesa», «desenvolvimento e política externa» e a «estratégia nacional cibernética». No que diz respeito à França, a *Revue Stratégique de Defense et de Sécurité*, de 2017, e a *Revue Nationale Stratégique*, de 2022, apontam as grandes tendências e panoramas futuros e estão em sintonia com o principal documento para o setor cibernético, a *Revue Stratégique de Cyberdéfense.*

Já para Portugal, o Conceito Estratégico de Defesa Nacional, de 2013, permanece sendo o principal instrumento da estratégia nacional para defesa e segurança. No tocante ao ciberespaço, destaca-se a publicação, em 2015, da *Estratégia Nacional de Segurança do Ciberespaço*, tendo sua segunda versão sido apresentada em 2019.

Uma vez certos da técnica empregada para análise e de suas fontes, apresentamos, a seguir, um conjunto de informações relevantes agrupadas nas categorias mencionadas.

GRANDE ESTRATÉGIA

A revisão integrada de segurança, defesa, desenvolvimento e política externa, *Global Britain in a Competitive Age*, publicada pelo Reino Unido, em 2021, reúne as grandes tendências do ambiente internacional e de segurança nacional. Em seu cerne está o compromisso com a segurança e com a resiliência e a proteção da população britânica, tanto no âmbito doméstico quanto internacional. Nesse sentido, sólidas estruturas na luta contraterrorista, de inteligência e de cibersegurança são apontadas como fundamentais[36].

A revisão define quatro principais objetivos: apoiar a ciência e a tecnologia, fortalecendo a posição do Reino Unido como poder cibernético; moldar a ordem internacional, reforçando e estabelecendo novos pilares, a exemplo do ciberespaço; robustecer a segurança e a defesa para enfrentar os desafios do mundo físico e virtual; incrementar a resiliência para responder e se recuperar de ataques[37].

O CIBERESPAÇO SERÁ UM DOMÍNIO CADA VEZ MAIS CONTESTADO, UTILIZADO TANTO POR ESTADOS QUANTO POR ATORES NÃO ESTATAIS, E, CONSEQUENTEMENTE, DETER PODER CIBERNÉTICO TERÁ UMA IMPORTÂNCIA CRESCENTE.

Outrossim, são listadas algumas adaptações necessárias para lidar com os desafios. Menciona-se, entre elas, a preocupação em se tornar um poder cibernético democrático e responsivo. De acordo com o documento, o ciberespaço será um domínio cada vez mais contestado, utilizado tanto por Estados quanto por atores não estatais, e, consequentemente, deter poder cibernético terá uma importância crescente[38].

Em vista disso, a revisão propõe adotar uma estratégia mais abrangente e utilizar o domínio cibernético de modo mais integrado e criativo, retirando o foco da segurança cibernética e considerando toda a gama de capacidades – dentre elas as ofensivas – na detecção, interrupção e dissuasão de possíveis ameaças. Ao mesmo tempo, pretende reunir esforços para a obtenção de tecnologias cibernéticas críticas[39].

Três importantes conclusões da revisão são: o poder cibernético é um fator cada vez mais importante na consecução dos objetivos nacionais, deter poder cibernético exige uma visão abrangente e uma estratégia integrada e, mais do que isso, toda a sociedade deve atuar em conjunto para o sucesso das ações no ciberespaço.

A França, por sua vez, publicou, em 2017, a *Revue Stratégique de Defense et de Sécurité Nationale*, na qual destacou o desenvolvimento tecnológico como responsável por impor novos desafios aos sistemas tradicionais. Em relação ao ciberespaço reforçou que «certos ataques podem ser considerados como uma agressão armada, devido à sua escala e gravidade»[40].

O documento estratégico *Actualisation Stratégique*, de 2021, deu destaque às ameaças híbridas, à ação deliberada de manipulação da informação e à vulnerabilidade dos dados: «O ciber e o espaço são agora campos assumidos de rivalidade estratégica»[41]. Com isso, a adaptação da estratégia teve como foco as áreas de cibernética, espacial e inteligência artificial e confirmou a aposta francesa em um processo de modernização militar, com vista a uma força armada completa, ágil e eficiente, e na superioridade estratégica e tecnológica do país[42].

Mais recentemente, em 2022, o país apresentou a *Revue Nationale Stratégique*; nela, a sofisticação da capacidade cibernética ofensiva foi tida como sem precedentes, além de um desafio estratégico a ser abordado. Definiu, ainda, que o esforço deveria estar concentrado na melhoria da resiliência cibernética: «Fortalecer o nível de cibersegurança é essencial para preparar o país para mais ameaças»[43].

No caso português, o Conceito Estratégico de Defesa Nacional é o principal instrumento de apresentação da estratégia nacional para a defesa e a segurança. O documento, aprovado em 2013, recomendou às Forças Armadas uma atuação conjunta, afora propor uma reorganização e simplificação das estruturas, com vista a uma maior eficiência, agilidade, modularidade e flexibilidade. No que tange o espaço cibernético, traçou objetivos como: definir uma estratégia de cibersegurança, criar órgãos técnicos, sensibilizar usuários e aprimorar a capacidade de ciberdefesa nacional[44].

PODER CIBERNÉTICO

A Estratégia Nacional Cibernética britânica, lançada em 2021, traz em seu cerne o conceito de poder cibernético aliado à pretensão de que, em 2030, o Reino Unido permaneça como um dos principais poderes cibernéticos do mundo. Para isso, cinco pilares orientam tal ambição: aprofundar a parceria governo, academia e indústria; construir um ambiente digital resiliente e próspero; assumir a dianteira tecnológica; liderar e influenciar a ordem internacional; detectar, interromper e dissuadir adversários[45].

No que tange a garantia do desenvolvimento do pleno potencial como poder cibernético, prevê um incremento contínuo da Força Cibernética Nacional (NCF, na sigla inglesa) e esforços intergovernamentais no enfrentamento das ameaças. Estabelece três principais objetivos: aumentar o investimento em agências de inteligência e na capacidade

de fiscalização e enfrentamento ao crime cibernético; aprimorar a coordenação na detecção das ameaças, com acesso conjunto às bases de dados e uma divulgação célere dos relatórios: expandir a rede de defensores cibernéticos e as pesquisas na área[46].
Além disso, vislumbra atualizar a legislação, maximizar as parcerias entre os órgãos dedicados ao ciberespaço, as comunidades de inteligência e diplomáticas e capacitar os oficiais para conduzir operações cibernéticas ofensivas legais e proporcionais[47].
A França, por sua vez, publicou, em 2018, a *Revue Stratégique de Cyberdéfense* – o Livro Branco da Defesa Cibernética francesa. O primeiro objetivo traçado na revisão foi encrudescer os dispositivos disponíveis de proteção cibernética e reforçar a resiliência das redes estatais e de operadores de serviços essenciais[48]. Já em âmbito internacional, buscar a regulamentação do ciberespaço, a prevenção de ataques e a capacitação para o gerenciamento de crises[49].
Em 2019, a França assumiu uma doutrina clara de defesa cibernética, organizada em dois polos, de um lado, a «luta informática ofensiva» e, de outro, a «luta informática defensiva». A luta informática ofensiva diz respeito ao conjunto das ações realizadas no ciberespaço que produzem efeitos contra um sistema antagônico. Por seu turno, as ações da «luta informática defensiva» são, em síntese, a antecipação, a detecção e a reação, bem como contribui com as missões de prevenção, proteção e atribuição[50].
Dois anos mais tarde, em 2021, foi acrescido ao quadro doutrinário dedicado ao ciberespaço o documento *Doctrine Militaire de Lutte Informatique d'Influence*. A doutrina advém da importância crescente das mídias sociais no cotidiano da população e a noção de que o ambiente informacional onipresente afeta, também, as operações militares e os processos de tomada de decisão, seja por meio da manipulação das informações seja pela propagação de notícias falsas[51].
Mormente ao ciberespaço, Portugal publicou, em 2015, a «Estratégia Nacional de Segurança do Ciberespaço» (ENSC), na qual tratou a questão da segurança das redes e dos sistemas de informação e a utilização livre, segura e eficiente do ciberespaço. O documento situou a importância de se produzir uma revisão periódica, em um prazo máximo de três anos, assim como de proceder a uma verificação anual dos objetivos estratégicos e das linhas de ação[52].
Desta feita, em 2019, foi aprovada a segunda ENSC assente em três objetivos estratégicos: maximizar a resiliência, promover a inovação e gerar e garantir recursos. No que tange à ciberdefesa propôs reforçar a resiliência das Forças Armadas e utilizar todos os meios para responder aos ciberataques, incluindo a capacidade ofensiva[53].
Na esteira da ENSC e diante da constatação da premência de densificar conceitos e de, devidamente, articular as estruturas dedicadas ao ciberespaço, foi publicada, em 2022, a Estratégia Nacional de Ciberdefesa, a qual reafirmou o ciberespaço como um domínio das operações militares defensivas e ofensivas, no qual deverão ser assegurados a defesa e os interesses nacionais. Nesse sentido, estabeleceu o ciberespaço como um elemento integrante do processo de planejamento, em uma lógica multidomínio[54].

Para mais, foram definidos quatro objetivos estratégicos: consolidar a capacidade de ciberdefesa, maximizar a resiliência e a coesão da ação nacional, promover a pesquisa, o desenvolvimento e a inovação e garantir recursos qualificados. E seis eixos orientadores: utilizar o ciberespaço como um domínio de operações; reforçar a capacidade de ciberdefesa nacional; criar a escola de ciberdefesa; intensificar a cooperação nacional e internacional; promover a pesquisa, o desenvolvimento e a inovação, incentivando o desenvolvimento de soluções de uso dual; assegurar as capacidades necessárias à ciberdefesa[55].

INSTITUIÇÕES

No que tange às instituições dedicadas ao ciberespaço sobressai, no Reino Unido, a criação do Centro Nacional de Segurança Cibernética e da NCF. O Centro, formalmente constituído em 2016, é responsável pelas infraestruturas críticas nacionais, sua atribuição, principal, é auxiliar na contenção e investigação dos crimes digitais. Por sua vez, a NCF, operacional desde 2020, foi projetada, especialmente, para conduzir operações ofensivas.

A NCF reúne o serviço de inteligência britânico, o Ministério da Defesa, o Serviço de Inteligência Secreta e o Laboratório de Ciência e Tecnologia de Defesa sob um comando unificado. As diferentes expertises atuam em conjunto, também, com os meios diplomático, econômico e político. A NCF atua em três grandes frentes: combate a ameaças terroristas, criminosas e estatais; combate a ameaças à confidencialidade, integridade e disponibilidade de dados e ao uso efetivo dos sistemas; apoio às operações de defesa e política externa[56].

Em se tratando das instituições dedicadas ao ciberespaço, no caso francês, é importante recordar o particularismo do seu modelo de resposta aos incidentes digitais, o qual preza pela separação entre as capacidades defensivas e as ofensivas.

EM SE TRATANDO DAS INSTITUIÇÕES DEDICADAS AO CIBERESPAÇO, NO CASO FRANCÊS, É IMPORTANTE RECORDAR O PARTICULARISMO DO SEU MODELO DE RESPOSTA AOS INCIDENTES DIGITAIS, O QUAL PREZA PELA SEPARAÇÃO ENTRE AS CAPACIDADES DEFENSIVAS E AS OFENSIVAS.

A estratégia ofensiva francesa é prerrogativa da Presidência através do Conselho Nacional de Defesa e Segurança, responsável pela produção de diretivas, as quais são implementadas pelo Comitê de Gestão da Defesa Cibernética, alocando os recursos necessários. É incumbência da Direção-Geral de Controle de Armamento-Informação a concepção das armas cibernéticas, seja para os serviços de inteligência ou para o Comando de Defesa Cibernética (COMCYBER)[57].

Constituído em 2017, o COMCYBER está diretamente subordinado ao chefe do Estado-Maior das Forças Armadas e consiste em um ator fundamental para a organização e a padronização da ação ofensiva, bem como para o fortalecimento de uma postura proativa do país na detecção dos ataques e compreensão das ameaças[58].

A estratégia defensiva é prerrogativa do primeiro-ministro através do Comité Diretor de Cibersegurança presidido pela Agência Nacional de Segurança de Sistemas de Informação (ANSSI). A ANSSI é a autoridade nacional responsável pela segurança dos sistemas de informação, com poder regulador, para definir regras, de certificação e qualificação de produtos e serviços e de imposição de medidas nos casos de condutas criminosas.

Ao chefe-geral da ANSSI é confiada a responsabilidade de conduzir as operações de proteção e garantir a segurança nacional em caso de um ciberataque. Por sua parte, o chefe das Forças Armadas fica encarregado pelas ações militares e de defesa nacional. Em Portugal, a Lei n.º 19/2022 alterou a estrutura, até então, destinada à ciberdefesa. Com a sua aprovação o Estado-Maior-General das Forças Armadas (EMGFA) teve sua missão ampliada, contemplando, desde então, a ciberdefesa. De maneira que foram, prontamente, criadas duas estruturas: o Centro de Comunicações e Informação, Ciberespaço e Espaço (CCICE), na direta dependência do chefe do EMGFA e o Comando de Operações de Ciberdefesa (COCiber).

EM PORTUGAL, A LEI N.º 19/2022 ALTEROU A ESTRUTURA, ATÉ ENTÃO, DESTINADA À CIBERDEFESA. COM A SUA APROVAÇÃO O ESTADO-MAIOR-GENERAL DAS FORÇAS ARMADAS (EMGFA) TEVE SUA MISSÃO AMPLIADA, CONTEMPLANDO, DESDE ENTÃO, A CIBERDEFESA.

O CCICE tem como missão habilitar a capacidade de comando e controle conjunto das Forças Armadas, além de assegurar o exercício do comando de operações militares no e através do ciberespaço. Compete ao CCICE planejar, coordenar e executar as medidas de segurança para a proteção e resiliência da infraestrutura tecnológica conjunta; propor e conduzir operações militares no e através do ciberespaço; participar e organizar exercícios conjuntos e combinados de ciberdefesa; disponibilizar e coordenar a capacidade de ciberdefesa.

O COCiber é responsável pelo planejamento, direção, controle e execução de operações no e através do ciberespaço. Sua estrutura compreende a Força de Operações de Ciberdefesa e pode ser reforçada por outras unidades das Forças. Compete ao COCiber estabelecer as ligações com as agências internacionais do setor.

Por último, o Centro Nacional de Cibersegurança, criado em 2014[59], é a autoridade nacional e coordenador operacional em matéria de cibersegurança e reação a ciberincidentes. Tem como missão contribuir para um ciberespaço seguro, confiável e livre, para isso desenvolvendo atividades dirigidas à população e às organizações.

INOVAÇÃO

Uma das iniciativas mais inovadoras do Reino Unido trata-se do plano Active Cyber Defence, o qual propõe enfrentar, em parceria com a indústria, de maneira relativamente automatizada, uma porção significativa dos ataques cibernéticos, reduzindo os danos e fornecendo ferramentas de proteção.

Novas regulamentações, a exemplo da UK General Data Protection Regulation, também impactaram de forma positiva a segurança cibernética britânica. Assim como estratégias para aproximar o cidadão e as instituições de órgãos capacitados para fornecer apoio e orientações, entre elas a rede Cyber Protect, responsável por ofertar aconselhamento cibernético para pequenas e médias empresas.

No que tange à inovação, a França conta com o Cyber Campus, um ambiente que reúne os principais atores nacionais e internacionais da área, com o intuito de aproximá-los e promover parcerias, além de um ecossistema de defesa cibernética na cidade de Rennes, onde estão abrigados o COMCYBER, laboratórios, estabelecimentos de ensino superior e multinacionais[60].

Outra iniciativa inovadora do Ministério da Defesa francês, em colaboração com a gendarmeria francesa, é a Rede de Defesa Cibernética da Reserva Cidadã – um contingente da reserva especializado, composto por voluntários com notória expertise e interesse. Esta rede é, acima de tudo, um importante vetor de ligação entre a sociedade civil e a militar, além de um instrumento para sensibilização da população[61].

Em Portugal, em 2023, foi criada a Cyber Academia and Innovation Hub, a qual tem como missão o desenvolvimento de atividades de interesse público que visam promover a formação, treinamento e exercícios, bem como estimular a pesquisa, o desenvolvimento e a inovação no domínio do ciberespaço.

Para além disso, a Direção-Geral dos Recursos Humanos da Defesa Nacional desenvolveu uma política de incentivo ao recrutamento, formação e retenção de civis ou militares para atuarem como ciberdefensores, operadores, analistas forenses ou programadores[62].

PARCERIAS

No ambiente internacional, a NCF inglesa participa de alianças como a Organização do Tratado do Atlântico Norte (NATO, na sigla inglesa) e a Five Eyes[63], estabelece parcerias, também, com países europeus e Estados Unidos. A França, por seu turno, atribui grande importância às relações bilaterais, é ativa nas discussões da Organização das Nações Unidas sobre o ciberespaço, além de participar da NATO, do grupo Ise-Shima Cyber[64], entre outros grupos que possuem a cibernética em sua agenda.

Já Portugal aderiu, em 2017, ao Cooperative Cyber Defence Center of Excellence, da NATO, projetado para potencializar o treinamento, a formação e a capacitação. Em 2019, foi instalada no país a principal sede da Communications and Information Academy, onde estão reunidas todas as atividades associadas à educação e treinamento.

DISCUSSÃO

Destarte, a análise ora empreendida demonstra que o poder cibernético – embora possua suas especificidades e seja distinto dos outros instrumentos do poder militar tradicionais – não está fora da estratégia; ao contrário, transformar os efeitos do poder cibernético em objetivos políticos faz parte da ciência da estratégia contemporânea.

Com relação aos três países analisados, observamos em suas grandes estratégias a percepção comum de que o desenvolvimento tecnológico gera a necessidade de reorganização, adaptação ou modernização das estruturas existentes, sejam de segurança ou de defesa. À medida em que Reino Unido e França possuem documentos recentemente atualizados, o ciberespaço recebe maior atenção ao se comparar com o caso português.

No tocante ao poder cibernético, os três países detêm documentos atuais em que se prevê o uso dessa ferramenta para a consecução de interesses nacionais e incremento da resiliência. O Reino Unido e a França demonstram maiores ambições no que tange a influenciar as regulamentações internacionais e a promoção da governança, ou seja, ambicionam assumir um protagonismo no cenário internacional, enquanto Portugal reforça a importância de pessoal qualificado para atuar no setor.

Nos três casos percebeu-se a necessidade de criar estruturas dedicadas, exclusivamente, ao domínio cibernético. Existem tanto instituições de segurança, associadas à esfera civil, quanto de defesa, associadas ao meio militar. França e Portugal optaram por criar comandos, enquanto o Reino Unido criou uma força, a qual reúne especialistas civis e militares, em uma parceria entre a defesa e a inteligência.

Relativamente às inovações resta claro que os três países têm buscado estabelecer laços com setores da sociedade, em especial, empresas privadas e universidades para apoio e incremento da capacidade de cibersegurança e ciberdefesa. Do mesmo modo que no âmbito internacional, no qual observou-se o empenho dos Estados em constituir alianças e estabelecer parcerias para conter as ameaças cibernéticas transfronteiriças.

O presente estudo ofereceu, portanto, um panorama das ações adotadas por três países europeus para o domínio cibernético, os quais, embora tenham percorrido trajetórias distintas, têm em comum a percepção da importância de se estar preparado para atuar neste ambiente. A estratégia metodológica eleita visou auxiliar o(a) leitor(a) na identificação e catalogação das informações, sem qualquer pretensão generalizante e/ou exaustiva, considerando de extrema valia a produção de outros estudos, os quais possam acrescentar novos dados e casos.

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Natália Diniz Schwether Doutora e pós-doutora em Ciência Política pela Universidade Federal de Pernambuco.

> Centro de Filosofia e Ciências Humanas (CFCH) – UFPE, Rua Acadêmico Hélio Ramos, s/n, 6.º andar, Cidade Universitária – Recife, PE, Brasil | n.schwether@unesp.br

Marcos Aurélio Guedes de Oliveira Professor titular do Departamento de Ciência Política da Universidade Federal de Pernambuco.

> Centro de Filosofia e Ciências Humanas (CFCH) – UFPE, Rua Acadêmico Hélio Ramos, s/n, 6.º andar, Cidade Universitária – Recife, PE, Brasil | marcosaurelioguedes@gmail.com

NOTAS

1 O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

2 ITU – «Global Cybersecurity Index». 2021. Consultado em: 20 de março de 2024. Disponível em: https://www.itu.int/pub/D-STR-GCI.01.

3 SWANSON, Michael – *The War State: The Cold War Origins of the Military-Industrial Complex and the Power Elite, 1945-1963*. South Carolina: Create Space, 2013; SILOVE, Nina – «Beyond the buzzword: the three meanings of "Grand Strategy"». In *Security Studies*. Vol. 27, N.º 1, 2017, pp. 27-57; DHENIN, Miguel – «Além da grand strategy e do entorno estratégico: uma proposta para esboçar uma grande estratégia fronteiriça». In *Revista da Escola de Guerra Naval*. Vol. 27, N.º 1, 2021, pp. 31-54.

4 LIDDELL-HART, Basil Henry – *Strategy: The Indirect Approach*. Londres: Faber & Faber, 1967, p. 322. Salvo indicação em contrário, todas as citações são traduções livres dos autores.

5 KENNEDY, Paul – *The Rise and Fall of Great Powers*. Nova Iorque: Random House, 1987, p. 5.

6 SILOVE, Nina – «Beyond the buzzword...».

7 MURRAY, Williamson – «Thoughts on grand strategy». *In* MURRAY, Williamson; SINNREICH, Richard Hart; LACEY, James, eds. – *The Shaping of Grand Strategy: Policy, Diplomacy, and War*. Cambridge: Cambridge University Press, 2011.

8 WALT, S. – «The case for finite containment: analyzing U.S. Grand Strategy». In *International Security*. Vol. 14, N.º 1, 1989.

9 SILOVE, Nina – «Beyond the buzzword...»; WALKER, Márcio; MARIÑO, Horacio – «A grande estratégia: mudanças de modos e meios pelas operações de informação e a ameaça aos interesses brasileiros e argentinos». In *Coleção Meira Mattos*. Vol. 17, N.º 60, 2023, pp. 473-486.

10 BRANDS, Hal – *The Promise and Pitfalls of Grand Strategy*. Strategic Studies Institute, US Army War College, 2012.

11 BROOKS, Stephen G.; WOHLFORTH, William C. – *America Abroad: The United States' Global Role in the 21st Century*. Nova Iorque: Oxford University Press, 2016.

12 Thomas J. Christiensen *apud* DHENIN, Miguel – «Além da grand strategy e do entorno estratégico...».

13 MILANI, Carlos; NERY, Tiago – «The sketch of Brazil's grand strategy under the Workers' Party (2003-2016): domestic and international constraints». In *South African Journal of International Affairs*. Vol. 26, N.º 1, 2019.

14 MIRANDA, Walter; VIOLANTE, Alexandre; VALENÇA, Marcelo – «A articulação entre diplomacia e poder militar nas grandes estratégias do Barão do Rio Branco e Amorim». In *Coleção Meira Mattos*. Vol. 15, N.º 53, 2021, pp. 185-205.

15 FIGUEIREDO, Eurico – *Pensamento Estratégico Brasileiro: Discursos*. Rio de Janeiro: Editora Luzes, 2015.

16 SHELDON, John – «The rise of cyber-power». *In* BAYLIS, John; WIRTZ, James; GRAY, Colin (org.) – *Strategy in the Contemporary World: An Introduction to Strategic Studies*. Nova Iorque: Oxford University Press, 2013.

17 MIRANDA, Walter; VIOLANTE, Alexandre; VALENÇA, Marcelo – «A articulação entre diplomacia e poder militar...».

18 DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «Strategy in an uncertain domain: threat and response in cyberspace». In *Journal of Strategic Security*. Vol. 15, N.º 2, 2022, pp. 34-47.

19 NYE, Joseph – *Cyber Power*. Harvard Kennedy School, Belfer Center, 2010.

20 SHELDON, John – «Deciphering cyber-power strategic purpose in peace and war». In *Strategic Studies Quarterly*. Vol. 5, N.º 2, 2011.

21 NYE, Joseph – *Cyber Power*.

22 SHELDON, John – «Deciphering cyber-power strategic purpose in peace and war», p. 103.

23 GRAY, Colin – *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Washington, DC: Strategic Studies Institute, US Army War College, 2013.

24 FERREIRA, Walfredo – «Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder». In *Coleção Meira Mattos*. Vol. 8, N.º 31, 2014, pp. 7-18.

25 BUCHANAN, Ben – *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge: Harvard University Press, 2020, p. 7.

26 O ciberespaço é o mais novo dos domínios operacionais da guerra, classificado, em 2016, pela NATO.

27 WALKER, Márcio; MARIÑO, Horacio – «A Grande Estratégia...».

28 MAZENAC, Brian – «Why international order in cyberspace is not inevitable». In *Strategic Studies Quarterly*. Vol. 9, N.º 2, 2015, pp. 78-98.

29 BIRDWELL, M. Bodine; MILLS, Robert – «War fighting in cyberspace: evolving force presentation and command and control». In *Air & Space Power Journal*. Vol. 25, N.º 1, 2011, pp. 26-36.

30 FERREIRA, Walfredo – «Territorializando o "novo" e (re)territorializando os tradicionais...», p. 7.

31 MAZENAC, Brian – «Why international order in cyberspace is not inevitable».

32 RID, Thomas; BUCHANAN, Ben – «Attributing cyber attacks». In *Journal of Strategic Studies*. Vol. 38, N.º 1-2, 2015, pp. 4-37.

33 LIBICKY, Martin – «Cyberwar as a confidence game». In *Strategic Studies Quarterly*. Vol. 5, N.º 1, 2011.

34 JERVIS, Robert – «Some thoughts on deterrence in the cyber era». In *Journal of Information Warfare*. Vol. 15, N.º 2, 2016, pp. 66-73.

35 LIJPHART, A. – «The comparable cases strategy in comparative research». In *Comparative Political Studies*. Vol. 8, 1975, pp. 158-177.

36 HM GOVERNMENT – «Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy». 16 de março de 2021. Atualizado em: 2 de julho de 2021. Policy paper. 2021. Disponível em: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

37 *Ibidem*.

38 *Ibidem*.

39 *Ibidem*.

40 RÉPUBLIQUE FRANÇAISE – *Revue Stratégique de Défense et de Securité Nationale*. 2017, p. 33.

41 MINISTÈRE DES ARMÉES – *Actualisation Stratégique 2021*. 2021, p. 18.

42 *Ibidem*.

43 RÉPUBLIQUE FRANÇAISE – *Revue Nationale Stratégique 2022*. 2022, p. 37.

44 GOVERNO DE PORTUGAL – *Conceito Estratégico de Defesa Nacional*. 2013.

45 HM GOVERNMENT – *National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK*. 2021.

46 *Ibidem*.

47 *Ibidem*.

48 RÉPUBLIQUE FRANÇAISE – *Revue Stratégique de Cyberdéfense*. 2018.

49 MOLNÁR, Dóra – «La cybersecurite en France: le passé, le présent et l'avenir». In *Hadmérnök*. Vol. 14, N.º 1, 2019, pp. 283-297.

50 MINISTÈRE DES ARMÉES – *Doctrine militaire de lutte informatique défensive*. COMCYBER, 2019.

51 MINISTÈRE DES ARMÉES – *Éléments Publics de Doctrine Militaire de Lutte Informatique d'Influence*. COMCYBER, 2021.

52 «RESOLUÇÃO DO Conselho de Ministros n.º 36/2015. Aprova a Estratégia Nacional de Segurança do Ciberespaço». In *Diário da República*. 2015.

53 «RESOLUÇÃO DO Conselho de Ministros n.º 92/2019. Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023». In *Diário da República*. 2019.

54 «RESOLUÇÃO DO Conselho de Ministros n.º 106/2022. Aprova a Estratégia Nacional de Ciberdefesa». In *Diário da República*. 2022.

55 *Ibidem*.

56 NATIONAL CYBER FORCE – *The National Cyber Force: Responsible Cyber Power in Practice*. 2023.

57 LE GUÉDARD, Martial – «Organisation de l'État français en gestión de crise cybernétique majeure». In *IHEMI*. 2019.

58 GERY, Aude – «La stratégie française de cyberdéfense». In *BRENNUS 4.0*. 2020.

59 Assumiu a atual configuração, em 2018, com a publicação da Lei N.º 46/2018, que estabeleceu o Regime Jurídico da Segurança do Ciberespaço.

60 MOLNÁR, Dóra – «La cybersecurite en France…».

61 *Ibidem*.

62 PEREIRA, Bruno – «A Evolução da Relevância do Ciberespaço para a NATO». Instituto Universitário Militar, 2022. Trabalho de Investigação Individual.

63 Aliança de inteligência, compartilhamento de informações e proteção contra ameaças entre os Estados Unidos, o Reino Unido, o Canadá, a Austrália e a Nova Zelândia.

64 Um grupo de trabalho formado pelos países do G7 (Japão, Itália, Canadá, França, Estados Unidos, Reino Unido e Alemanha) sobre cibersegurança.

BIBLIOGRAFIA

BIRDWELL, M. Bodine; MILLS, Robert – «War fighting in cyberspace: evolving force presentation and command and control». In *Air & Space Power Journal*. Vol. 25, N.º 1, 2011, pp. 26-36.

BRANDS, Hal – *The Promise and Pitfalls of Grand Strategy*. Strategic Studies Institute, US Army War College, 2012.

BROOKS, Stephen G.; WOHLFORTH, William C. – *America Abroad: The United States' Global Role in the 21st Century*. Nova Iorque: Oxford University Press, 2016.

BUCHANAN, Ben – *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge: Harvard University Press, 2020.

DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «Strategy in an uncertain domain: threat and response in cyberspace». In *Journal of Strategic Security*. Vol. 15, N.º 2, 2022, pp. 34-47. DOI: 10.5038/1944-0472.15.2.1954.

DHENIN, Miguel – «Além da grand strategy e do entorno estratégico: uma proposta para esboçar uma grande estratégia fronteiriça». In *Revista da Escola de Guerra Naval*. Vol. 27, N.º 1, 2021, pp. 31-54.

FERREIRA, Walfredo – «Territorializando o "novo" e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder». In *Coleção Meira Mattos*. Vol. 8, N.º 31, 2014, pp. 7-18.

FIGUEIREDO, Eurico – *Pensamento Estratégico Brasileiro: Discursos*. Rio de Janeiro: Editora Luzes, 2015.

GERY, Aude – «La stratégie française de cyberdéfense». In *BRENNUS 4.0*. 2020.

«GLOBAL BRITAIN in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy». Updated 2 July 2021. Policy paper. 2021. Disponível em: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

GRAY, Colin – *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Washington, DC: Strategic Studies Institute, US Army War College, 2013.

GOVERNO DE PORTUGAL – *Conceito Estratégico de Defesa Nacional*. 2013.

HM GOVERNMENT – «Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy». 16 de março de 2021. Atualizado em: 2 de julho de 2021. Policy paper. 2021. Disponível em: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

HM GOVERNMENT – *National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK*. 2021.

ITU – «Global Cybersecurity Index». 2021. Consultado em: 20 de março de 2024. Disponível em: https://www.itu.int/pub/D-STR-GCI.01.

JERVIS, Robert – «Some thoughts on deterrence in the cyber era». In *Journal of Information Warfare*. Vol. 15, N.º 2, 2016, pp. 66-73.

KENNEDY, Paul – *The Rise and Fall of Great Powers*. Nova Iorque: Random House, 1987.

LE GUÉDARD, Martial – «Organisation de l'État français en gestión de crise cybernétique majeure». In *IHEMI*. 2019.

LIBICKY, Martin – «Cyberwar as a confidence game». In *Strategic Studies Quarterly*. Vol. 5, N.º 1, 2011.

LIDDELL-HART, Basil Henry – *Strategy: The Indirect Approach*. Londres: Faber & Faber, 1967.

LIJPHART, A. – «The comparable cases strategy in comparative research». In *Comparative Political Studies*. Vol. 8, 1975, pp. 158-177.

MAZENAC, Brian – «Why international order in cyberspace is not inevitable». In *Strategic Studies Quarterly*. Vol. 9, N.º 2, 2015, pp. 78-98.

MILANI, Carlos; NERY, Tiago – «The sketch of Brazil's grand strategy under the Workers' Party (2003-2016): domestic and international constraints». In *South African Journal of International Affairs*. Vol. 26, N.º 1, 2019.

MINISTÈRE DES ARMÉES – *Doctrine militaire de lutte informatique défensive*. COMCYBER, 2019.

MINISTÈRE DES ARMÉES – *Actualisation Stratégique 2021*. 2021.

MINISTÈRE DES ARMÉES – *Éléments Publics de Doctrine Militaire de Lutte Informatique d'Influence*. COMCYBER, 2021.

MIRANDA, Walter; VIOLANTE, Alexandre; VALENÇA, Marcelo – «A articulação entre diplomacia e poder militar nas grandes estratégias do Barão do Rio Branco e Amorim». In *Coleção Meira Mattos*. Vol. 15, N.º 53, 2021, pp. 185-205.

MOLNÁR, Dóra – «La cybersecurite en France: le passé, le présent et l'avenir». In *Hadmérnök*. Vol. 14, N.º 1, 2019, pp. 283-297.

MURRAY, Williamson – «Thoughts on grand strategy». *In* MURRAY, Williamson; SINNREICH, Richard Hart; LACEY, James, eds. – *The Shaping of Grand Strategy: Policy, Diplomacy, and War*. Cambridge: Cambridge University Press, 2011.

NATIONAL CYBER FORCE – *The National Cyber Force: Responsible Cyber Power in Practice*. 2023.

NYE, Joseph – *Cyber Power*. Harvard Kennedy School, Belfer Center, 2010.

PEREIRA, Bruno – «A Evolução da Relevância do Ciberespaço para a NATO». Instituto Universitário Militar, 2022. Trabalho de Investigação Individual.

RÉPUBLIQUE FRANÇAISE – *Revue Stratégique de Défense et de Securité Nationale*. 2017.

RÉPUBLIQUE FRANÇAISE – *Revue Stratégique de Cyberdéfense*. 2018.

RÉPUBLIQUE FRANÇAISE – *Revue Nationale Stratégique 2022*. 2022.

«RESOLUÇÃO DO Conselho de Ministros n.º 36/2015. Aprova a Estratégia Nacional de Segurança do Ciberespaço». In *Diário da República*. 2015.

«RESOLUÇÃO DO Conselho de Ministros n.º 92/2019. Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023». In *Diário da República*. 2019.

«RESOLUÇÃO DO Conselho de Ministros n.º 106/2022. Aprova a Estratégia Nacional de Ciberdefesa». In *Diário da República*. 2022.

RID, Thomas; BUCHANAN, Ben – «Attributing cyber attacks». In *Journal of Strategic Studies*. Vol. 38, N.º 1-2, 2015, pp. 4-37.

SHELDON, John – «Deciphering cyberpower strategic purpose in peace and war». In *Strategic Studies Quarterly*. Vol. 5, N.º 2, 2011.

SHELDON, John – «The rise of cyberpower». *In* BAYLIS, John; WIRTZ, James; GRAY, Colin (org.) – *Strategy in the Contemporary World: an Introduction to Strategic Studies*. Nova Iorque: Oxford University Press, 2013.

SILOVE, Nina – «Beyond the buzzword: the three meanings of "Grand Strategy"». In *Security Studies*. Vol. 27, N.º 1, 2017, pp. 27-57.

SWANSON, Michael – *The War State: The Cold War Origins of the Military-Industrial Complex and the Power Elite, 1945-1963*. South Carolina: Create Space, 2013.

WALKER, Márcio; MARIÑO, Horacio – «A Grande Estratégia: mudanças de modos e meios pelas operações de informação e a ameaça aos interesses brasileiros e argentinos». In *Coleção Meira Mattos*. Vol. 17, N.º 60, 2023, pp. 473-486.

WALT, Stephen – «The case for finite containment: analyzing U.S. Grand Strategy». In *International Security*. Vol. 14, N.º 1, 1989, pp. 5-49.

Proteção de dados: experiência internacional e o caso brasileiro

Relação com a segurança da informação e a governança cibernética

Constança Maria Maia Arruda
Pedro Arthur Linhares Lima

INTRODUÇÃO

Manuel Castells[1], em sua obra *A Cidade Informacional*, afirma que «as revoluções tecnológicas fazem parte sempre de um processo de mudança mais amplo, dentro do paradigma tecno-econômico que constitui a base do processo de produção, consumo e gestão».

Desta forma, as últimas décadas trouxeram consigo o debate da privacidade no âmbito digital e, em consequência, a necessidade de implementar um marco normativo capaz de proteger os direitos dos cidadãos quanto à privacidade de seus dados, tal como a Lei Geral de Proteção de Dados (LGPD) brasileira.

Em relação à segurança da informação e a segurança cibernética, no caso específico do Brasil, destaca-se o documento «Lista de Alto Risco (LAR) da Administração Pública federal», elaborado pelo Tribunal de Contas da União (TCU) em junho de 2022 no qual são tratadas as «áreas da Administração Pública federal em que o TCU identificou riscos que podem comprometer tanto a qualidade dos serviços ofertados pelo governo quanto a eficácia das políticas públicas»[2]. Uma dessas áreas é a segurança da informação e a segurança cibernética.

No mencionado documento, o TCU afirma: «Existe, portanto, carência de [...] atos normativos que regulem os

RESUMO

No presente artigo é realizada uma análise dos principais aspectos que envolvem a privacidade no âmbito digital e dos normativos que tratam do tema e sua evolução, tanto no Brasil como em outros países e blocos, destacando a proteção de dados. Em relação à Lei Geral de Proteção de Dados no Brasil é apresentado um estudo detalhado da evolução da temática no país e a repercussão que a lei ocasionou, em particular quanto à visualização pela necessidade de ampliação da segurança da informação e da governança cibernética no país. São revisitados também fatos ocorridos, tais como o episódio das denúncias de Edward Snowden, que levaram, em conjunto com o advento da Lei Geral de Proteção de Dados, a uma necessidade de ampliar a regulação brasileira que trata da segurança cibernética, trazendo, assim, os aspectos que levaram à elaboração e publicação de uma Política Nacional de Segurança Cibernética no Brasil. São abordados ainda os aspectos relacionados aos levantamentos e auditorias realizados pelo Tribunal de Contas da União, órgão de controle externo do país, visando avaliar as ações e riscos envolvidos quanto à proteção de dados pessoais,

→

 https://doi.org/10.23906/ri2024.82a04

no que se refere às ações governamentais, que vêm suscitando a necessidade de que novas regulações sejam editadas e, após postas em vigor, conhecer dados sobre sua implementação.

Palavras-chave: proteção de dados, governança cibernética, segurança cibernética, Lei Geral de Proteção de Dados.

ABSTRACT

Data protection: international experience and the Brazilian case – relationship with information security and cyber governance

This article presents an analysis of the main aspects related to privacy in the digital environment and the regulations that deal with the subject and its evolution, highlighting the issue of data protection both in Brazil and in other countries and blocs. In relation to the General Data Protection Law in Brazil, a detailed study has been carried out on the evolution of the issue in the country and the repercussions that the law has caused, especially in relation to the need to expand information security and cyber governance. Also reviewed are events that occurred, such as the episode of Edward Snowden's accusations, which, together with the advent of the General Data Protection Law, led to the need to expand the Brazilian regulation that deals with cybersecurity, thus bringing the aspects that led to the elaboration and publication of a National Cybersecurity Policy in Brazil. Aspects related to surveys and audits carried out by the Federal Audit Court, the country's external control body, are also covered, with the aim of evaluating the actions and risks related to the protection of personal data, in terms of government actions, which raises the need to issue new regulations and, once they are in force, to know data on their implementation.

Keywords: data protection, cyber governance, cybersecurity, General Data Protection Law.

temas em todo o território nacional, incluindo os setores público e privado; investimentos em segurança da informação e segurança cibernética, áreas de importância estratégica para o país»[3].

Desta forma, o presente artigo busca abordar um tema considerado extremamente relevante para o país, além de buscar comparativos em termos da regulação da privacidade de dados em outros países e blocos ao redor do planeta.

A PROTEÇÃO DE DADOS PESSOAIS: EVOLUÇÃO E ABORDAGENS REGULATÓRIAS

PROTEÇÃO DE DADOS PESSOAIS NA EUROPA E EM OUTROS BLOCOS E PAÍSES

A criação da Comunidade Econômica Europeia (CEE), cuja origem data de 1957, quando foi instituída pelo Tratado de Roma – o chamado «Mercado Comum» –, conduziu à necessidade de ser criada uma legislação unificada para o bloco, para o tratamento de dados, tendo em vista a diversidade jurídica de seus membros.

Os primeiros normativos sobre proteção de dados surgiram nas décadas de 1960 e 1970. Reinaldo Filho[4] salienta que, embora o «direito à privacidade» (*right to privacy*) tenha se desenvolvido originalmente na jurisprudência e doutrina norte-americanas, são europeus os principais e mais completos conjuntos de leis sobre proteção de dados pessoais, que emergiram nessas décadas.

Assim, em 1970, o Estado alemão Hesse editou a chamada «Hessisches Datenschutzgesetz» (Ato de Proteção de Dados de Hesse)[5], primeira lei sobre essa matéria. A Suécia conta com a «Sw. Datalagen» (Ato de Dados Sueco), editada em 1973, como menciona Öman[6]. Desde 1977, a Alemanha tem uma lei federal de proteção de uso ilícito de dados pessoais. A Dinamarca regulamenta a questão da proteção de dados pelas leis 243 e 244, ambas de 8 de julho de 1978, que estenderam a proteção também para as pessoas jurídicas. A França conta com a Lei 78-77, de 6 de janeiro de 1978. Espanha e Portugal consideram a privacidade como direito fundamental em suas constituições, bem como a Áustria. De acordo com Reinaldo Filho[7]

e Monteiro et al.[8], a Espanha possui uma regra constitucional determinando a regulamentação da proteção da privacidade contra invasões da atividade informática (artigo 18, par. 1.º). A Constituição de Portugal de 1977 contempla, em seu artigo 35.º, a previsão do direito do cidadão de conhecer os dados que lhe são concernentes, de que esses dados sejam utilizados de acordo com a finalidade para o qual foram recolhidos e, ainda, de retificá-los (em caso de erro) e de atualizá-los.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[9], desde 1980, trata da proteção da privacidade entre seus países-membros. As «Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais» foram adotadas como recomendação do Conselho da OCDE, em apoio aos três princípios comuns aos países-membros da Organização: democracia pluralista, respeito aos direitos humanos e economias de mercado aberto, entraram em vigor em 23 de setembro de 1980.

No ano de 1981, o Conselho da Europa aprovou a Convenção 108: «Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal»[10], por considerar

> «desejável alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado».

Posteriormente, a Diretiva 95/46/CE, aprovada pelo Parlamento Europeu em 1995, cuja versão consolidada data de 2003, vigorou até maio de 2018, diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Tal diretiva foi substituída pelo Regulamento n.° 2016/679, de 27 de abril de 2016, popularmente conhecido como «General Data Protection Regulation (GDPR)», a nova lei geral de proteção de dados da União Europeia[11].

Como retrata Klosowski[12], no caso dos Estados Unidos, somente três estados americanos contam com leis relativas à privacidade de dados: Califórnia (CCPA e suas emendas, CPRA), Virgínia (VCDPA) e Colorado (ColoPA). Independentemente do estado em que a empresa está localizada, os direitos que as leis fornecem aplicam-se apenas às pessoas que moram nesses estados.

A Lei de Privacidade do Consumidor da Califórnia (CCPA), considerada uma das leis de privacidade dos Estados Unidos mais abrangentes até hoje, entrou em vigor em 1 de janeiro de 2020. A CCPA impôs limitações significativas à coleta e venda de informações pessoais de um consumidor e fornece aos consumidores direitos expansivos em relação às suas informações pessoais. Como registra Lewis[13], menos de um ano depois, em 3 de novembro de 2020, a maioria dos residentes da Califórnia votou a favor da Proposição 24, que incluía a Lei de Direitos de Privacidade da Califórnia (CPRA), cuja base

está na extensa estrutura de direitos e obrigações de privacidade da CCPA, que entrou em vigor em 1.º de janeiro de 2023, expandindo e modificando os principais aspectos da CCPA.

ENQUANTO NO BRASIL, O RESPEITO À PRIVACIDADE É UM DIREITO FUNDAMENTAL, NOS ESTADOS UNIDOS, A PRIVACIDADE É INTERPRETADA COMO *COMMODITY*, OU SEJA, OS DADOS PESSOAIS SÃO MERCADORIA PASSÍVEL DE LIVRE COMERCIALIZAÇÃO.

Enquanto no Brasil, o respeito à privacidade é um direito fundamental, nos Estados Unidos, a privacidade é interpretada como *commodity*, ou seja, os dados pessoais são mercadoria passível de livre comercialização, salvo quando se trata dos menores de 13 anos e alguns setores específicos, estes regulados por normas setoriais. Conforme destacado por Stephens[14], a CCPA, mesmo trazendo direitos aos titulares dos dados pessoais, não muda essa concepção, pois a venda de tais informações continua livre, salvo em caso de oposição.

Ainda tratando da legislação estadunidense a respeito de privacidade de dados, menciona-se a lei que trata da coleta de dados de crianças e adolescentes, a Children's Online Privacy Protection Act (COPPA)[15] entrou em vigor em 21 de abril de 2000.

Brancher[16], em relação à abordagem que trata da regulação da proteção de dados, ao redor do mundo, explica que os modelos mais recorrentes são os de regulação setorial ou geral. O modelo setorial se baseia na propositura de legislações que regulam o tratamento de dados pessoais com foco em elementos específicos, em geral direcionadas, podendo focar no setor público ou no privado, a determinados setores do mercado e a categorias de titulares de dados distintos. O segundo modelo, o geral, propõe que um mesmo regime de proteção de dados se aplique a todos os tratamentos de dados pessoais independentemente de elementos específicos. Assim, todas as entidades, sejam públicas ou privadas, que tratem dados pessoais estarão, via de regra, sujeitas às mesmas obrigações, enquanto todo titular de dados terá acesso às mesmas garantias e direitos.

Quanto aos países que possuem legislação cujo modelo é o de regulação geral, em relação à proteção de dados pessoais destacam-se, além da União Europeia (UE), o Brasil, a Argentina e o Japão.

Na direção de uma regulação geral, Katz[17] destaca que a China aprovou, em 20 de agosto de 2021, a Personal Information Protection Law (PIPL), que entrou em vigor em 1.º de novembro do mesmo ano. Ao realizar análise sobre a nova lei chinesa, à primeira vista, a PIPL é simplesmente um reflexo do GDPR da UE. Neste aspecto, a PIPL e a GDPR têm um escopo amplo, e, portanto, se aplicam a todas as empresas que lidam com dados de cidadãos chineses ou da UE, respectivamente, sejam empresas domésticas ou internacionais.

No entanto, como afirma Burgess[18], o aspecto que representa o maior impacto da nova lei de privacidade da China é que ela representa um aumento severo de custos e uma

série de restrições às operações de companhias externas na China, o que provocou o início do êxodo do país de grandes empresas de tecnologia.

No cenário da América do Sul, Monteiro et al.[19] relatam que, dos 12 países pertencentes ao continente, somente Argentina, Chile, Colômbia, Peru, Uruguai, Paraguai e Guiana Francesa possuem leis gerais para a proteção dos dados dos titulares. Ainda no contexto sul-americano, entre os países que possuem leis setoriais sobre proteção de dados estão o Equador, a Bolívia, a Venezuela e a Guiana, restando o Suriname como único país do continente que ainda não possui lei específica sobre o tema. No entanto, em sua Constituição, no artigo 17, consta que todos possuem direito ao respeito à sua privacidade, à vida de sua família, sua residência, sua honra e sua boa reputação.

O Chile foi um dos primeiros países da América Latina a conceber a sua lei de proteção de dados, a Lei de Proteção de Dados de Caráter Pessoal[20], de agosto de 1999. A Argentina aprovou a Lei de Proteção de Dados Pessoais, em outubro de 2000[21], contendo disposições e princípios gerais relativos à proteção de dados, e que, entre outros aspectos, deu ao país uma legislação que inclui em seu âmbito um órgão de controle denominado «Registro Nacional de Bases de Dados».

Na Colômbia, vigora a Lei Estatutária N.º 1581 de 17 de outubro de 2012[22], cujo objetivo «é desenvolver o direito constitucional de que todas as pessoas têm de conhecer, atualizar e retificar as informações que delas tenham sido recolhidas em bases de dados ou arquivos». O Peru conta com a Lei N.º 29.733/2011 (lei de proteção de dados pessoais)[23], cujo objetivo é «garantir o direito fundamental à proteção dos dados pessoais, previsto no artigo 2 n.º 6, da Constituição Política do Peru, através de seu adequado tratamento, em um quadro de respeito aos demais direitos fundamentais».

No Uruguai, a Lei N.º 18.331, de 11 de agosto de 2008, reconhece a proteção de dados pessoais como um direito fundamental incluído na Constituição do país, cria a Unidade Reguladora de Controle de Dados Pessoais (URCDP), como órgão que garante o direito e institui um regime baseado em princípios e direitos. O país dispõe ainda de um «Guía sobre Protección de Datos Personales en Uruguay»[24].

Conforme consta na Red Iberoamericana de Protección de Datos[25], o Paraguai não dispõe de uma lei geral de proteção de dados, contando apenas com a Lei N.º 1.682/2001, que regula a informação privada, a qual consiste em um dispositivo genérico sobre o tema e que aborda de forma ampla quais dados podem ser tratados e como isso pode ocorrer, além de estabelecer sanções para as organizações que descumpram tais disposições.

O Equador não possuía, até 2021, uma legislação específica sobre a proteção de dados. Em 26 de maio de 2021, foi publicada a Ley Orgánica de Protección de Datos Personales[26]. A sua finalidade é garantir o direito à proteção de dados pessoais, o que inclui o acesso e decisão sobre informações e dados desta natureza, bem como a respetiva proteção.

No âmbito do Mercosul, um marco para a proteção de dados foi assinado no Dia Internacional da Proteção de Dados Pessoais, dia 28 de janeiro de 2021, entre Brasil, Argentina,

Paraguai e Uruguai, estados partes do bloco. Trata-se do Acordo sobre Comércio Eletrônico do Mercosul[27], aprovado por meio da Decisão 15/20 do Conselho do Mercado Comum. O acordo, em seu artigo 6.º, trata, especificamente, da proteção de dados pessoais.

A padronização do arcabouço jurídico de proteção de dados pessoais em todo o mundo vem sendo pesquisada por organismos de cooperação internacional, por meio de grupos de estudo sobre temas relevantes e trocas de informações sobre práticas internas e leis nacionais pelas autoridades. Entre esses grupos, destaca-se o Grupo de Trabalho sobre Segurança e Privacidade na Economia Digital, da OCDE[28]. O grupo reúne especialistas em políticas de governos membros e parceiros da OCDE, bem como empresas, sociedade civil e comunidade técnica da internet para compartilhar experiências sobre melhores abordagens de segurança e privacidade em um ambiente aberto e globalmente interconectado.

PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A Constituição brasileira de 1988[29] menciona alguns pontos sobre proteção de dados. Em seu artigo 5.º, a Carta Magna faz menção à privacidade dos brasileiros: «são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação».

Não obstante, uma das importantes decorrências da LGPD[30] é a promulgação, em 10 de fevereiro de 2022, da Emenda Constitucional 115[31], que inclui a proteção de dados pessoais entre os direitos e garantias fundamentais previstos na Constituição Federal. O texto também fixa a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

No início dos anos 1990, surge no Brasil o Código de Defesa do Consumidor[32], que definiu regras para as relações entre empresas e clientes, que possui uma seção específica sobre cadastros e banco de dados e, ainda, defende o direito do consumidor a acessar os dados que uma empresa possua sobre ele e solicitar sua correção, caso alguma informação esteja incorreta.

Em relação às atividades que tratam de telecomunicações e internet, no Brasil, existe uma separação funcional, estabelecida em lei. A regulação das redes de telecomunicações se encontra sob responsabilidade da Agência Nacional de Telecomunicações (Anatel), enquanto a regulação dos serviços relacionados com as atividades de internet é realizada de forma distribuída, sendo que diferentes atores têm diferentes responsabilidades, conforme suas próprias atribuições.

Os principais dispositivos legais que tratam dos assuntos relacionados às telecomunicações são: a Norma 004/1995 – que tem como objetivo regular o uso de meios da Rede Pública de Telecomunicações para o provimento e utilização de Serviços de Conexão à Internet[33] – e a Lei N.º 9.472/1997 (denominada Lei Geral de Telecomunicações)[34] – que «Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador».

Apontadas tais considerações, Schmidt[35] lembra que, até o ano de 2012, o Brasil não dispunha de leis para punir os crimes cibernéticos próprios [aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)]. O país dispunha somente de legislação para tratar crimes cibernéticos impróprios (aqueles que atingem um bem jurídico comum, como o patrimônio, e utilizam os sistemas informáticos apenas como *animus operandi*, ou seja, um novo meio de execução).

Tendo em vista fatos ocorridos no ano de 2012, em que ataques do tipo «DDoS» (ataques distribuídos de negação de serviço) foram perpetrados a *sites* do Governo e ocorreu a divulgação de fotos íntimas da atriz Carolina Dieckmann, houve urgência na aprovação de duas leis, que cobriam algumas lacunas, entre aquelas existentes no ordenamento jurídico do país em relação a essa matéria. São elas: a Lei 12.735/201215, conhecida como «Lei Azeredo», por ter sido proposta pelo ex-senador; e a Lei 12.737/201216, conhecida como «Lei Carolina Dieckmann», após o vazamento de fotos íntimas da atriz na internet em 2012.

No entanto, o Marco Civil da Internet[36], conhecido como a «Constituição da Internet», é considerado uma das mais importantes leis brasileiras. Um longo e conturbado percurso foi percorrido até a aprovação dessa lei, sendo finalmente sancionada pela Presidente da República em 23 de abril de 2014, após aprovada em 22 de abril de 2014, pelo Senado Federal, durante a abertura do Encontro Global Multissetorial sobre o Futuro da Governança da Internet – NET Mundial, em São Paulo, que reuniu representantes de mais de 80 países. Em 2016, o Marco Civil da Internet foi regulamentado pelo Decreto N.º 8.771, de 11 de maio de 2016[37].

O MARCO CIVIL DA INTERNET, CONHECIDO COMO A «CONSTITUIÇÃO DA INTERNET», É CONSIDERADO UMA DAS MAIS IMPORTANTES LEIS BRASILEIRAS.

Bem antes da criação da LGPD, a necessidade de uma lei de proteção de dados já se discutia no país. Em novembro de 2010 foi iniciado no Brasil o debate sobre a proteção de dados pessoais, visando elaborar uma lei específica sobre o tema. Até abril de 2011, o Ministério da Justiça manteve um blogue para colher manifestações na plataforma Cultura Digital, do Ministério da Cultura.

Em junho de 2012, foi apresentado na Câmara dos Deputados um projeto de lei que dispunha sobre o tratamento de dados pessoais, que foi produto das discussões do V Congresso Brasileiro da Indústria da Comunicação. Ainda em 2012, foi apresentado, no Senado, outro projeto de lei do Senado para estabelecer princípios, garantias e obrigações referentes à proteção de dados pessoais. Em janeiro de 2015, o Ministério da Justiça lançou consulta pública para discutir a proteção de dados pessoais armazenados em centrais dentro ou fora do país.

Não se pode deixar de mencionar o episódio das denúncias de Edward Snowden sobre espionagem cibernética em larga escala, o que conduziu à instauração da Comissão Parlamentar de Inquérito da Espionagem Cibernética no Senado Federal, criada em 17 de

julho de 2013, para apurar denúncias de interceptação de dados pelo governo dos Estados Unidos. O relatório da Comissão Parlamentar[38], publicado em abril de 2014, apontou um diagnóstico bastante contundente do panorama da cibersegurança brasileira e apresentou diversas recomendações para a melhoria da segurança cibernética no Brasil, entre elas: «o país deve discutir e elaborar uma Política Nacional de Segurança Cibernética».

Por seu turno, a aprovação, pela UE do Regulamento Geral de Proteção de Dados Pessoais (GDPR)[39], em abril de 2016, veio a precipitar os fatos, pois, dentre as exigências do GDPR, todos os países e organizações que pretendessem manter relações comerciais com a UE deveriam dispor de uma legislação de proteção de dados pessoais em conformidade com o que determinava o regulamento.

Após diversas ações e tratativas, em julho de 2018, o Projeto de Lei da Câmara 53/2018 foi finalmente aprovado no Plenário do Senado, gerando a Lei N.º 13.709/2018 (Lei Geral de Proteção de Dados)[40]. Estava previsto que o início da vigência seria em dezoito meses a contar da publicação. Esta lei inaugura, no Brasil, um sistema de proteção de dados, proporcionando princípios basilares para salvaguardar os dados pessoais de seus respectivos titulares.

LGPD: ASPECTOS A DESTACAR, IMPLEMENTAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL E SUA RELAÇÃO COM A SEGURANÇA DA INFORMAÇÃO E A GOVERNANÇA CIBERNÉTICA

Em muitos aspectos, a LGPD contempla boas práticas em riscos e segurança da informação, esta última, cujas boas práticas e controles são norteados pela Norma ABNT NBR ISO/IEC 27002, que contempla as melhores técnicas mundialmente reconhecidas sobre o assunto. Além desse ponto, a LGPD, da mesma forma que o GDPR, tem aplicação extraterritorial, pois, as empresas estrangeiras que oferecem serviços ao mercado nacional e possuem filial no Brasil, precisam estar adequadas à lei, tendo em vista que essas organizações tratam dados de brasileiros.

Em relação à implementação na Administração Pública Federal, Zimmer[41] apresenta os resultados de uma pesquisa realizada pela PRODESP (empresa de informática do Governo do Estado de São Paulo) em 2020, com o objetivo de identificar como a administração pública estava percebendo o início da vigência da lei, sendo evidenciado que ainda existe um longo caminho no aculturamento de tratamento de dados e segurança da informação. Ao todo foram consultados 133 órgãos e entidades da administração. Nesse estudo, 42% das entidades declararam não ter práticas relacionadas à governança, privacidade e segurança da informação, 60% não utilizam meios eletrônicos ao tratar dados, e 33% declaram ainda utilizar meios físicos.

Com o objetivo de implementar a LGPD no âmbito da Administração Pública Federal, além de fortalecer a segurança da informação e promover melhorias na governança cibernética no país, foi criado o Programa de Privacidade e Segurança da Informação

(PPSI)[42], que se caracteriza como um conjunto de projetos e processos de adequação nas áreas de privacidade e segurança da informação, o qual tem como valores: a maturidade, a resiliência, a efetividade, a colaboração e a inteligência.
No sentido de viabilizar a implementação do PPSI, foram disponibilizados diversos guias, modelos e ferramentas para os órgãos e entidades, entre os quais se destacam[43]: a *Cartilha do PPSI*, um *Modelo de Política de Proteção de Dados Pessoais* e um *Modelo de Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação*. Além destas publicações, foram disponibilizadas pela Diretoria de Privacidade e Segurança da Informação diversos outros guias operacionais.
Ressalte-se, ainda, que a vigência da LGPD acabou por afetar todos os setores do país, não somente o setor público, tornando a segurança cibernética um tema cada vez mais urgente. Neste sentido, cabe registrar a importância da publicação da PNCiber – Política Nacional de Cibersegurança, instituída pelo Decreto N.º 11.856, de 26 de dezembro de 2023[44]. Com a PNCiber foi também instituído o Comitê Nacional de Cibersegurança (CNCiber), no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, com o objetivo de acompanhar a implementação e a evolução da PNCiber.
Como consta na Nota Técnica SSIC/GSI N.º 01/2023, que apresenta a exposição de motivos para o projeto de lei que visa o estabelecimento da PNCiber:

> «A PNCiber é uma proposta voltada a unificar a "colcha de retalhos" regulatória existente no país, minimizar o crescente número de incidentes que acometem o país, gerando enormes prejuízos para a sociedade brasileira, buscar diminuir o débito tecnológico nacional no setor, e ampliar a participação brasileira na cooperação internacional sobre a temática»[45].

A exemplo do que ocorreu com a LGPD, cuja influência veio da GDPR europeia, a PNCiber, conforme consta na mesma nota técnica referenciada, recebeu forte influência do modelo proposto pelo Parlamento Europeu, a Diretiva 2022/2555, também conhecida como NIS2[46], publicada em 14 de dezembro de 2022, a qual tem como objetivo alcançar um «elevado nível comum de cibersegurança na União» e que apresenta um conjunto de medidas cuja adoção pelos Estados-Membros da UE é obrigatória até 17 de outubro de 2024.
Em relação à implementação da LGPD nas organizações da Administração Pública Federal, foi realizada, pelo TCU, em 2022, uma auditoria para avaliar as ações governamentais e os riscos à proteção de dados pessoais, a qual originou o Acórdão 1384/2022 – TCU – Plenário[47], que apresenta uma extensa lista de recomendações ao governo. A análise abrangeu 382 organizações federais e foram verificadas iniciativas e medidas implementadas para o cumprimento das exigências estabelecidas na lei.

Assim, observa-se que o avanço na governança cibernética no país vem sendo buscado, em especial após a aprovação da LGPD. Um conjunto de leis e decretos vem regulando o setor cibernético no país. Destaca-se entre estes a Estratégia Nacional de Segurança Cibernética, e-Ciber[48] (que apresenta como visão para o Brasil: «Tornar-se país de excelência em segurança cibernética») e a PNCiber – Política Nacional de Cibersegurança, conforme abordado.

Pela pesquisa realizada, além dos aspectos já considerados, observa-se que tanto a LGPD quanto a PNCiber conduzem a uma necessidade de melhoria da governança cibernética nas instituições públicas e privadas. Tal fato pode favorecer a queda dos quantitativos de incidentes de segurança consumados, pois visualiza-se que, em face da obrigatoriedade de cumprimento das regulações mencionadas, além da imposição de multas em caso de descumprimento de regras postas nas mesmas, uma maior conscientização da alta administração das instituições é esperada, possibilitando o crescimento dos investimentos na área cibernética, conduzindo a uma evolução natural do país, como um todo, na proteção contra as ameaças cibernéticas.

CONSIDERAÇÕES FINAIS

Ao longo das pesquisas realizadas foi possível concluir que a LGPD insere o Brasil no rol dos países considerados seguros para tratamento de dados. No entanto, as mudanças necessárias para adaptação às regras propostas pela lei não ocorrem com facilidade, em especial, porque há uma cultura existente, que necessita ser alterada.

Cabe destaque o fato de que a LGPD considera a proteção do dado pessoal em todo o seu ciclo de vida, o que faz necessário garantir a segurança da informação em todo o ciclo, desde a criação, passando pela coleta, manuseio, processamento, armazenamento, transporte, transmissão, exclusão ou destruição definitiva da informação, mesmo depois de concluído o seu tratamento, conforme mencionado no artigo 15 da lei em análise.

Da pesquisa realizada, em especial no caso brasileiro, é possível constatar que as mudanças da regulação relativa à privacidade da informação, à segurança da informação e à governança cibernética, vêm ocorrendo de forma relativamente rápida, pois, a mais importante lei brasileira que trata de uso da internet, privacidade e proteção se dados, o «Marco Civil da Internet», data de 2014. E é fato que as mudanças a serem realizadas no modelo de gestão e governança de dados e cibernética das instituições, no país, abrangem um sem-número de áreas de conhecimento, incluindo a área de direito, a de tecnologia da informação, economia, gestão de riscos, melhoria de processos organizacionais, entre outras, a médio e longo prazos.

Em relação à auditoria para avaliar as ações governamentais e os riscos à proteção de dados pessoais, realizada pelo TCU, supracitada, o diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD apresentou situação de alto risco à privacidade dos cidadãos que têm dados pessoais coletados e tratados pela Administração Pública Federal.

Após essa auditoria, diversos normativos foram emitidos pela Autoridade Nacional de Proteção de Dados, entre os quais se destaca a Política de Governança de Processos da Autoridade Nacional de Proteção de Dados (ANPD)[49], aprovada em 2023.

Conforme já exposto, buscando obter maior aderência e adequação à LGPD, a Administração Pública vem promovendo treinamentos e cursos, editando cartilhas de boas práticas e editando normas e outras formas de regulação, em função da necessidade de mitigar eventuais riscos relacionados ao tratamento de dados pessoais.

No entanto, as organizações da Administração Pública Federal brasileira ainda estão trilhando o caminho da adaptação, para que todos os seus processos de tratamento de dados estejam de acordo com a nova realidade que se apresenta, em função da regulação já existente.

Desta forma, resultados plenamente satisfatórios, provenientes da aplicação dessa gama de legislação, ainda não se materializaram. Isso se deve, em grande medida, ao fato de a maioria dessa regulamentação ser ainda recente e, em alguma medida, à necessidade de recursos das organizações públicas para se ajustarem completamente às novas exigências.

Finalmente, é possível constatar, pela pesquisa empreendida, que a LGPD possibilita ao Brasil adotar padrões globais de proteção de dados, simplificando a condução de transações comerciais e o compartilhamento de informações com nações que mantenham leis similares. Dessa forma, entende-se ser crucial que organizações e indivíduos se ajustem aos preceitos da LGPD, visando assegurar a salvaguarda dos direitos essenciais e promover o crescimento de uma economia digital mais sólida e protegida no país. RI

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Constança Maria Maia Arruda Professora convidada de nível superior da Universidade da Força Aérea (UNIFA). Analista de Sistemas da Carreira de Tecnologia Militar do Comando da Aeronáutica – COMAER; chefe da Assessoria de Governança de TI do CCA-RJ. Mestre em Matemática Aplicada a Sistemas, pela Universidade Federal Fluminense (UFF), Niterói, Brasil (1985); especialização em Governança de Tecnologia da Informação pelo Centro Universitário do Sul de Minas, UNIS/MG, Brasil (2014). Doutoranda do Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA), da Universidade da Força Aérea (UNIFA).
> Universidade da Força Aérea – UNIFA, Av. Marechal Fontenelle, 800 , Campo dos Afonsos, Rio de Janeiro – RJ. CEP: 21740-000, Brasil | constancamaia@yahoo.com.br

Pedro Arthur Linhares Lima Professor de nível superior da Universidade da Força Aérea (UNIFA). Atualmente, participa, como coordenador da UNIFA, do Projeto Ciência, Tecnologia e Inovação em Defesa: Cibernética e Defesa Nacional, do Programa Pro-Defesa IV. Mestre em Computer Science pela Air Force Institute of Technology (1996), doutorado em Engenharia de Produção pela Universidade Federal do Rio de Janeiro – COPPE-UFRJ (2003) e MBA em Planejamento Estratégico pela COPPE-UFRJ (2009).
> Universidade da Força Aérea – UNIFA, Av. Marechal Fontenelle, 800, Campo dos Afonsos, Rio de Janeiro – RJ. CEP: 21740-000, Brasil | pedroalima@yahoo.com

NOTAS

1 CASTELLS, Manuel – *La ciudad informacional: tecnologías de la información, reestruturación económica y el proceso urbano-regional*. Madrid: Alianza Editorial, 1995. Consultado em: 20 de setembro de 2021. Disponível em: https://e-tcs.org/wp-content/uploads/2017/03/Castells_19951.pdf. Salvo indicação em contrário, todas as citações são traduções livres dos autores.

2 *LISTA DE Alto Risco (LAR) da Administração Pública Federal*. 1.ª edição. Brasília, DF: Tribunal de Contas da União. 22 de junho de 2022. Consultado em: 20 de fevereiro de 2024. Disponível em https://portal.tcu.gov.br/lista-de-alto-risco-na-administracao-publica-federal.htm.

3 *Ibidem*.

4 REINALDO FILHO, Demócrito – «A Diretiva Europeia sobre Proteção de Dados Pessoais – uma análise de seus aspectos gerais». In *Revista Jus Navigandi*. Teresina. Ano 18, N.º 3507, 6 de fevereiro de 2013. Consultado em: 21 de novembro de 2021. Disponível em: https://jus.com.br/artigos/23669.

5 «HESSISCHES DATENSCHUTZGESETZ». 19 de fevereiro de 1999. Consultado em: 29 de setembro de 2020. Disponível em: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/HDSG.pdf.

6 ÖMAN, Sören – «Implementing Data Protection in Law». In *Scandinavian Studies in Law*. Vol. 47, *It Law*, 2004, pp. 389-403. Consultado em: 20 de setembro de 2021. Disponível em: https://filedn.com/ljdBas5OJsrLJOq6KhtBYC4/skrifter/implementing-data-protection-in-law.pdf.

7 *Ibidem*.

8 MONTEIRO, Renato Leite, et al. – «Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos». Baptista Luz Advogados. 2019. Consultado em: 4 de setembro de 2021. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf.

9 «DIRETRIZES DA OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais». 2003. Consultado em: 2 de junho de 2022. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf.

10 «CONVENTION FOR the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)». 28 de janeiro de 1981. Consultado em: 25 de setembro de 2021. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

11 REGULAMENTO (UE) 2016/679 do Parlamento Europeu do Conselho de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados). In *Jornal Oficial da União Europeia*. 4 de maio de 2016. Consultado em: 15 de agosto de 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN.

12 KLOSOWSKI, Thorin – «The state of consumer data privacy laws in the US (and why it matters)». Wirecutter. 6 de setembro de 2021. Consultado em: 2 de outubro de 2022. Disponível em: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

13 GAVEJIAN, Jason C., et al. – «California Consumer Privacy Act, California Privacy Rights Act FAQs for covered businesses». Jackson Lewis Publications. 19 de janeiro de 2022. Consultado em: 2 de agosto de 2022. Disponível em: https://www.jacksonlewis.com/insights/california-consumer-privacy-act-california-privacy-rights-act-faqs-covered-businesses.

14 STEPHENS, J. – «California Consumer Privacy Act». ABA. 14 de fevereiro de 2019. Consultado em: 20 de setembro de 2021. Disponível em: www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

15 Lei americana da proteção da privacidade das crianças *online*.

16 BRANCHER, Paulo Marcos Rodrigues – «Proteção internacional de dados pessoais». Enciclopédia Jurídica da PUCSP. Tomo Direito Internacional. 1.ª edição. Fevereiro de 2022. São Paulo: Pontifícia Universidade Católica de São Paulo, 2022. Consultado em: 15 de setembro de 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais.

17 KATZ, Noah – «How China is weaponizing privacy». In *The Student Journal of Information Privacy Law*. 15 de março de 2022. Consultado em: 10 de setembro de 2022. Disponível em: https://wpsites.maine.edu/mlipa/2022/03/15/how-china-is-weaponizing-privacy/.

18 BURGESS, Matt – «Ignore China's new data privacy law at your peril». WIRED. 5 de novembro de 2021. Consultado em: 10 de julho de 2022. Disponível em: https://www.wired.com/story/china-personal-data-law-pipl/.

19 *Ibidem*.

20 LEY 19628, 28 de agosto de 1999. Proteccion de datos de caracter personal. Consultado em: 15 de agosto de 2021. Disponível em: www.bcn.cl/leychile/navegar?idNorma=141599&idParte=864270.

21 LEY N. 25.326. Disposiciones Generales. Principios generales relativos a la protección de datos. 4 de outubro de 2000. Consultado em: 29 de setembro de 2020. Disponível em: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf.

22 LEY ESTATUTARIA 1581 de 2012 (octubre 17). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá. Consultado em: 19 de agosto de 2020. Disponível em: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

23 LEY N.º 29.733, 3 julio 2011. Ley de protección de datos personales. Consultado em: 19 de agosto de 2021. Disponível em: www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf.

24 «GUÍA SOBRE Protección de datos personales en Uruguay». Unidad Reguladora y de Control de Datos Personales. 26 de setembro de 2023. Consultado em: 20 de novembro de 2023. Disponível em: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/guia-sobre-proteccion-datos-personales-uruguay#:~:text=En%20Uruguay%2C%20la%20Ley%20N,competencias%20necesarias%20para%20garantizar%20el.

25 «LEGISLACIÓN – REPÚBLICA del Paraguay. Red IPD@2019». Consultado em: 12 de setembro de 2021. Disponível em: https://www.redipd.org/es/legislacion?nid=80.

26 LEY ORGÁNICA de protección de datos personales. Registro Oficial. Quinto Suplemento. Ao II – N.º 459, 26 de maio de 2021. Assembleia Nacional, República do Equador. Consultado em: 10 de julho de 2022. Disponível em: https://drive.google.com/file/d/1UhmqRQpkkBjWs5iGGiB_oOxKeRdaX2Ut/view.

27 «ACORDO SOBRE o Comércio Eletrônico do Mercosul». 2021. Consultado em: 10 de julho de 2022. Disponível em: https://www.gov.br/siscomex/pt-br/arquivos-e-imagens/2020/12/82753_dec_015-2020_pt_acordo-comercio-eletronico.pdf.

28 «SUMMARY OF the OECD Privacy Expert Roundtable». Working Party on Security and Privacy in the Digital Economy. 20 de maio de 2014. Consultado em: 2 de setembro de 2023. Disponível em: https://one.oecd.org/document/DSTI/ICCP/REG(2014)3/en/pdf.

29 CONSTITUIÇÃO DA República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Consultado em: 10 de outubro de 2021. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/508200.

30 LEI GERAL de Proteção de Dados Pessoais (LGPD), Dada pela Lei N.º 13.853, de 8 de julho de 2019. Atualizado até julho de 2019. Presidência da República. Brasília, DF. Consultado em: 10 de novembro de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

31 EMENDA CONSTITUCIONAL N.º 115, de 10 de fevereiro de 2022: Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garan-

tias fundamentais. Presidência da República. Brasília, DF. Consultado em: 24 de setembro de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais.

32 *CÓDIGO DE Defesa do Consumidor e Normas Correlatas*. 2.ª edição. Atualizado até setembro de 2017. Senado Federal. Brasília, DF. Consultado em: 10 de outubro de 2021. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/533814/cdc_e_normas_correlatas_2ed.pdf?sequence=1.

33 PORTARIA N.º 148, de 38 de maio de 1995: Aprova a Norma N.º 004/95 – Uso da Rede Pública de Telecomunicações para acesso à Internet. Ministério das Comunicações. Agência Nacional de Telecomunicações. PORTAL Gov.br. Brasília, DF. Consultado em: 20 de setembro de 2021. Disponível em: https://informacoes.anatel.gov.br/legislacao/normas-do-mc/78-portaria-148.

34 LEI N.º 9.472, de 16 de julho de 1997: Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais. Presidência da República. Brasília, DF. Consultado em: 24 de setembro de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm.

35 SCHMIDT, Guilherme – «Crimes cibernéticos». Jusbrasil. 6 de novembro de 2014. Consultado em: 15 de setembro de 2021. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos.

36 LEI N.º 12.965, de 23 de abril de 2014: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Presidência da República. Brasília, DF. Consultado em: 24 de setembro de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

37 DECRETO N.º 8.771, de 11 de maio de 2016. Regulamenta a Lei N.º 12.965, de 23 de abril de 2014. Presidência da República. Brasília, DF. Consultado em: 24 de setembro de 2022. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm.

38 «COMISSÃO PARLAMENTAR de Inquérito – CPI da espionagem: Relatório Final N.º 1, de 2014». Senado Federal. Brasília, DF. Consultado em: 24 de setembro de 2021. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/609904.

39 *Ibidem*.

40 *Ibidem*.

41 ZIMMER, P. – «A Lei Geral de Proteção de Dados (LGPD) e seu impacto nas organizações públicas». Gestão Pública. Softplan. Atualizado em: 16 de junho de 2021. Consultado em: 10 de agosto de 2022. Disponível em: https://www.gestaopublica.softplan.com.br/conteudo/a-lei-geral-de-protecao-de-dados-lgpd-e-seu-impacto-nas-organizacoes-publicas/.

42 PORTARIA SGD/MGI N.º 852, de 28 de março de 2023: Programa de Privacidade e Segurança da Informação (PPSI)». Ministério da Gestão e da Inovação em Serviços Públicos. Governo Digital. Brasília, DF. Consultado em: 10 de janeiro de 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908.

43 «GUIAS E modelos do Programa de Privacidade e Segurança da Informação (PPSI)». Ministério da Gestão e da Inovação em Serviços Públicos. Governo Digital. Brasília, DF. Atualizado em: março de 2023. Consultado em: 10 de janeiro de 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/guias-e-modelos/pagina_guias_e_modelos.

44 DECRETO N.º 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Presidência da República. Brasília, DF. Consultado em: 10 de janeiro de 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm.

45 «NOTA TÉCNICA SSIC/GSI N.º 01/2023. Assunto: Proposta de Projeto de Lei de Criação da Política Nacional de Cibersegurança». GSI. Brasília. DF. Consultado em: 10 de janeiro de 2024. Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf.

46 DIRETIVA (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022. In *Jornal Oficial da União Europeia*. 27 de dezembro de 2022. Consultado em: 27 de março de 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&from=EN.

47 «SECOM TCU. TCU verifica risco alto à privacidade de dados pessoais coletados pelo governo». PORTAL TCU. Brasília, DF. 21 de junho de 2022. Consultado em: 14 de setembro de 2022. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm.

48 DECRETO N.º 10.222, de 5 de fevereiro de 2020: Aprova a Estratégia Nacional de Segurança Cibernética. Presidência da República. Brasília, DF. Consultado em: 10 de outubro de 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

49 RESOLUÇÃO CD/ANPD N.º 8, de 5 de setembro de 2023. Institui a Política de Governança de Processos da Autoridade Nacional de Proteção de Dados. Ministério da Justiça e Segurança Pública. Governo Digital. Autoridade Nacional de Proteção de Dados. Publicações da ANPD. Atualizado em: 20 de fevereiro de 2024. Consultado em: 25 de fevereiro de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-8-de-5-de-setembro-de-2023-508638337.

BIBLIOGRAFIA

LEGISLAÇÃO NACIONAL

ALEMANHA

«HESSISCHES DATENSCHUTZGESETZ». 19 de fevereiro de 1999. Consultado em: 29 de setembro de 2020. Disponível em: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/HDSG.pdf.

ARGENTINA

LEY N. 25.326. Disposiciones Generales. Principios generales relativos a la protección de datos. 4 de outubro de 2000. Consultado em: 29 de setembro de 2020. Disponível em: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf.

BRASIL

CONSTITUIÇÃO DA República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Consultado em: 10 de outubro de 2021. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/508200.

«COMISSÃO PARLAMENTAR de Inquérito – CPI da espionagem: Relatório Final N.º 1, de 2014». Senado Federal. Brasília, DF. Consultado em: 24 de setembro de 2021. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/609904.

CÓDIGO DE Defesa do Consumidor e Normas Correlatas. 2.ª edição. Atualizado até setembro de 2017. Senado Federal. Brasília, DF. Consultado em: 10 de outubro de 2021. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/533814/cdc_e_normas_correlatas_2ed.pdf?sequence=1.

DECRETO N.º 8.771, de 11 de maio de 2016. Regulamenta a Lei N.º 12.965, de 23 de

abril de 2014. Presidência da República. Brasília, DF. Consultado em: 24 de setembro de 2022. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm.

DECRETO N.º 10.222, de 5 de fevereiro de 2020: Aprova a Estratégia Nacional de Segurança Cibernética. Presidência da República. Brasília, DF. Consultado em: 10 de outubro de 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

DECRETO N.º 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Presidência da República. Brasília, DF. Consultado em: 10 de janeiro de 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm.

EMENDA CONSTITUCIONAL N.º 115, de 10 de fevereiro de 2022: Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Presidência da República. Brasília, DF. Consultado em: 24 de setembro de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais.

LEI GERAL de Proteção de Dados Pessoais (LGPD), Dada pela Lei N.º 13.853, de 8 de julho de 2019. Atualizado até julho de 2019. Presidência da República. Brasília, DF. Consultado em: 10 de novembro de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

LEI N.º 9.472, de 16 de julho de 1997: Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais. Presidência da República. Brasília, DF. Consultado em: 24 de setembro de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm.

LEI N.º 12.965, de 23 de abril de 2014: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Presidência da República. Brasília, DF. Consultado em: 24 de setembro de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

LISTA DE Alto Risco (LAR) da Administração Pública Federal. 1.ª edição. Brasília, DF: Tribunal de Contas da União. 22 de junho de 2022. Consultado em: 20 de fevereiro de 2024. Disponível em https://portal.tcu.gov.br/lista-de-alto-risco-na-administracao-publica-federal.htm.

«GUIAS E modelos do Programa de Privacidade e Segurança da Informação (PPSI)». Ministério da Gestão e da Inovação em Serviços Públicos. Governo Digital. Brasília, DF. Atualizado em: março de 2023. Consultado em: 10 de janeiro de 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/guias-e-modelos/pagina_guias_e_modelos.

«NOTA TÉCNICA SSIC/GSI N.º 01/2023. Assunto: Proposta de Projeto de Lei de Criação da Política Nacional de Cibersegurança». GSI. Brasília, DF. Consultado em: 10 de janeiro de 2024. Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf.

PORTARIA N.º 148, de 38 de maio de 1995: Aprova a Norma N.º 004/95 – Uso da Rede Pública de Telecomunicações para acesso à Internet. Ministério das Comunicações. Agência Nacional de Telecomunicações. PORTAL Gov.br. Brasília, DF. Consultado em: 20 de setembro de 2021. Disponível em: https://informacoes.anatel.gov.br/legislacao/normas-do-mc/78-portaria-148.

PORTARIA SGD/MGI N.º 852, de 28 de março de 2023: Programa de Privacidade e Segurança da Informação (PPSI)». Ministério da Gestão e da Inovação em Serviços Públicos. Governo Digital. Brasília, DF. Consultado em: 10 de janeiro de 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908.

RESOLUÇÃO CD/ANPD N.º 8, de 5 de setembro de 2023. Institui a Política de Governança de Processos da Autoridade Nacional de Proteção de Dados. Ministério da Justiça e Segurança Pública. Governo Digital. Autoridade Nacional de Proteção de Dados. Publicações da ANPD. Atualizado em: 20 de fevereiro de 2024. Consultado em: 25 de fevereiro de 2024]. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-8-de-5-de-setembro-de-2023-508638337.

«SECOM TCU. TCU verifica risco alto à privacidade de dados pessoais coletados pelo governo». PORTAL TCU. Brasília, DF. 21 de junho de 2022. Consultado em: 14 de setembro de 2022. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm.

CHILE
LEY 19628, 28 de agosto de 1999. Proteccion de datos de caracter personal. Consultado em: 15 de agosto de 2021. Disponível em: www.bcn.cl/leychile/navegar?idNorma=141599&idParte=864270.

COLÔMBIA
LEY ESTATUTARIA 1581 de 2012 (octubre 17). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá. Consultado em: 19 de agosto de 2020. Disponível em: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

COUNCIL OF EUROPE
«CONVENTION FOR the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)». 28 de janeiro de 1981. Consultado em: 25 de setembro de 2021. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108.

EQUADOR
LEY ORGÁNICA de protección de datos personales. Registro Oficial. Quinto Suplemento. Ao II – N.º 459, 26 de maio de 2021. Assembleia Nacional, República do Equador. Consultado em: 10 de julho de 2022. Disponível em: https://drive.google.com/file/d/1UhmqRQpkkBjWs5iGGiB_oOxKeRdaX2Ut/view.

MERCOSUL
«ACORDO SOBRE o Comércio Eletrônico do Mercosul». 2021. Consultado em: 10 de julho de 2022. Disponível em: https://www.gov.br/siscomex/pt-br/arquivos-e-imagens/2020/12/82753_dec_015-2020_pt_acordo-comercio-eletronico.pdf.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE
«DIRETRIZES DA OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais». 2003. Consultado em: 2 de junho de 2022. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf.

«SUMMARY OF the OECD Privacy Expert Roundtable». Working Party on Security and Privacy in the Digital Economy. 20 de maio de 2014. Consultado em: 2 de setembro de 2023. Disponível em: https://one.oecd.org/document/DSTI/ICCP/REG(2014)3/en/pdf.

PERU
LEY N.º 29.733, 3 julio 2011. Ley de protección de datos personales. Consultado em: 19 de agosto de 2021. Disponível em: www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf.

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS
«LEGISLACIÓN – REPÚBLICA del Paraguay. Red IPD@2019». Consultado em: 12 de setembro de 2021. Disponível em: https://www.redipd.org/es/legislacion?nid=80.

UNIÃO EUROPEIA
DIRETIVA (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022. In *Jornal Oficial da União Europeia*. 27 de dezembro de 2022. Consultado em: 27 de março de 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&from=EN.

REGULAMENTO (UE) 2016/679 do Parlamento Europeu do Conselho de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados). In *Jornal Oficial da União Europeia*. 4 de maio de 2016. Consultado em: 15 de agosto de 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN.

URUGUAI
«GUÍA SOBRE Protección de datos personales en Uruguay». Unidad Reguladora y de Control de Datos Personales. 26 de setembro de 2023. Consultado em: 20 de novembro de 2023. Disponível em: https://www.gub.uy/unidad-reguladora-control-

-datos-personales/comunicacion/noticias/guia-sobre-proteccion-datos-personales--uruguay#:~:text=En%20Uruguay%2C%20la%20Ley%20N,competencias%20necesarias%20para%20garantizar%20el.

BIBLIOGRAFIA GERAL

BRANCHER, Paulo Marcos Rodrigues – «Proteção internacional de dados pessoais». Enciclopédia Jurídica da PUCSP. Tomo Direito Internacional. 1.ª edição. Fevereiro de 2022. São Paulo: Pontifícia Universidade Católica de São Paulo, 2022. Consultado em: 15 de setembro de 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais.

BURGESS, Matt – «Ignore China's new data privacy law at your peril». WIRED. 5 de novembro de 2021. Consultado em: 10 de julho de 2022. Disponível em: https://www.wired.com/story/china-personal-data-law-pipl/.

CASTELLS, Manuel – *La ciudad informacional: tecnologías de la información, reestruturación económica y el proceso urbano-regional*. Madrid: Alianza Editorial, 1995. Consultado em: 20 de setembro de 2021. Disponível em: https://e-tcs.org/wp-content/uploads/2017/03/Castells_19951.pdf.

GAVEJIAN, Jason C.; LAZZAROTTI, Joseph J.; SILVER, Damon W.; COSTIGAN, Mary T.; PAISAN, Sean – «California Consumer Privacy Act, California Privacy Rights Act FAQs for covered businesses». Jackson Lewis Publications. 19 de janeiro de 2022. Consultado em: 2 de agosto de 2022. Disponível em: https://www.jacksonlewis.com/insights/california-consumer-privacy-act-california-privacy-rights-act-faqs-covered-businesses.

KATZ, Noah – «How China is weaponizing privacy». In *The Student Journal of Information Privacy Law*. 15 de março de 2022. Consultado em: 10 de setembro de 2022. Disponível em: https://wpsites.maine.edu/mlipa/2022/03/15/how-china-is-weaponizing-privacy/.

KLOSOWSKI, Thorin – «The state of consumer data privacy laws in the US (and why it matters)». Wirecutter. 6 de setembro de 2021. Consultado em: 2 de outubro de 2022. Disponível em: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriane Loureiro; MORIBE, Gabriela; CAMARA, Dennys Eduardo Gonsales; GHERIN, Pamela Michelena De Marchi – «Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos». Baptista Luz Advogados. 2019. Consultado em: 4 de setembro de 2021. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf.

ÖMAN, Sören – «Implementing Data Protection in Law». In *Scandinavian Studies in Law*. Vol. 47, *It Law*, 2004, pp. 389-403. Consultado em: 20 de setembro de 2021. Disponível em: https://filedn.com/ljdBas5OJsrLJOq6KhtBYC4/skrifter/implementing-data-protection-in-law.pdf.

REINALDO FILHO, Demócrito – «A Diretiva Europeia sobre Proteção de Dados Pessoais – uma análise de seus aspectos gerais». In *Revista Jus Navigandi*. Teresina. Ano 18, N.º 3507, 6 de fevereiro de 2013. Consultado em: 21 de novembro de 2021. Disponível em: https://jus.com.br/artigos/23669.

SCHMIDT, Guilherme – «Crimes cibernéticos». Jusbrasil. 6 de novembro de 2014. Consultado em: 15 de setembro de 2021. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos.

STEPHENS, J. – «California Consumer Privacy Act». ABA. 14 de fevereiro de 2019. Consultado em: 20 de setembro de 2021. Disponível em: www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

ZIMMER, P. – «A Lei Geral de Proteção de Dados (LGPD) e seu impacto nas organizações públicas». Gestão Pública. Softplan. Atualizado em: 16 de junho de 2021. Consultado em: 10 de agosto de 2022. Disponível em: https://www.gestaopublica.softplan.com.br/conteudo/a-lei-geral-de-protecao-de-dados-lgpd-e-seu-impacto-nas-organizacoes-publicas/.

Defesa cibernética na guerra russo-ucraniana
Um mapeamento dos ataques cibernéticos às infraestruturas críticas da Ucrânia

Thays Felipe David de Oliveira | *Renato Victor Lira Brito* | *Priscylla Cristina de Souza Lippo*

INTRODUÇÃO

Quais ataques cibernéticos às infraestruturas críticas (IC) sofreu a Ucrânia entre fevereiro de 2022 e fevereiro de 2023 durante a Guerra russo-ucraniana? Sabemos que os ataques cibernéticos às IC têm como escopo gerar uma desordem ao Estado que sofreu com o dano. Uma vez que, quando isso acontece, há um comprometimento inteiro de sistemas através de *softwares* maliciosos.

No ano de 2022, a incidência de ataques cibernéticos foi menos recorrente quando comparado ao ano de 2023. Dessa forma, os dados referentes a este fenômeno apontam que a Dinamarca sofreu um total de 11 ataques, enquanto a França sete e em menor número os Países Baixos com seis[1]. Perante o exposto, esta temática é de suma importância para a área da defesa nacional, pois as IC são bens e serviços essenciais para o pleno funcionamento de um Estado. Logo, áreas como administração pública, comunicação e energia compõem esta esfera, que, quando atacadas, geram danos devastadores à sociedade, como no caso Stuxnet.

Nesse diapasão, a Ucrânia pode ser tomada como exemplo de estudo de caso único[2] para discutir questões de políticas de defesa de um Estado no espaço cibernético, uma vez que, por falta de regulação e fis-

RESUMO

Quais ataques cibernéticos às infraestruturas críticas sofreu a Ucrânia entre fevereiro de 2022 e fevereiro de 2023 durante a guerra russo-ucraniana? Nos últimos meses, a Ucrânia vem sofrendo uma grande ofensiva de ataques cibernéticos às suas infraestruturas críticas. Assim, o objetivo deste trabalho é analisar quais ataques cibernéticos às infraestruturas críticas sofreu a Ucrânia dentro do recorte selecionado. Para isso, foi realizada uma pesquisa de método misto, que foi operacionalizada por meio de estatística descritiva, análise documental e revisão sistemática da literatura. Assim, a partir dos dados analisados do CyberPeace Institute, o setor mais atingido foi o de administração pública (66), enquanto a categoria de ataques mais utilizada foi de disrupção (139). Em seguida, avaliamos os tipos de ataques cibernéticos, sendo o mais utilizado o de tipo «DDoS» (135). Já na categoria de atores, a categoria «coletiva» (124), com destaque para o People's CyberArmy (48), foi a de maior ocorrência. Em suma, concluímos que os ataques às infraestruturas críticas constituem uma questão de defesa nacional, sendo necessário revisar a →

 https://doi.org/10.23906/ri2024.82a05

legislação relacionada a esse tema e garantir que os órgãos responsáveis estejam preparados para enfrentar problemas futuros.

Palavras-chave: infraestruturas críticas, defesa nacional, Ucrânia, ataques cibernéticos.

ABSTRACT

Cyber defense in the Russo-Ukrainian war: a mapping of cyber attacks on Ukrainian critical infrastructure

What cyberattacks did Ukraine's critical infrastructure experience between February 2022 and February 2023 during the Russo-Ukrainian war? In recent months, Ukraine has experienced a significant increase in cyberattacks on its critical infrastructure. Therefore, the purpose of this study is to analyze the cyberattacks suffered by Ukraine's critical infrastructure within the selected cutout. A mixed method research approach was used, operationalized through descriptive statistics, documentary analysis, and a systematic literature review. Based on the analyzed data from the CyberPeace Institute, the sector most affected was public administration (66), with the Disruption attack category being the most utilized (139). The types of cyberattacks were also evaluated, with the DDoS type being the most common (135). The collective (124), especially the People's CyberArmy (48), was the most common in the actor category. In conclusion, we can say that attacks on critical infrastructure are a matter of national defense, which requires a revision of legislation on this issue and ensuring that the responsible bodies are prepared for future challenges.

Keywords: critical infrastructure, national defense, Ukraine, cyberattacks.

calização, este domínio é visto como um campo de infinitas possibilidades de ações que podem gerar consequências no meio físico.

Este trabalho tem por objetivo geral analisar quais ataques cibernéticos às IC sofreu a Ucrânia entre fevereiro de 2022 e fevereiro de 2023 durante a guerra russo-ucraniana. Para tanto, operacionalizou-se a pesquisa por meio de técnicas de métodos mistos, como de estatística descritiva, análise documental e revisão sistemática da literatura.

Nas próximas seções, apresenta-se brevemente o contexto da guerra russo-ucraniana, seguido por considerações acerca do espaço cibernético e suas IC e pela análise dos ataques direcionados à Ucrânia que têm acontecido no âmbito dessa guerra.

METODOLOGIA

A Ucrânia sofreu diversos ataques cibernéticos às suas IC desde o início da guerra russo-ucraniana. Sendo assim, para compreender este fenômeno, foi elaborado o seguinte panorama:

Quadro 1 > Desenho da pesquisa

Pergunta de pesquisa	Quais ataques cibernéticos às IC sofreu a Ucrânia entre fevereiro de 2022 e fevereiro de 2023 durante a guerra russo-ucraniana?
Unidade espacial de análise	Infraestruturas críticas ucranianas
Unidade temporal de análise	Fevereiro de 2022 a fevereiro de 2023
Método	Misto (quantitativo e qualitativo)
Técnica	Estatística descritiva, análise documental e revisão sistemática da literatura

Fonte: Elaborado pelos autores.

Perante o recorte metodológico realizado nesta pesquisa, foi utilizado o estudo de caso único que, segundo Yin[3], é uma das maneiras de se fazer pesquisa nas Relações Internacionais, que envolve experimentos, levantamentos, pesquisas históricas e análise de informações de documentos. Portanto, este trabalho realiza um recorte dentre os temas existentes no contexto da guerra russo-ucraniana, especialmente os ataques cibernéticos às IC da Ucrânia.

De forma complementar, essa pesquisa foi conduzida por meio de métodos mistos segundo Paranhos et al.[4], dado que foram utilizados os métodos qualitativo e quantitativo. Assim, a metodologia qualitativa responde a questões nas Relações Internacionais com um nível de complexidade difícil de ser quantificado. A partir dessa perspectiva, o presente artigo foi operacionalizado por meio de uma análise documental e de uma revisão sistemática da literatura.

Conforme exposto, o quadro 2 apresenta as fontes primárias e secundárias utilizadas neste artigo. As fontes secundárias foram utilizadas unicamente com a finalidade de exemplificar os ataques cibernéticos às IC ucranianas cometidos no espaço temporal analisado.

Quadro 2 > Categoria das fontes

Fontes primárias	CyberPeace Institute
	Documentos governamentais da Ucrânia e da Rússia
	Documentos do Conselho de Segurança das Nações Unidas
Fontes secundárias	CNN, BBC, g1, The Cyber Express

Fonte: Elaborado pelos autores.

A revisão sistemática proporcionou um levantamento do arcabouço teórico, com o intuito de auxiliar na compreensão sobre o fenômeno estudado a partir das fontes supracitadas.

O outro método utilizado foi o quantitativo, que é definido como uma «restrição ao uso de determinadas estatísticas para a identificação [...] das variáveis»[5]. Para operacionalização deste, foram considerados os dados do CyberPeace Institute, que serão exibidos nos resultados e discussões a partir de gráficos, a fim de auxiliar na compreensão das informações.

Complementarmente, foi utilizada a estatística descritiva, pois «[a] estatística descritiva auxilia os métodos quantitativos de forma a definir (frequência, média, mediana, moda etc.) a revelar formas úteis, rápidas e confiáveis a respeito de um grande número de observações»[6]. Assim, esta técnica auxiliou na elaboração de uma análise estatística sobre os ataques cibernéticos às IC sofridos pela Ucrânia no período de fevereiro de 2022 a fevereiro de 2023 da guerra em curso no leste europeu e na perfilação dos resultados quantificados. Para isso, os dados foram tabulados no Microsoft Excel.

Por fim, foram analisados os dados referenciados ao ataque cibernético das IC da Ucrânia e estão disponibilizados no GitHub[7] para oferecer uma maior replicabilidade à presente pesquisa nos termos de King[8]. Assim, uma pesquisa acadêmica de boa qualidade deve permitir gerar inferências válidas[9].

O CONTEXTO DA GUERRA RUSSO-UCRANIANA

Com o colapso da União das Repúblicas Socialistas Soviéticas, em 1991, a Ucrânia se tornou uma nação independente. A região ucraniana é dividida em dois lados: o oeste, onde fica a capital Kiev, localização que facilita o elo com o ocidente europeu, por sua posição geoestratégica, e é a região que apresenta uma maior atuação da União Europeia e da Organização do Tratado do Atlântico Norte (NATO, na sigla inglesa). Em contrapartida, existe o lado leste, predominantemente a área do Donbass, que possui uma grande quantidade de russos e de movimentos de cunho separatista.

Todavia, a partir de 2014, a Ucrânia desenvolveu uma relação de preferência, em termos de política externa, às potências ocidentais sob a liderança de Petro Poroshenko. Após esse movimento, a clara insatisfação russa com o Governo ucraniano serviu de base para que a Rússia invadisse a região da Crimeia, desrespeitando assim o Memorando de Budapeste[10].

Após este conjunto de acontecimentos, no ano de 2019, para deteriorar a situação, Volodymyr Zelensky, o atual Presidente da Ucrânia, ascendeu ao poder com um ideal de romper com a Rússia e de que apenas voltaria a ter relações com o país caso os separatistas devolvessem territórios ocupados para a Ucrânia[11]. Simultaneamente a isso, o Estado se mostrou cada vez mais próximo da NATO, deixando um sentimento ainda maior de ameaça na Federação Russa, já que uma parte de sua fronteira estava sob o domínio da NATO, devido à adesão da Polônia.

O POSSÍVEL PRIMEIRO ATAQUE DE PUTIN FOI UTILIZAR A REGIÃO DE DONBASS AO SEU FAVOR, PROMOVENDO ATAQUES CIBERNÉTICOS E DISSEMINAÇÃO DE *FAKE NEWS*, DESENCADEANDO ASSIM UMA ESPÉCIE DE GUERRA CIVIL NO PAÍS.

Em suma, a Ucrânia divide geograficamente uma grande parte da fronteira com a Rússia. Logo, a anexação desse território à organização ocidental significaria que tropas estadunidenses poderiam estar cada vez mais próximas do domínio russo. Por isso, o possível primeiro ataque de Putin foi utilizar a região de Donbass ao seu favor, promovendo ataques cibernéticos e disseminação de *fake news*, desencadeando assim uma espécie de guerra civil no país, contradizendo os princípios de ingresso à NATO de que o território não pode estar passando por conflitos internos.

O ESPAÇO CIBERNÉTICO E AS INFRAESTRUTURAS CRÍTICAS

Na atualidade, o espaço cibernético tem sido extremamente utilizado por atores estatais e não estatais em seu favor, tanto em questões referentes à defesa nacional, quanto em ofensivas diretas a outro Estado sem necessariamente existir um *front* direto. Um grande exemplo dessa ação é o caso Stuxnet, um *worm* que invadiu o sistema de supervisão e

aquisição de dados (SCADA) da empresa Siemens, que afetou gravemente as usinas nucleares iranianas e desestabilizou o funcionamento das ogivas, e que caso levasse à explosão, seria de dano inestimável ao Irã[12].

Nesse sentido, este tipo de ação é característico no espaço cibernético. Logo, podemos considerar este fenômeno como «o território não físico criado por meios computacionais, onde pessoas podem se comunicar, realizar pesquisas e trafegar dados de maneira geral, valendo-se de Tecnologias da Informação e Comunicação (TIC)»[13]. Ademais, o espaço cibernético é um fenômeno relativamente recente para os Estados, e ainda há certo receio de como estes podem atuar, tendo em vista que ainda não existe uma legislação internacional amplamente aceita que regulamente este domínio[14].

De forma complementar, a defesa do espaço cibernético é efetivada de acordo com a legislação de cada país. Assim, no Brasil, é competência de órgãos como o Ministério da Defesa e o Gabinete de Segurança Interinstitucional (GSI). Enquanto isso, nos Estados Unidos, por exemplo, o principal regulador do espaço cibernético é a National Security Agency (NSA), uma agência do Departamento de Defesa norte-americano, que trata das questões tangentes aos ataques e educação cibernética do país. A defesa cibernética dos Estados Unidos da América também é responsabilidade de 16 agências, que constituem a US Intelligence Community[15]. A Ucrânia também é um país de governança cooperativa do espaço cibernético:

> «um ambiente (espaço virtual) que oferece oportunidades de comunicação e/ou implementação de relações públicas, formado como resultado do funcionamento de sistemas de comunicação compatíveis (ligados) e de comunicações eletrônicas utilizando a Internet e/ou outras redes de dados globais»[16].

Dessa forma, a governança do espaço cibernético para o referido Estado é realizada por entidades do setor público e privado, responsáveis pela prevenção e investigação de ataques cibernéticos contra a defesa nacional. O país possui o Centro de Coordenação de Ciberdefesa e Cibersegurança, que promove assistência para formações militares atuantes na defesa de ameaças no espaço cibernético e mapeia dados de crimes virtuais com o objetivo de proteger a si e aos países com os quais coopera[17].

Sendo assim, podemos considerar os ataques cibernéticos como «qualquer tipo de manobra ofensiva para invadir um computador ou sistema»[18]. Logo, estes ataques possuem potencial de paralisar o funcionamento de serviços essenciais a um Estado, através de destruição ou interrupção do serviço, por exemplo.

No contexto atual, os Estados se tornam cada vez mais dependentes do meio cibernético, onde possuem bens e serviços essenciais para seu funcionamento. Tal dependência culmina na exposição das IC. De acordo com Martii Lehto:

> «Em geral, a infraestrutura crítica descreve os sistemas e ativos físicos e cibernéticos que são tão vitais para a nação que sua incapacidade ou destruição teria um impacto debilitante

na segurança física ou econômica ou na saúde ou segurança pública. Assim, a infraestrutura crítica da nação fornece os serviços essenciais que sustentam a sociedade»[19].

Logo, vemos que as IC possuem suma importância para a população. Portanto, são um recurso que «uma vez prejudicados por fenômenos de causas naturais, como terremotos ou inundações ou por ações intencionais de sabotagem ou terrorismo, trazem grandes reflexos negativos para toda uma nação e sua sociedade»[20].
Nesse sentido, para a Ucrânia, as IC «Devem significar e incluir os sistemas e recursos, físicos ou virtuais, que suportam funções e serviços cuja interrupção terá efeitos negativos mais graves na atividade da sociedade, no desenvolvimento socioeconômico do país e na segurança nacional»[21].
Com isso, percebemos que uma infraestrutura crítica ucraniana atacada resulta em sérios problemas para o Estado, como pode ser visto no quadro 3[22]:

Quadro 3 > Setores de IC e instituições responsáveis

Setor de IC	Principais instituições responsáveis por segurança, proteção e operação das instalações dos setores
Combustível e complexo de energia	Ministry of Energy and Coal Industry of Ukraine (MoECI), Security Service of Ukraine (SSU), Ministry of Internal Affairs of Ukraine (MIA), State Service of Special Communications and Information Protection of Ukraine (SSSCIP)
Transporte	Ministry of Infrastructure of Ukraine, SSU, MIA
Redes de suporte à vida	Ministry of Regional Development of Ukraine, Construction and Communal Services of Ukraine, State Services of Ukraine for Emergency Situations (SESU)
Telecomunicações e redes de comunicações	SSSCIP, MIA
Finanças e setor bancário	National Bank of Ukraine, Ministry of Finance of Ukraine, SSU, SSSCIP
Administração pública e aplicação da lei	SSU, MIA, State Guard Service
Complexo de defesa e segurança	Ministry of Defense of Ukraine (MoD), MIA, SSU
Indústria química	State Service of Ukraine for Labor, SSE, SSU
Serviços de emergência e proteção civil	SESU, Ministry of Health of Ukraine
Indústria de processamento alimentício e complexo agrário	Ministry of Agrarian Policy and Food of Ukraine

Fonte: Elaborado pelos autores.

Portanto, observamos que há uma gama de órgãos e instituições ucranianos responsáveis por cada setor de IC, dada a importância destes bens e serviços. Apesar de haver órgãos responsáveis, diante do cenário complexo atual, é necessário o debate acadêmico sobre os desafios e potencialidades enfrentados pelo Estado.

RESULTADOS E DISCUSSÕES

Nesta parte do artigo serão discutidos os resultados acerca da análise feita sobre os ataques cibernéticos às IC ucranianas no primeiro ano da Guerra da Ucrânia. Dessa maneira, os dados aqui apresentados foram retirados de relatórios do CyberPeace Institute no período de fevereiro de 2022 a fevereiro de 2023. Esta análise visa observar as consequências diretas para a defesa nacional da Ucrânia, visto que um ataque cibernético às suas IC tem o potencial de impactar toda uma rede de interdependência de bens e serviços.

Segundo a atual versão da Diretiva sobre a Identificação e Designação das Infraestruturas Críticas Europeias[23],o aumento da proteção das IC possibilita que o impacto gerado por ataques cibernéticos seja consideravelmente reduzido. Dessa maneira, podemos aplicar o fator da importância relativo às IC na defesa nacional dentro do contexto russo-ucraniano.

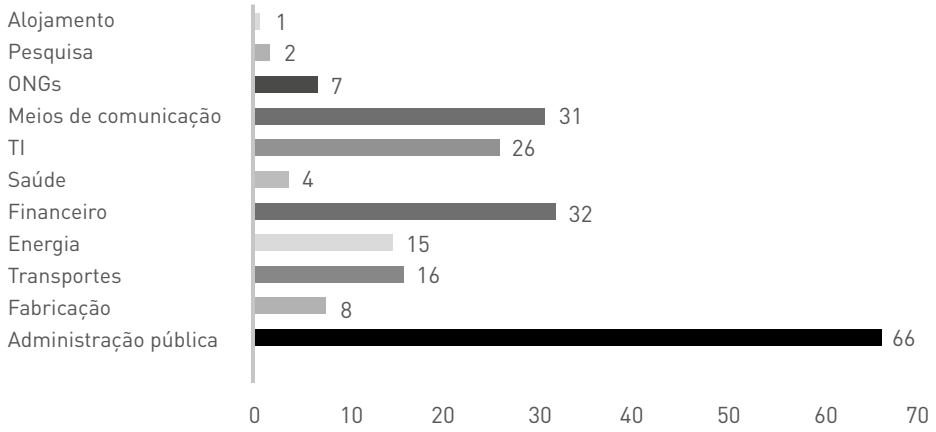
Para tal efeito, um ataque cibernético é um subconjunto de operações realizadas no espaço cibernético que fazem o uso hostil de suas capacidades, sendo realizadas por Estados ou atores não estatais com o intuito de causar danos e destruição, para alcançar objetivos militares ou políticos[24].

DURANTE A GUERRA DA UCRÂNIA HOUVE 1258 ATAQUES CIBERNÉTICOS ÀS INFRAESTRUTURAS CRÍTICAS NO MUNDO.

No entanto, durante a Guerra da Ucrânia houve 1258 ataques cibernéticos às IC no mundo, tais como em março de 2022, quando o *site* do presidente da França sofreu um ataque em meio às eleições presidenciais, enquanto apenas na Ucrânia houve 291 ataques no período estudado, e destes, 83 são desconhecidos e estão sob análise segundo o CyberPeace Institute. Mas, ao comparar com os anos anteriores, houve um aumento. Uma infraestrutura crítica, ao sofrer um ataque cibernético, gera danos às mais diversas áreas de uma sociedade. A pesquisa demonstrou que as IC da Ucrânia são compostas pelos setores presentes no gráfico 1 (p. 068), bem como seu número de ataques.

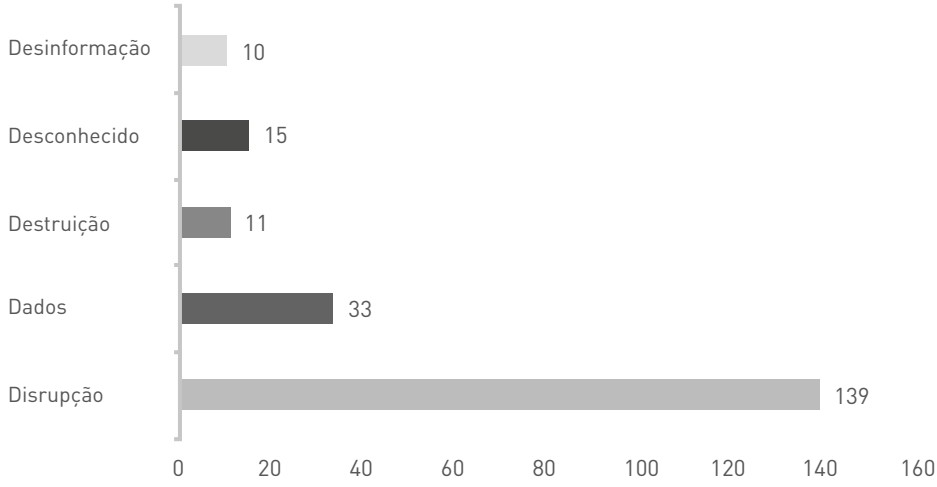
A partir dos dados apresentados, inferimos que o setor de administração pública recebeu o maior número de ataques cibernéticos (66), visto que os poderes de governar, gerenciar e regulamentar impactam diretamente o funcionamento básico de um Estado. De acordo com a CNN Brasil[25], em março de 2022 um ataque de categoria desconhecida comprometeu a rede da Ukrtelecom, uma grande operadora de telecomunicações ucraniana. Contudo, o ator responsável não foi identificado, algo comum dentro do cenário cibernético, espaço que possibilita que os atores de ataques passassem despercebidos devido à sua ausência de fiscalização.

Gráfico 1 > Ataques aos setores de infraestrutura crítica ucraniana entre fevereiro de 2022 a fevereiro de 2023



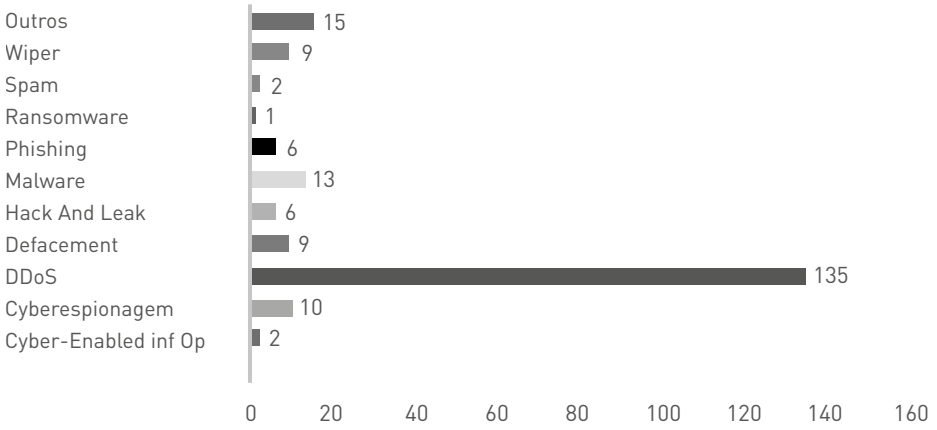
Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

Gráfico 2 > Categorias dos ataques cibernéticos às IC ucranianas entre fevereiro de 2022 e fevereiro de 2023



Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

Gráfico 3 > Tipos de ataques cibernéticos às IC da Ucrânia entre fevereiro de 2022 e fevereiro de 2023



Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

Ademais, outro setor afetado foi o da energia. Em abril de 2022, o setor da energia da Ucrânia foi afetado por um ataque cibernético de destruição, no qual *malwares* cortaram o fornecimento de energia do país, que resultou na interrupção no fornecimento de energia para aproximadamente dois milhões de ucranianos.

No gráfico 2 é possível observar que os ataques da categoria «disrupção» representam mais de metade do valor total de ataques (208) sofridos pela Ucrânia.

Assim, é indispensável salientar que a disrupção é a modalidade de ataque que ameaça a disponibilidade ou a integridade de um sistema[26], sendo estes dois dos princípios da segurança da informação de acordo com Dantas[27].

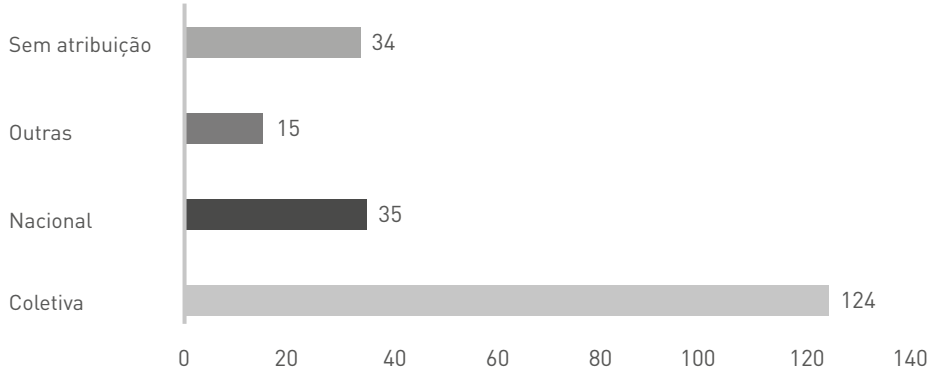
Dessa forma, a destruição, para fins comparativos, é definida por Cavelty[28] como ataques de ciberhacktivismo ou cibervandalismo – explica-se como o equivalente *online* para formas de vandalismo ou ativismo, através de panfletagem (*websites* de protesto), grafitti (*defacement*/desfiguração de algum *website*), bloqueios (ataques de negação de serviço) e ocupações (uso ilegal de algum domínio, *cybersquatting*) que visam destruir o conteúdo de um site ou sistema[29].

Além disso, ataques de desinformação baseiam-se em compartilhamento de *fake news*, modalidade esta que afeta, sobretudo, a forma como a população recebe informações. Por fim, o «desconhecido» é que ainda não se tem informação necessária para categorizar o ataque.

O gráfico 3 apresenta os tipos de ataques direcionados ao nosso objeto de estudo. O destaque vai para os 135 ataques de tipo «DDoS» (negação de serviço distribuído), que funciona por meio de envios massivos de requisições a um servidor, levando ao travamento e, consequentemente, sua interrupção[30].

Diante disso, podemos mencionar o ataque de disrupção do tipo «DDoS» ocorrido em fevereiro de 2022, noticiado pela CNN Brasil, contra o setor de finanças da Ucrânia[31]. O ator responsável pelo ataque não foi identificado, mas deixou duas importantes redes bancárias do país fora do ar.

Gráfico 4 > Categorias dos atores atribuídos aos ataques entre fevereiro de 2022 e fevereiro de 2023



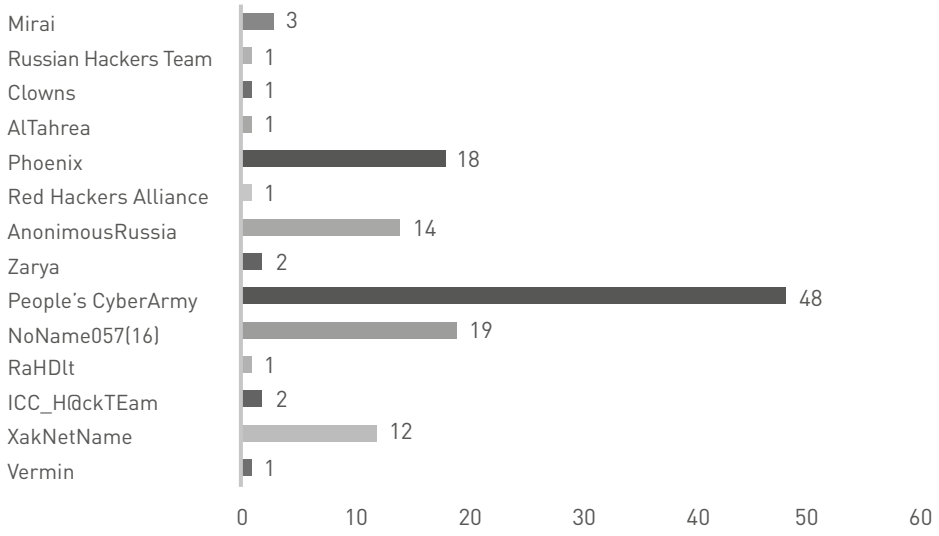
Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

O gráfico 4, da categoria dos atores, é composto por: coletiva (124), nacional (35), outras (15) e sem atribuição (34). Assim, inferimos que os atores coletivos, isto é, atores que não são vinculados a um Estado, predominam nos ataques. A exemplo de ataques atribuídos aos atores coletivos, segundo a revista *The Cyber Express*[32], em 21 de novembro de 2022, o grupo de *hackers* russos conhecido como «XakNet», foi responsável por invadir os serviços do Ministério de Finanças da Ucrânia, que possibilitou aos *hackers* obterem informações sobre mais de um milhão de documentos.

Por outro lado, em contraste com a categoria de atores coletiva, a segunda unidade com maior incidência de ataques cibernéticos é a categoria de atores nacionais, que é constituída por agentes que se intitulam como vinculados a algum governo[33].

Perante o gráfico 5 (p. 071), observamos um grande número (48) de atribuições ao grupo People's CyberArmy, grupo que se proclama afiliado à Rússia. Eles utilizam ataques «DDoS», como em janeiro de 2023 contra o *site* de uma rede de postos de gasolina da Ucrânia, em que provocaram uma disrupção na plataforma, conforme o CyberPeace Institute. Ademais, o grupo NoName057(16) possui notória participação, com o exemplo do ataque ocorrido em setembro de 2022, onde utilizou de *defacement* para violar o *site* de uma importante universidade sediada em Kiev, capital ucraniana.

Gráfico 5 > Atores atribuídos aos ataques entre fevereiro de 2022 e fevereiro de 2023



Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

O *defacement* consiste em alterações não autorizadas em *sites*, afetando o princípio da integridade, o que gera um grande impacto na reputação[34]. Ao desfigurar um *site* ou sistema, é gerada desinformação para aqueles que o acessam, visto que podem considerar como informações de procedência da própria instituição.

A partir do que foi analisado, percebemos que a Ucrânia passou por diversos ataques cibernéticos às IC durante o período da guerra com a Rússia. Logo, encoraja-se que se tomem medidas cada vez mais enérgicas referentes à segurança cibernética na Ucrânia, como, por exemplo, os cinco aspectos da segurança cibernética[35] que têm o potencial de auxiliar na prevenção e mitigação dos ataques às infraestruturas críticas, sendo estes:

Eficiência operacional: em meio ao crescimento dos investimentos tecnológicos, a colaboração entre os envolvidos faz-se indispensável para que a necessidade de proteção de dados seja compreendida.

Colaboração: todas as esferas governamentais precisam estar alinhadas em uma política de combate ao crime cibernético.

Higiene cibernética: medidas como controles de segmentação de *patching* para *firmware* e métodos de autenticação multifator compõem uma boa higiene cibernética.

Educação: em um cenário onde a maior parte das violações cibernéticas é consequência de erro humano, faz-se imprescindível o enfoque à educação cibernética em todos os âmbitos de uma sociedade, tanto no eixo individual quanto no coletivo.

Tecnologia: é importante o investimento constante na tecnologia, haja vista os rápidos avanços de *software* e de *hardware*, que quando defasados e obsoletos abrem portas para exploração de vulnerabilidades.

Os resultados acima discutidos elencam a fragilidade das IC de um Estado em meio a uma guerra no que se trata de sua defesa nacional. Esta análise cobre apenas os primeiros doze meses da guerra russo-ucraniana, porém possibilita visualizar tendências de ataques a IC ao pleno funcionamento da sociedade ucraniana.

CONSIDERAÇÕES FINAIS

Conforme descrito no presente artigo, os ataques cibernéticos às IC vêm acontecendo de forma recorrente no sistema internacional. Assim, o fato de o espaço cibernético ainda ser um cenário desconhecido facilita a perpetuação desses ataques. Portanto, sabemos que o objetivo deste estudo foi analisar quais ataques cibernéticos às IC da Ucrânia sofreu entre fevereiro de 2022 e fevereiro de 2023 durante a guerra russo-ucraniana. Logo, a Ucrânia foi um país que recebeu vários ataques cibernéticos antes e durante a guerra, o que acentua ainda mais a fragilidade do Estado e suas IC. Assim, este tema é de grande valia para a defesa nacional, pois demonstra que os Estados devem ter um determinado conhecimento relacionado aos ataques cibernéticos às IC. Nesse sentido, tais ataques podem causar danos irreparáveis para a população, especialmente porque a Ucrânia está passando por um período de guerra e acaba negligenciando uma temática de extrema relevância para a agenda de defesa nacional.

A partir do exposto, podemos perceber que a Ucrânia sofreu 291 ataques no período estudado, sendo em sua maioria no setor de administração pública, como por exemplo, um ataque de disrupção, que afetou diversos bancos ucranianos, além de ministérios como o da Defesa, Relações Exteriores e outros órgãos governamentais, do tipo «DDoS». Como apresentado durante todo o artigo, fica evidente que um país com políticas de defesa cibernética robustas pode se tornar mais eficiente e resiliente aos ataques. Então, para evitar ataques às IC é necessário que o governo tenha políticas específicas para a proteção nacional baseadas na higiene cibernética, na colaboração, na educação, na tecnologia e na eficiência operacional.

Assim como um trem, que tem a sua estrutura por inteiro afetada caso um vagão descarrilhe, um país com suas IC em mau funcionamento tem as suas demais áreas vitais desestabilizadas em uma breve questão de tempo. Desse modo, é possível perceber como os Estados e outros atores utilizam-se da vulnerabilidade de países, cujas IC foram afetadas, para instaurar guerras e conflitos de interesse. Portanto, a partir de análises realizadas no presente trabalho, concluímos que não somente os Estados mencionados neste estudo, mas também nações como o Brasil, tão presente no cenário internacional, urge a criação de um Programa de Defesa Cibernética, que tenha como seu principal objetivo aprimorar o fortalecimento da defesa cibernética nacional. Pois, por ser um

fenômeno recente, é criada uma necessidade de que o país se adeque aos novos fenômenos inerentes ao cenário internacional de Estados e que interferem diretamente na soberania estatal. R:I

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Thays Felipe David de Oliveira Coordenadora e professora de Relações Internacionais no Centro Universitário Estácio do Recife, e professora substituta em Gestão Pública na Universidade Federal da Paraíba (UFPB). Coordenadora do Núcleo de Estudos em Processos Cibernéticos em Relações Internacionais (NEPCRI). Doutora em Ciência Política pela Universidade Federal de Pernambuco (UFPE).
> Centro Universitário Estácio do Recife, Av. Eng. Abdias de Carvalho, 1678, Madalena, Recife, Pernambuco, Brasil | thaysfelipe@gmail.com

Renato Victor Lira Brito Vice-coordenador do Núcleo de Estudos em Processos Cibernéticos em Relações Internacionais (NEPCRI). Doutorando, mestre e bacharel em Ciência Política pela Universidade Federal de Pernambuco (UFPE). Editor executivo da *Revista Política Hoje*. Membro da Comissão de Direitos Humanos Dom Helder Câmara da UFPE. Membro da Comissão Própria de Avaliação da UFPE.
> Centro Universitário Estácio do Recife, Av. Eng. Abdias de Carvalho, 1678, Madalena, Recife, Pernambuco, Brasil | renato.lirabrito@ufpe.br

Priscylla Cristina de Souza Lippo Aluna da gradução em Relações Internacionais pelo Centro Universitário Estácio do Recife. Licenciada em Letras (Língua Portuguesa) pela Universidade Federal de Pernambuco e mestre em Linguística pela mesma universidade.
> Centro Universitário Estácio do Recife, Av. Eng. Abdias de Carvalho, 1678, Madalena, Recife, Pernambuco, Brasil | priscyllaalippo@gmail.com

NOTAS

1 CYBERPEACE INSTITUTE – «Cyber threats landscape». Consultado em: 14 de março de 2023. Disponível em: https://cyberconflicts.cyberpeaceinstitute.org/threats.

2 YIN, Robert K. – «Discovering the future of the case study: method in evaluation research». In *Evaluation practice*. Vol. 15, N.º 3, 1994, pp. 283-290.

3 YIN, Robert K. – *Estudo de Caso: Planejamento e Métodos*. 5.ª edição. Porto Alegre: Editora Bookman, 2014.

4 PARANHOS, Ranulfo, et al. – «Uma introdução aos métodos mistos». In *Sociologias*. Vol. 18, N.º 42, 2016, pp. 384-411.

5 CERVI, Emerson Urizzi – «Métodos quantitativos nas ciências sociais: uma abordagem alternativa ao fetichismo dos números e ao debate com qualitativistas». In *Pesquisa Social Reflexões: Teóricas e Metodológicas*. Ponta Grossa: Todapalavra Editora, 2009, pp. 125-144.

6 PARANHOS, Ranulfo, et al. – «Uma introdução aos métodos mistos», p. 388.

7 Para visitar os dados acesse: https://github.com/nepcri/CADN-2023.

8 KING, Gary – «Replicação, replicação». In *Revista Eletrônica de Ciência Política*. Vol. 6, N.º 2, 2015, pp. 382-401.

9 KING, Gary; KEOHANE, Robert O.; VERBA, Sidney – *Designing Social Inquiry: Scientific Inference in Qualitative Research*. 1.ª edição. New Jersey: Princeton University Press, 1994.

10 KONRAD, Kaiser David Vargas; LOURENÇÃO, Humberto José – «O conflito na Ucrânia entre 2014 e 2018 e seu impacto na segurança internacional». In *Brazilian Journal of Development*. Vol. 5, N.º 8, 2019, pp. 12906-12920.

11 PEREIRA COUTINHO, Francisco – «A agressão russa à Ucrânia e o direito internacional: uma tragédia em quatro atos». In *e-publica*. Lisboa. Vol. 10, N.º 1, 2023, pp. 4-17.

12 ZETTER, Kim – «An unprecedented look at stuxnet, the world's first digital weapon». Consultado em: 13 de abril de 2023. Disponível em: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

13 HOSANG, Alexandre – *Política Nacional de Segurança Cibernética: Uma Necessidade para o Brasil*. Consultado em: 16 de abril

de 2023. Disponível em: https://www.abeic.org.br/Admin/Publicacoes/29/PolNacSegCib.pdf.

14 O Manual de Tallinn é um documento estritamente normativo que visa a aplicabilidade da lei em conflitos cibernéticos e que ainda não é amplamente aceito no Sistema Internacional de Estados. Além disso, também temos a Convenção de Budapeste, que também não é aceita largamente pelos Estados.

15 CRUZ JÚNIOR, Samuel César – «A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual». Consultado em: 13 de abril de 2023. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/1590/1/TD_1850.pdf.

16 DAI GLOBAL, LLC – *Usaid Cybersecurity for Critical Infrastructure in Ukraine Review of the Regulatory Framework for Critical Infrastructure Cybersecurity in Ukraine: Legislative Assessment Report*. Consultado em: 9 de abril de 2023. Disponível em: https://pdf.usaid.gov/pdf_docs/PA00XX1T.pdf. Tradução livre a partir do original.

17 SPÎNU, Natalia – «Ukraine cybersecurity governance assessment». Consultado em: 9 de abril de 2023. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

18 TAQUARY SEGUNDO, Célio Borges – «A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos». Consultado em: 8 de abril de 2023. Disponível em: https://repositorio.esg.br/handle/123456789/1205.

19 LEHTO, Martti – «Cyber-attacks against critical infrastructure». In *Computational Methods in Applied Sciences*. Suíça: Springer, 2022. pp. 3-42. Tradução livre dos autores a partir do original.

20 LIMA, Pedro Arthur Linhares – «Segurança cibernética: a necessidade de se estruturar, sistematizar e integrar a proteção cibernética das infraestruturas críticas nacionais, órgãos estratégicos do Governo e Forças Armadas». Consultado em: 14 de abril de 2023. Disponível em: https://www.enabed2018.abedef.org/resources/anais/8/1534802448_ARQUIVO_Artigo-PedroALinharesLima-X-ENABED-SegurancaeDefesaCibernetica.pdf.

21 KONDRATOV, Sergiy, et al. – «Developing the critical infrastructure protection system in Ukraine: monograph». Kiev: National Institute For Strategic Studies, 2017. Consultado em: 14 de abril de 2023. Disponível em: https://niss.gov.ua/sites/default/files/2017-11/niss_Engl_findruk-0e9af.pdf. Tradução livre a partir do original.

22 *Ibidem*.

23 COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Council of European Union. Consultado em: 14 de abril de 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32008L0114.

24 SIGHOLM, Johan – «Non-State actors in cyberspace operations». Consultado em: 14 de abril de 2023. Disponível em: https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations.

25 «ATAQUE CIBERNÉTICO atinge provedora de telecomunicações ucraniana, dizem autoridades». CNN Brasil. Consultado em: 13 de abril de 2023. Disponível em: https://www.cnnbrasil.com.br/internacional/ataque-cibernetico-atinge-provedora-de-telecomunicacoes-ucraniana-dizem-autoridades/.

26 COIMBRA, Sara – «Ameaças e vulnerabilidades à segurança da informação dos sistemas de informação da Força Aérea». Consultado em: 8 de abril de 2023. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/24931/1/10_CapSara-Coimbra_TII_VF.pdf.

27 DANTAS, Marcus Leal – *Segurança da Informação: Uma Abordagem Focada em G de Riscos*. 1.ª edição. Olinda: Livro Rápido, 2011.

28 CAVELTY, Myriam Dunn – «Cyberwar: concept, status quo, and limitations». In *ETH Zurich*. Zurique. Vol. 71, 2010, pp. 1-3.

29 AUTY, Caroline – «Political hacktivism: tool of the underdog or scourge of cyberspace?». In *Aslib Proceedings*. Vol. 56, N.º 4, 2023, pp. 212-221.

30 MELLO, Fábio P.; MENDES JÚNIOR, Ricardo da C.; ROCHA, Daniel G. – *Análise de Ataques DDoS*. Rio de Janeiro: Instituto Militar de Engenharia. 2010. Trabalho de Conclusão de Curso. Consultado em: 2 de abril de 2023. Disponível em: http://www.defesacibernetica.ime.eb.br/pub/repositorio/2010-Pinhao_Mendes_Daniel.pdf.

31 «APÓS APARENTE ataque, dois bancos retomam funcionamento na Ucrânia». CNN Brasil. Consultado em: 13 de abril de 2023. Disponível em https://www.cnnbrasil.com.br/internacional/ministerio-da-defesa-e-banco-ucranianos-sao-atingidos-por-possivel-ciberataque/.

32 «RUSSIA-BASED hacker group "XakNet" infiltrates Ukraine Finance Ministry». The Cyber Express. Consultado em: 14 de abril de 2023. Disponível em: https://thecyberexpress.com/hacker-xaknet-infiltrates-ukraine-ministry/.

33 SAILIO, Mirko; LATVALA, Outi-Marja; SZANTO, Alexander – «Cyber threat actors for the factory of the future». In *Applied Sciences*. Suíça. Vol. 10, N.º 12, 2020, p. 4334.

34 MACA, Oscar; ARCOS, Andrés Felipe; URCUQUI, Christian – «Security control for website defacement». In *Sistemas y Telemática*. Colômbia. Vol. 15, N.º 41, 2017, pp. 45-55.

35 MEYER, Eric; MONTOYA, Michael – «Como proteger a infraestrutura crítica contra ataques cibernéticos». Consultado em: 14 de abril de 2023. Disponível em: https://www.securityreport.com.br/overview/como-proteger-a-infraestrutura-critica-contra-ataques-ciberneticos/#.ZDmksXbMLrd.

BIBLIOGRAFIA

«APÓS APARENTE ataque, dois bancos retomam funcionamento na Ucrânia». CNN Brasil. Consultado em: 13 de abril de 2023. Disponível em https://www.cnnbrasil.com.br/internacional/ministerio-da-defesa-e-banco-ucranianos-sao-atingidos-por-possivel-ciberataque/.

«ATAQUE CIBERNÉTICO atinge provedora de telecomunicações ucraniana, dizem autoridades». CNN Brasil. Consultado em: 13 de abril de 2023. Disponível em: https://www.cnnbrasil.com.br/internacional/ataque-cibernetico-atinge-provedora-de-telecomunicacoes-ucraniana-dizem-autoridades/.

AUTY, Caroline – «Political hacktivism: tool of the underdog or scourge of cyberspace?». In *Aslib Proceedings*. Vol. 56, N.º 4, 2023, pp. 212-221.

CAVELTY, Myriam Dunn – «Cyberwar: concept, status quo, and limitations». In *ETH Zurich*. Zurique. Vol. 71, 2010, pp. 1-3.

CERVI, Emerson Urizzi – «Métodos quantitativos nas ciências sociais: uma abordagem alternativa ao fetichismo dos números e ao debate com qualitativistas». In *Pesquisa Social Reflexões: Teóricas e Metodológicas*. Ponta Grossa: Todapalavra Editora, 2009, pp. 125-144.

COIMBRA, Sara – «Ameaças e vulnerabilidades à segurança da informação dos sistemas de informação da Força Aérea». Consultado em: 8 de abril de 2023. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/24931/1/10_CapSara-Coimbra_TII_VF.pdf.

COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Council of European Union. Consultado em: 14 de abril de 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32008L0114.

CRUZ JÚNIOR, Samuel César – «A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual». Consultado em: 13 de abril de 2023. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/1590/1/TD_1850.pdf.

CYBERPEACE INSTITUTE – «Cyber threats landscape». Consultado em: 14 de março de 2023. Disponível em: https://cyberconflicts.cyberpeaceinstitute.org/threats.

DAI GLOBAL, LLC – *Usaid Cybersecurity for Critical Infrastructure in Ukraine Review of the Regulatory Framework for Critical Infrastructure Cybersecurity in Ukraine: Legislative Assessment Report*. Consultado em: 9 de abril de 2023. Disponível em: https://pdf.usaid.gov/pdf_docs/PA00XX1T.pdf.

DANTAS, Marcus Leal – *Segurança da Informação: Uma Abordagem Focada em G de Riscos*. 1.ª edição. Olinda: Livro Rápido, 2011.

HOSANG, Alexandre – *Política Nacional de Segurança Cibernética: Uma Necessidade para o Brasil*. Consultado em: 16 de abril de 2023. Disponível em: https://www.abeic.org.br/Admin/Publicacoes/29/PolNacSegCib.pdf.

KING, Gary – «Replicação, replicação». In *Revista Eletrônica de Ciência Política*. Vol. 6, N.º 2, 2015, pp. 382-401.

KING, Gary; KEOHANE, Robert O.; VERBA, Sidney – *Designing Social Inquiry: Scientific Inference in Qualitative Research*. 1.ª edição. New Jersey: Princeton University Press, 1994.

KONDRATOV, Sergiy; BOBRO, Dmytro; HORBULIN, Volodymyr; SUKHODOLIA, Oleksandr; IVANIUTA, Serhii; NASVIT, Oleh; BIRIUKOV, Dmytro; RIABTSEV, Genadiy – «Developing the critical infrastructure protection system in Ukraine: monograph». Kiev: National Institute For Strategic Studies, 2017. Consultado em: 14 de abril de 2023. Disponível em: https://niss.gov.ua/sites/default/files/2017-11/niss_Engl_findruk-0e9af.pdf.

KONRAD, Kaiser David Vargas; LOURENÇÃO, Humberto José – «O conflito na Ucrânia entre 2014 e 2018 e seu impacto na segurança internacional». In *Brazilian Journal of Development*. Vol. 5, N.º 8, 2019, pp. 12906-12920.

LEHTO, Martti – «Cyber-attacks against critical infrastructure». In *Computational Methods in Applied Sciences*. Suíça: Springer, 2022, pp. 3-42.

LIMA, Pedro Arthur Linhares – «Segurança cibernética: a necessidade de se estruturar, sistematizar e integrar a proteção cibernética das infraestruturas críticas nacionais, órgãos estratégicos do Governo e Forças Armadas». Consultado em: 14 de abril de 2023. Disponível em: https://www.enabed2018.abedef.org/resources/anais/8/1534802448_ARQUIVO_Artigo-PedroALinharesLima-X-ENABED-SegurancaeDefesaCibernetica.pdf.

MACA, Oscar; ARCOS, Andrés Felipe; URCUQUI, Christian – «Security control for website defacement». In *Sistemas y Telemática*. Colômbia. Vol. 15, N.º 41, 2017, pp. 45-55.

MELLO, Fábio P.; MENDES JÚNIOR, Ricardo da C.; ROCHA, Daniel G. – *Análise de Ataques DDoS*. Rio de Janeiro: Instituto Militar de Engenharia. 2010. Trabalho de Conclusão de Curso. Consultado em: 2 de abril de 2023. Disponível em: http://www.defesacibernetica.ime.eb.br/pub/repositorio/2010-Pinhao_Mendes_Daniel.pdf.

MEYER, Eric; MONTOYA, Michael – «Como proteger a infraestrutura crítica contra ataques cibernéticos». Consultado em: 14 de abril de 2023. Disponível em: https://www.securityreport.com.br/overview/como-proteger-a-infraestrutura-critica-contra-ataques-ciberneticos/#.ZDmksXbMLrd.

PARANHOS, Ranulfo; FIGUEIREDO FILHO, Dalson Britto; ROCHA, Enivaldo Carvalho da; SILVA JÚNIOR, José Alexandre da; FREITAS, Diego – «Uma introdução aos métodos mistos». In *Sociologias*. Vol. 18, N.º 42, 2016, pp. 384-411.

PEREIRA COUTINHO, Francisco – «A agressão russa à Ucrânia e o direito internacional: uma tragédia em quatro atos». In *e-publica*. Lisboa. Vol. 10, N.º 1, 2023, pp. 4-17.

«RUSSIA-BASED hacker group "XakNet" infiltrates Ukraine Finance Ministry». The Cyber Express. Consultado em: 14 de abril de 2023. Disponível em: https://thecyberexpress.com/hacker-xaknet-infiltrates-ukraine-ministry/.

SAILIO, Mirko; LATVALA, Outi-Marja; SZANTO, Alexander – «Cyber threat actors for the factory of the future». In *Applied Sciences*. Suíça. Vol. 10, N.º 12, 2020, p. 4334.

SIGHOLM, Johan – «Non-State actors in cyberspace operations». Consultado em: 14 de abril de 2023. Disponível em: https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations.

SPÎNU, Natalia – «Ukraine cybersecurity governance assessment». Consultado em: 9 de abril de 2023. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

TAQUARY SEGUNDO, Célio Borges – «A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos». Consultado em: 8 de abril de 2023. Disponível em: https://repositorio.esg.br/handle/123456789/1205.

YIN, Robert K. – «Discovering the future of the case study: method in evaluation research». In *Evaluation practice*. Vol. 15, N.º 3, 1994, pp. 283-290.

YIN, Robert K. – *Estudo de Caso: Planejamento e Métodos*. 5.ª edição. Porto Alegre: Editora Bookman, 2014.

ZETTER, Kim – «An unprecedented look at stuxnet, the world's first digital weapon». Consultado em: 13 de abril de 2023. Disponível em: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Marco zero
As origens da guerra cibernética orquestrada pelos Estados Unidos para atingir a República Islâmica do Irã (2007-2010)[1]

Fernando H. Casalunga | *Eduardo Munhoz Svartman* | *Bruno Cardoso Reis*

INTRODUÇÃO

Ao passo em que cada vez mais casos envolvendo o uso do poder cibernético em conflitos interestatais, seja para realizar campanhas de reconhecimento e informação, otimizar ou comprometer sistemas operacionais militares e/ou civis de infraestruturas físicas, e/ou impactar de modo significativo a moral doméstica dos alvos atingidos vêm à tona, cresce a demanda por estudos capazes de compreender a origem do interesse dos Estados pelo desenvolvimento de capacidades táticas e operacionais neste domínio[2].

Ante ao desafio, é ponto pacífico que o problema da segurança cibernética está a exercer função ambivalente sobre as decisões estratégicas dos Estados, pois, se por um lado é preciso mitigar os riscos à segurança do funcionamento das infraestruturas críticas, por outro é necessário reconhecer que este novo domínio tem se destacado como um novo engenho de força capaz de ampliar as possibilidades de projetar poder em conflitos interestatais[3].

Frente ao cenário, as instituições securitárias norte-americanas apontam para o ciberespaço[4] como um domínio estratégico que requer o desenvolvimento de capacidades não apenas para assegurar o funcionamento adequado dos sistemas de informação responsáveis por controlar setores de infraestrutura crítica, mas, sobretudo, oferecer

RESUMO

Neste artigo realizamos um estudo de caso-único do conflito desencadeado entre os Estados Unidos e a República Islâmica do Irã (2007-2010), sob a perspectiva dos retornos estratégicos auferidos em função do uso da tecnologia da informação para atingir setores de infraestrutura crítica. Nossa análise destaca as condições que permitiram aos norte-americanos ampliarem as capacidades de projeção de poder sobre o seu adversário, fatores significativos para explicar a origem e o impacto da guerra cibernética nos dias atuais. A partir da coleta de evidências que revelam o funcionamento do mecanismo das operações orquestradas por atores estatais e não estatais para conter o programa nuclear iraniano, verificamos como o ciberespaço se tornou um domínio chave para a consecução de objetivos estratégicos nacionais. Por este prisma, com base em fontes primárias e secundárias utilizamos técnicas de análise qualitativa para responder à seguinte questão: como os Estados Unidos utilizaram o ciberespaço para atingir o programa nuclear iraniano?

Palavras-chave: guerra cibernética, poder nacional, tecnologia da informação, código malicioso.

→

 https://doi.org/10.23906/ri2024.82a06

ABSTRACT

GROUND ZERO: THE ORIGINS OF THE UNITED STATES'S CYBER WAR AGAINST THE ISLAMIC REPUBLIC OF IRAN (2007-2010)

In this article, we conduct a single-case study of the conflict between the United States and the Islamic Republic of Iran (2007–10), from the perspective of the strategic returns obtained through the use of information technology to achieve criticism of infrastructure sectors. Our analysis highlights the conditions that allowed the North Americans to expand their power projection capabilities over their adversary, significant factors in explaining the origin and impact of cyber warfare today. By collecting evidence that reveals the functioning of the operational mechanism orchestrated by state and non-state actors to contain the Iranian nuclear program, we verify how cyberspace has become a key domain for achieving national strategic objectives. From this perspective, based on primary and secondary sources, we use qualitative analysis techniques to answer the following question: how did the United States use cyberspace to target the Iranian nuclear program?

Keywords: cyber warfare, national power, information technology, malicious code.

alternativas efetivas ao uso da força que não ultrapassem os limites tradicionais da guerra[5].

Diretamente conectada ao nível do poder nacional, a operação Jogos Olímpicos (2007-2010), atribuída aos Estados Unidos e Israel, afetou o programa nuclear iraniano minando as capacidades físicas e psicológicas do alvo por intermédio de campanhas de reconhecimento e exploração que resultaram no primeiro ataque cibernético cinético documentado[6].

Nesta pesquisa destacamos as condições que proporcionaram a constituição desta operação com intuito de oferecer resposta ao seguinte questionamento: como os Estados Unidos utilizaram o ciberespaço para atingir o programa nuclear iraniano? À vista disso, nosso desenho de pesquisa segue uma abordagem qualitativa para examinar o processo de uso do ciberespaço para projeção de poder nacional com base em evidências que revelam o mecanismo de ação interagências que se encontra no bojo da guerra cibernética[7].

A partir do exame de relatórios técnicos, artigos de jornal e documentos oficiais, nossa análise destaca dois fatores que permitiram aos Estados Unidos ampliarem a magnitude da assimetria de poder ante um adversário regional. Para tanto, o artigo está dividido em três seções, as quais examinam: *i*) o contexto histórico que envolve a relação entre estes adversários; *ii*) a complexidade da operação Jogos Olímpicos; *iii*) a mudança institucional na estrutura de força norte-americana.

Nossa contribuição para o campo de estudos de política internacional e defesa é marcada por ilustrar como o problema da segurança cibernética se tornou fulcral para as disputas interestatais contemporâneas. Ademais, aspiramos lançar luz sob o obscuro funcionamento do mecanismo que regula o uso do ciberespaço para consecução de objetivos estratégicos nacionais.

CONTEXTO HISTÓRICO

Com intuito de compreender as razões que colocaram os interesses norte-americanos e iranianos em rota de colisão é preciso considerar, ainda que de modo sucinto, as nuances que constituem a historicidade das relações exteriores entre estes países. Território com recursos energéticos naturais em abundância, a atual República Islâmica

do Irã esteve por mais de cinco décadas sob controle da dinastia Pahlavi, e foi durante o governo de Reza Xá Pahlavi (1925-1941) que, em 1935, o antigo reino da Pérsia foi reconhecido internacionalmente como Irã[8].

A monarquia constitucional perdurou até 1953, data em que Mohammad Reza Pahlavi, com o apoio de instituições de inteligência dos Estados Unidos, comandou um golpe de Estado que depôs Mohamed Mossadegh. Com isso, um regime autocrata foi estabelecido, dando início, dentre outras medidas, ao programa nuclear vinculado ao projeto norte-americano «Átomos para a Paz»[9] que visava alavancar o desenvolvimento internacional de tecnologia nuclear para fins de produção energética[10].

Ao longo dos anos 1960, na medida em que os norte-americanos ampliavam sua influência internacional, as relações entre estes dois Estados se fortaleciam e, em 1968, o Irã se torna signatário do Tratado de Não Proliferação de Armas Nucleares reforçando o interesse político em estreitar laços com as nações ocidentais[11]. Contudo, o processo de convulsão social que culminou na derrocada do antigo regime abalou este equilíbrio. Longe do escopo desta pesquisa examinar os meandros da Revolução Iraniana (1977--1979), cabe ressaltar que, em janeiro de 1979, estudantes islâmicos que haviam invadido a Embaixada dos Estados Unidos, em Teerã, provocaram forte tensão nas relações externas com os norte-americanos, 52 pessoas foram mantidas reféns durante a ocupação que perdurou por mais de um ano[12].

A fim de arrefecer as tensões, o conselho regente e o então primeiro-ministro Shapour Bakhtiar decidem convidar o mentor intelectual do movimento, Ruhollah Khomeini, a regressar do exílio imposto em 1964. O retorno do aiatolá e a posterior proclamação da República Islâmica do Irã, em 1979, da qual se tornou o Líder Supremo, culminou numa série de reformas que incidiram sobre as instituições civis e militares iranianas, dentre as quais, o abandono do programa nuclear[13].

A Administração Khomeini foi marcada por forte instabilidade política no Oriente Médio, a guerra travada com o Iraque (1980-1988) teve forte impacto sobre as capacidades militares iranianas ao longo do conflito. Com a morte de Khomeini um ano após o término oficial da guerra, Ali Khamenei assume o poder central. Dentre outras medidas, o novo Líder Supremo inicia o Plano AMAD (1989-2003), um conjunto de projetos para desenvolvimento e produção de tecnologia nuclear com finalidade civil e militar denominado[14].

A Administração Khamenei promove uma política externa independente que procura se aproximar com a Federação Russa no intuito de recompor o poderio bélico desgastado durante a guerra, na prática, selando o distanciamento entre o Irã e as nações ocidentais. Com a virada do século, as relações russo-iranianas se estreitaram e, em 2001, o Presidente russo Vladimir Putin tornou pública sua intenção em comercializar armas e tecnologia energética nuclear para fins pacíficos com o Irã[15].

Deste ponto em diante, as críticas da comunidade ocidental ao programa nuclear iraniano se asseveraram. Em setembro de 2002, o discurso proferido pelo Presidente

norte-americano George W. Bush classificou o Irã como um adversário pertencente ao chamado «Eixo do Mal», ao lado de Iraque e da Coreia do Norte, considerando o Estado uma ameaça à segurança internacional[16].

Neste ínterim, o sigilo em torno da construção de complexos nucleares no Irã aumentou a preocupação das agências de controle internacional que passaram a exercer pressão para monitorar suas atividades. Os iranianos permitiram que a Agência Internacional de Energia Atômica inspecionasse as instalações em 2003, por conseguinte, os relatórios publicados registraram evidências de que os processos realizados nas instalações violavam as normativas do Tratado de Não Proliferação de Armas Nucleares, em efeito, o programa nuclear foi paralisado novamente[17].

AO DELIMITAR O DESENVOLVIMENTO DE ENERGIA NUCLEAR COMO PRIORIDADE ESTRATÉGICA, A ADMINISTRAÇÃO AHMADINEJAD (2005-2013) CRIOU UM IMPASSE COM OS ESTADOS UNIDOS QUE TORNOU IRREPARÁVEL A EQUALIZAÇÃO DOS INTERESSES DE AMBOS NO ORIENTE MÉDIO.

Todavia, dois anos depois, após vencer as eleições presidenciais, Mahmmoud Ahmadinejad reativa o programa e firma um novo acordo para conclusão do complexo de Bushehr com a Federação Russa. Ao delimitar o desenvolvimento de energia nuclear como prioridade estratégica, a Administração Ahmadinejad (2005-2013) criou um impasse com os Estados Unidos que tornou irreparável a equalização dos interesses de ambos no Oriente Médio.

Destarte, a Agência Internacional de Energia Atômica e a comunidade de inteligência norte-americana apresentaram relatórios contendo evidências de que o Irã estaria empenhado em produzir artefatos bélicos nucleares[18]. Frente ao cenário, em 2006, a tensão aumentou e o Estado de Israel se uniu aos Estados Unidos nas críticas aos iranianos[19]. À altura o recurso à força tradicional foi descartado e, num esforço conjunto entre os Estados Unidos, a Organização das Nações Unidas (ONU) e a União Europeia (UE), sanções diplomáticas e econômicas foram aplicadas ao Irã. As resoluções adotadas pelo Conselho de Segurança das Nações Unidas exigiam a suspensão do programa de enriquecimento de urânio, o cumprimento dos protocolos internacionais e a constituição de controles financeiros e de exportação de materiais[20].

Conquanto, tais ações não produziram os efeitos esperados e a classe política norte-americana passou a considerar o uso de medidas alternativas para lidar com a ameaça iraniana. Em efeito, conforme veremos na seção seguinte, uma forma inédita de demonstração do poder nacional veio à tona.

GUERRA CIBERNÉTICA: A OPERAÇÃO JOGOS OLÍMPICOS (2007-2010)

Nesta seção, a fim de compreender de forma substantiva os efeitos da guerra cibernética, examinamos o ataque que atingiu setores de infraestrutura crítica do complexo nuclear de Natanz (2009-2010) no Irã em seu contexto mais amplo, na qualidade de uma operação especial que se constituiu numa cadeia de eventos interconectados que

aproximaram campanhas de reconhecimento e exploração de sistemas de informação e uso da força militar[21], considerada condição suficiente para o uso efetivo do ciberespaço para projeção de poder nacional.

De acordo com o projeto inicial, o complexo nuclear de Natanz deveria abrigar cerca de 50 mil centrífugas de enriquecimento de urânio, porém, até 2010, menos de 20% haviam sido instaladas[22], estimativas apontaram que entre 2008 e 2009 cerca de nove mil estavam operantes em Natanz[23].

Sem embargo, um acontecimento chamou a atenção da comunidade de segurança internacional quando ao menos mil delas foram substituídas sem quaisquer motivos oficialmente reportados[24]. A resposta ao enigma seria dada nos anos seguintes, através de relatórios que apresentaram evidências de que um ataque cibernético orquestrado por adversários do Irã interessados em frustrar o andamento do programa nuclear havia atingido o complexo[25].

Conforme as informações que vieram à tona a preocupação com a vulnerabilidade de sistemas de controle que operam processos críticos em infraestruturas industriais passou ao centro da agenda de instituições securitárias ao redor do mundo que buscavam compreender a configuração dos ataques, as armas utilizadas e seus efeitos[26].

Descoberto em junho de 2010, o código malicioso, posteriormente denominado «Stuxnet», fora projetado para intervir na capacidade de monitoramento e controle de processos industriais de sistemas complexos, causando falhas sequenciais que provocaram o colapso de estruturas físicas[27]. Sua identificação constitui o primeiro registro de uma arma cibernética capaz de produzir danos cinéticos.

Análises apontaram que os criadores do código possuíam conhecimento avançado sobre os parâmetros de funcionamento de sistemas ciberfísicos[28], outrossim, indicaram que a atuação conjunta entre os invasores e agências de espionagem proporcionou o acesso a informações sigilosas sobre a divisão e operação das centrífugas de Natanz. Com intuito de danificá-las, os controladores lógicos programáveis (PLC) da Siemens Simatic S7-300 (CPU 315)[29] foram estabelecidos como os principais alvos, para acessá-los, os atacantes exploraram uma ampla gama de vulnerabilidades desconhecidas de «dia-zero»[30] e invadiram os sistemas de *software* Windows da Microsoft e de supervisão e aquisição de dados (SCADA) da Siemens (SIMATIC WinCC/Step7)[31] instalados em computadores dos operadores do complexo[32].

Uma vez dentro do alvo, de forma discreta, o código malicioso executava por alguns dias uma série de rotinas de reconhecimento para mimetizar o funcionamento adequado dos rotores, em sequência, alterava periodicamente a frequência dos motores elétricos que acionavam as centrífugas e, concomitantemente, enviava informações de verificação de rotina aos operadores indicando que o processo estava sendo realizado de modo correto[33].

Ao final de 2009 o código malicioso havia afetado o módulo A26, causando falhas sequenciais em 11 cascatas interconectadas, a invasão comprometeu o funcionamento da CPU da Siemens que enviava informações aos PLC. Utilizando credenciais de acesso

remoto subtraídos das empresas RealTek e JMicron, ambas localizadas em Taiwan, os invasores foram capazes de alterar o funcionamento das centrífugas levando ao colapso ao menos mil delas, sem que os operadores tivessem conhecimento de que estavam sob ataque[34].

A análise do código malicioso chamou a atenção dos especialistas em tecnologia da informação devido à quantidade de vulnerabilidades desconhecidas utilizadas para alterar a funcionalidade dos PLC de modo imperceptível aos sensores de vigilância, ao longo das investigações quatro delas foram identificadas. Igualmente, a precisão do artefato surpreendeu, uma vez que a sabotagem ocorria apenas quando um PLC específico, conectado a um determinado tipo de dispositivo, e operando dentro de parâmetros pré-estabelecidos era identificado[35].

Cientes da ausência de conexão com redes externas nas instalações da usina, os construtores da arma cibernética a equiparam com uma vasta quantidade de informação para que pudesse atingir o alvo sem que fosse necessário qualquer comando externo para executá-lo[36]. Todavia, a engenharia por detrás de sua construção não foi o único tópico que chamou a atenção.

Análises posteriores verificaram que sua produção envolveu cerca de dez mil horas de trabalho, considerando a participação de especialistas com conhecimento avançado em interfaces operacionais da Microsoft, bem como de linguagem de gerenciamento de sistemas industriais complexos[37]. Desde a fase de experimentos até sua execução, o processo envolveu o esforço conjunto de mais de 30 programadores, a um custo de cerca de três milhões de dólares, recursos humanos e técnicos que auxiliaram na aquisição de informações sobre o funcionamento interno do complexo de Natanz, e implantação da arma nos computadores de operadores do complexo[38].

Após a ampla divulgação do Stuxnet, novas amostras derivadas de seu código fonte foram registradas revelando a complexidade desta operação, dentre as mais significativas estão os códigos maliciosos Duqu[39] e Flame[40] capazes de agir furtivamente sem que sua presença pudesse ser detectada.

As avaliações identificaram que a estrutura e os mecanismos internos de infecção do Duqu eram similares as do Stuxnet, utilizando certificados legítimos de acesso remoto de empresas privadas para enviar informações e receber comandos remotos dos invasores durante o período de exploração dos sistemas infectados. Já o Flame se propagava localmente explorando vulnerabilidades em impressoras conectadas em redes, permitindo aos invasores que obtivessem certificados legítimos indetectáveis pelos sistemas de segurança, tal qual o código original[41].

Ambos empregavam técnicas avançadas de criptografia computadorizada e foram utilizados para fins de espionagem cibernética, coletando dados confidenciais sobre a estrutura e os métodos operacionais das instalações nucleares de Natanz, movimentos que confirmaram as suspeitas de que os invasores detinham informações sobre o funcionamento interno dos equipamentos da usina e horário de trabalho dos operadores[42].

No entanto, embora tenha atrasado o programa nuclear do Irã em quase um ano, a operação não o deteve completamente, uma vez que as centrífugas danificadas foram gradativamente substituídas e as atividades retomadas[43]. Por outro ângulo, agentes securitários norte-americanos atestam que o objetivo da operação era produzir efeitos dissuasórios demonstrando aos iranianos a permeabilidade de seus sistemas operacionais[44].

Destarte, fatores como a desconfiança quanto à presença de espiões atuando em setores críticos e a possibilidade de que outros sistemas operacionais de infraestrutura de rede estivessem comprometidos, podem ter «diminuído a capacidade do Irã de adquirir poderio bélico nuclear em até dois anos – significativamente mais do que o tempo necessário para substituir as centrífugas danificadas»[45].

Não obstante, a operação quebrou o paradigma vigente dos conflitos interestatais ao demonstrar um elevado grau de precisão no uso do poder cibernético para provocar danos cinéticos de modo discreto e eficiente, fato inédito até aquele momento[46]. Por essa lógica, se tornou axiomático que os norte-americanos inauguram uma nova fase de conflitos, a qual se estabelece mediante o uso de armas cibernéticas que possuem riscos gerenciáveis e podem produzir efeitos cinéticos sem infringir os códigos internacionais de conflito armado[47].

FRENTE À DINÂMICA, A ESPIONAGEM CIBERNÉTICA EMERGE COMO OPÇÃO VALIOSA PARA PROMOVER OS INTERESSES NACIONAIS.

Frente à dinâmica, a espionagem cibernética emerge como opção valiosa para promover os interesses nacionais, pois, ainda que possamos considerar os ataques cibernéticos disruptivos e a espionagem como atividades distintas, é inegável que o uso de vetores de intrusão similares para penetrar os alvos de modo furtivo macula a linha divisória que as separa[48].

A operação permitiu que aspectos outrora puramente teóricos do fenômeno pudessem ser observados em um caso concreto, examinado e documentado por especialistas das mais diversas áreas relacionadas à segurança cibernética, condição que contribuiu para avanços na fronteira do conhecimento do uso potencial da guerra cibernética na dinâmica dos conflitos interestatais[49]. Mais do que isso, modificou a forma como as comunidades acadêmicas e de segurança passaram a enxergar a realidade objetiva das ameaças provenientes do ciberespaço, uma vez que os mecanismos de segurança vigentes se provaram insuficientes.

Frente ao exposto, naquilo que tangencia a relevância acadêmica e securitária da operação, se faz *mister* compreender como se deu o processo de mudança institucional nas forças de segurança nacional dos Estados Unidos para promover os incentivos necessários para seu desenvolvimento e posterior execução. Com base na análise de fontes oficiais, a próxima seção destaca a incorporação do domínio cibernético à estrutura de defesa norte-americana com vistas à projeção de poder nacional.

OS EFEITOS DA OPERAÇÃO JOGOS OLÍMPICOS NAS INSTITUIÇÕES SECURITÁRIAS NORTE-AMERICANAS

Nesta seção verificamos os efeitos institucionais da operação Jogos Olímpicos com base na análise de documentos oficiais, produzidos anterior e posteriormente ao fenômeno (2003-2011). O material analisado contém evidências do processo de mudança pelo qual passaram as instituições securitárias norte-americanas ao incorporarem o ciberespaço como um novo domínio de guerra, considerada condição necessária para seu uso efetivo e discreto.

Conter o programa nuclear iraniano e, assim, evitar que o país consiga obter acesso a armas de destruição em massa (ADM) que poderiam abalar o equilíbrio estratégico securitário no Oriente Médio se converteu em objetivo estratégico declarado dos Estados Unidos na primeira década deste século[50].

Neste ensejo, em 25 de novembro de 2002, a Lei de Segurança Interna promulgada pelo então Presidente George W. Bush deu origem ao Departamento de Segurança Interna (DHS), entidade constituída por vinte e duas entidades federais. Com a finalidade de se tornar o «centro federal de excelência para segurança cibernética e servir de ponto nodal da articulação entre instituições federais, estaduais, locais e não-governamentais, incluindo o setor privado, a academia e o público»[51], dentre as suas mais diversas atribuições, se destacam a coordenação de informações interagências e o fomento à pesquisa e ao desenvolvimento científico-tecnológico.

O documento formaliza a alvorada das transformações na estrutura de defesa cibernética norte-americana, dotada de forte inclinação colaborativa, por essa lógica, orienta o DHS a promover incentivos ao fortalecimento das capacidades de contenção de ameaças cibernéticas que possam afetar o funcionamento de processos industriais. A fim de mitigá-las prevê o fomento à atuação conjunta entre instituições públicas e privadas em quatro componentes do ciberespaço: «mecanismos da Internet; DCS/SCADA; correção de vulnerabilidades de *software* e *hardware*; infraestrutura física e interdependência»[52].

No que concerne à identificação e correção de vulnerabilidades em sistemas de controle industrial, frisa que códigos maliciosos representam desafios com potencial para causar danos graves ao funcionamento das infraestruturas críticas ao explorarem aberturas desconhecidas a fim de comprometer processos que regulam o funcionamento de sistemas DCS/SCADA[53].

O documento promove a cooperação entre agências de segurança e o Departamento de Defesa para coordenar pesquisas direcionadas: a proteção de setores críticos de infraestrutura, divulgação de informações, avaliação de ameaças externas às redes e sistemas de informação nacional, e investigação de crimes cibernéticos. Dentre as estruturas institucionais públicas responsáveis, destaca o Escritório de Ciência e Tecnologia, Departamento de Estado, Central de Inteligência, Departamento de Justiça e o FBI, os centros de compartilhamento e análise de informações e de resposta a emergências de computadores/centro de coordenação[54].

Por conseguinte, a Estratégia de Segurança Nacional (ESN) de 2006 assinala que o enfrentamento de novos desafios securitários depende da mudança institucional em curso, que tem na criação do DHS e instituições de inteligência seu pilar principal. O documento enfatiza os valores democráticos em oposição à tirania de grupos extremistas, tendo a liberdade e a justiça como chaves da jornada nacional de libertação dos povos: «Todas as tiranias ameaçam o interesse mundial na expansão da liberdade, e algumas, em sua busca por ADM ou patrocínio do terrorismo, ameaçam também nossos interesses imediatos de segurança»[55].

A primeira evidência da preparação de operações cibernéticas ofensivas no bojo das forças securitárias está registrada na definição dos meios necessários para conquistar os objetivos nacionais, os norte-americanos consideram agir com base no princípio da preempção no uso da força de forma controlada em ações justificáveis do ponto de vista estratégico para conter as ameaças, e citam o Irã como exemplo de Estado nocivo que objetiva adquirir artefatos nucleares e impõe restrições às liberdades políticas e religiosas aos seus cidadãos: «Nosso objetivo é convencer os adversários de que eles não podem atingir seus objetivos com ADM e, assim, dissuadi-los de tentar usar ou mesmo adquirir essas armas»[56].

OS NORTE-AMERICANOS CONSIDERAM AGIR COM BASE NO PRINCÍPIO DA PREEMPÇÃO NO USO DA FORÇA DE FORMA CONTROLADA EM AÇÕES JUSTIFICÁVEIS DO PONTO DE VISTA ESTRATÉGICO PARA CONTER AS AMEAÇAS, E CITAM O IRÃ COMO EXEMPLO DE ESTADO NOCIVO.

Tanto a ENPC (2003) quanto a ESN (2006) foram produzidas durante o período de gestação da operação Jogos Olímpicos e representam, pois, mudanças significativas que promoveram os primeiros incentivos de sua constituição. Na esteira destes documentos, a Estratégia de Defesa Nacional (EDN) de 2008 e a ESN de 2010, pontuam os meios com os quais as instituições securitárias deverão perseguir as diretrizes pré-estabelecidas.

O documento sublinha a existência de Estados desonestos como desafios de primeira ordem, e aponta para o Irã como um adversário que ameaça os interesses regionais norte-americanos devido à obscuridade de seu programa nuclear. Com intuito de resolver o problema, destaca a implementação de medidas cabíveis para assegurar a efetividade das operações militares, dentre as quais destaca aquelas com alto potencial dissuasório, mantidas abaixo do limiar da guerra tradicional: «os Estados Unidos irão, se necessário, agir preventivamente no exercício de seu direito de autodefesa para prevenir ou impedir atos hostis de nossos adversários»[57].

A segunda evidência se refere ao reconhecimento da existência de conflitos irregulares em andamento para os quais não há declaração tradicional que delimite seu início. Diante disso, os militares consideram prioritária a promoção do desenvolvimento de «capacidades de inteligência para detectar, reconhecer e analisar novas formas de guerra, bem como explorar abordagens e estratégias conjuntas para combatê-las»[58].

Por este ângulo, manifestam o interesse na incorporação de civis aos esforços da defesa, o conhecimento produzido por institutos de pesquisa e indústria é descrito como um componente significativo tanto para apoiar e garantir a efetividade das operações quanto evitar sua mobilização: «Esses desenvolvimentos exigirão uma compreensão ampliada de "conjunção", que combine perfeitamente capacidades e opções civis e militares»[59]. Ademais, dentre as metas traçadas para incrementar as capacidades da defesa, considera fulcral a parceria com o DHS que promova incentivos à constituição de operações de «penetração de redes terroristas e inteligência de medição e assinatura para identificar sistemas de distribuição de ADM»[60].

Ao final da Administração Bush (2001-2008) a operação Jogos Olímpicos foi considerada um recurso significativo para projeção de poder nacional e teve continuidade durante a administração de Barack H. Obama (2009-2017)[61]. Promulgada em maio de 2010, a ESN manteve a preocupação com proliferação de artefatos nucleares: «o maior perigo para o povo americano e para a segurança global continua a vir das ADM, particularmente o perigo representado pela busca de armas nucleares por extremistas violentos e sua proliferação para outros estados»[62].

O PROGRAMA NUCLEAR DO IRÃ É APONTADO COMO UM FATOR DE RISCO NÃO APENAS AOS SEUS VIZINHOS REGIONAIS, MAS A TODA COMUNIDADE INTERNACIONAL.

Novamente, o programa nuclear do Irã é apontado como um fator de risco não apenas aos seus vizinhos regionais, mas a toda comunidade internacional. Em vista disso, os norte-americanos reivindicaram a atitude responsiva da classe dirigente iraniana a fim de assegurar o reestabelecimento da confiança mútua, conquanto, não descartaram a possibilidade do uso de recursos estratégicos dissuasórios[63].

A terceira evidência se verifica nos indicativos da aproximação entre instituições públicas e privadas, presentes tanto na EDN (2008) quanto na ESN (2010) publicadas durante a fase sigilosa da operação Jogos Olímpicos que sugerem sua existência.

No mês seguinte daquele ano quando as informações da operação vieram a público, a engenharia institucional por detrás de sua constituição passou ao foco. Em efeito, as operações de proteção contra-ataques cibernéticos se tornaram fulcrais e o ciberespaço passou a ser considerado um domínio operacional, decisão que colocou a segurança cibernética no quadro de missões primárias do Departamento de Defesa.

Em 2011, a EDN reforçou a preocupação com a segurança cibernética e a proliferação de ADM patrocinada por Estados desonestos, como fator que colocava em questão a estabilidade regional e a segurança internacional. Nesse sentido, sublinhou a possibilidade de uso da força para impedir que o Irã obtivesse artefatos nucleares, fator que «poderia desencadear uma cascata de Estados na região em busca de paridade nuclear ou aumento das capacidades convencionais»[64].

Face ao problema, as capacidades das forças securitárias para operar no domínio cibernético ganharam relevo, em virtude disso, a quarta evidência se verifica na importância

conferida às operações dissuasórias, as quais deveriam ser orquestradas em conjunto com setores estratégicos de modo a encerrar a questão. O documento tonifica os incentivos à constituição de operações conjuntas para organizar a defesa ativa com base na cooperação interagências[65].

Diante do cenário, os militares assumem um compromisso com a produção de incentivos à cooperação entre atores estatais e não estatais para constituição de uma Força Conjunta, produto dos «comandos cibernético e estratégico, agências governamentais norte-americanas, entidades não governamentais, indústria e atores internacionais para desenvolver novas normas, capacidades, organizações e habilidades cibernéticas»[66], a fim de aprimorar os mecanismos de identificação e controle de ameaças.

Novamente, o programa nuclear do Irã foi considerado um desafio a ser superado mediante atuação das instituições securitárias nacionais e promoção de incentivos ao incremento das defesas de aliados e parceiros na região, a fim de conter o ímpeto iraniano em adquirir e/ou utilizar ADM os norte-americanos enfatizam a manutenção de «uma presença adequada capaz de tranquilizar parceiros e aliados e impedir que o Irã adquira armas nucleares»[67]. Por essa lógica, frisam o impacto tático da integração entre as capacidades operacionais militares e os esforços interagências para aquisição de informações por meio de campanhas de inteligência, vigilância e reconhecimento[68].

Com base no exame das fontes oficiais supracitadas, nossa análise registra efeitos permanentes da operação Jogos Olímpicos sobre a estrutura institucional securitária norte-americana, dentre as transformações promovidas, se destacam a criação do DHS, Comando Cibernético Norte-Americano, Força Conjunta, a Equipa de Resposta a Emergências Informáticas dos Estados Unidos, bem como sua atuação em conjunto com centros acadêmicos, setores da iniciativa privada e parceiros internacionais.

Ao explorarmos os meandros institucionais que deram origem ao fenômeno da guerra cibernética, nossa análise documental identifica as diretrizes e orientações normativas que promoveram transformações nas forças de segurança e defesa nacional norte-americanas, necessárias para garantir o uso discreto e efetivo da operação Jogos Olímpicos (2007-2010). Conforme exposto, os efeitos da criação de incentivos a constituição de movimentos desta natureza indicam não somente o nível de desenvolvimento do aparato científico e tecnológico norte-americano, mas, sobretudo, sua eficiência institucional. As evidências coletadas contribuem para sustentar o argumento de que os ataques cibernéticos que atingiram as instalações nucleares de Natanz compunham uma operação especial mais ampla, pioneira no emprego de armas cibernéticas em operações ofensivas.

CONCLUSÃO

Nesta pesquisa verificamos como o processo de mudança institucional pelo qual passaram as forças securitárias norte-americanas se conecta aos momentos críticos que culminaram no ataque cibernético às centrífugas de enriquecimento de urânio do complexo nuclear de Natanz (2009-2010).

Nossa análise identificou duas condições significativas para o emprego efetivo e discreto do ciberespaço com vistas à consecução de objetivos estratégicos dos Estados Unidos. Nesse ensejo, consideramos a operação Jogos Olímpicos um marco para os estudos de segurança por revelar o obscuro envolvimento de atores estatais e não estatais em atividades cibernéticas com consequências no mundo físico.

A operação permitiu que aspectos outrora puramente teóricos da guerra cibernética pudessem ser observados em um caso concreto, examinado e documentado por especialistas das mais diversas áreas relacionadas à defesa. De tal maneira que modificou a forma como as comunidades acadêmicas e de segurança passaram a enxergar a realidade objetiva das ameaças provenientes do ciberespaço.

Não obstante, a mudança nas instituições securitárias examinada teve efeito, sobretudo, sobre os processos de tomada de decisão, devido aos incentivos aos esforços interagências e a disponibilização de novos recursos militares moralmente superiores aos convencionais em termos de precisão e controle que permitiram à classe política norte-americana optar pelo domínio cibernético em detrimento de ataques cinéticos tradicionais para consecução de objetivos estratégicos nacionais.

Por fim, ao considerarmos a dinâmica política que circunscreve o uso do ciberespaço com intuito de auferir retornos assimétricos em um conflito regional, nossa análise enfatiza a adição de uma nova dimensão ao problema da segurança internacional, fruto da expansão dos métodos de uso da força para projeção de poder nacional disponível aos Estados, fatores que não podem ser explicados com base em conceitos tradicionais sobre a guerra. À vista disso, sublinhamos a configuração de uma nova realidade, ainda pouco explorada, que demanda esforços por parte de acadêmicos e agentes institucionais interessados em decodificar os enigmas da guerra cibernética. R:I

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Fernando H. Casalunga Investigador integrado do Centro de Estudos Estratégicos do Exército (CEEEx). Doutor em Ciência Política pela Universidade Federal do Rio Grande do Sul (UFRGS). Membro da Associação Brasileira de Estudos de Defesa. Atualmente desenvolve estudos sobre os impactos das instituições de inteligência no planejamento estratégico do Exército brasileiro.

> Centro de Estudos Estratégicos do Exército SMU, Brasília, DF, 70655-775, Brasil | fernandocasalunga@gmail.com

Eduardo Munhoz Svartman Professor do Departamento de Ciência Política da Universidade Federal do Rio Grande do Sul (UFRGS). Atualmente realiza estudos sobre o desenvolvimento do pensamento militar brasileiro e a introdução de sistemas de mísseis no Exército brasileiro.

> Universidade Federal do Rio Grande do Sul (UFRGS), Av. Bento Gonçalves, 9090, Agronomia, Porto Alegre, RS, 91540-000, Brasil | eduardo.svartman@ufrgs.com

Bruno Cardoso Reis Professor do Departamento de História e investigador integrado do Centro de Estudos Internacionais do Instituto Universitário de Lisboa (ISCTE). Doutor em War Studies pelo King's College. Atualmente desenvolve estudos comparados das guerras da descolonização, conflitos irregulares, grande estratégia e golpes militares.
> Instituto Universitário de Lisboa (ISCTE), Av. das Forças Armadas, 1649-026 Lisboa, Portugal | bruno.cardoso.reis@iscte-iul.pt

NOTAS

1 O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001 – no âmbito do programa PROPEX/Defesa edital n.º 14/2021.

2 KUMAR, Rajesh, et al. – «APT attacks on industrial control systems: a tale of three incidents». In *International Journal of Critical Infrastructure Protection*. Vol. 37, 2022, pp. 1-11.

3 BETZ, David J.; STEVENS, Tim – *Cyberspace and the State: Towards a Strategy for Cyber-Power*. 1.ª edição. Reino Unido: IISS Routledge, 2011.

4 Definição: domínio invisível da ação humana que se dá através de atividade eletromagnética com uso de tecnologias de informação e comunicação, se trata de um ambiente onde estão conectados e são controlados os mais diversos sistemas: financeiro, energético, transporte e telecomunicações que se constituem como infraestruturas onde ocorrem processos industriais complexos que são críticos para o funcionamento das sociedades e economias modernas. BUTRIMAS, Vytautas – «National security and international policy challenges in a post Stuxnet world». In *Lithuanian Annual Strategic Review*. Vol. 12, 2014, pp. 11-31. Consultado em: 8 de maio de 2023. Disponível em: https://kam.lt/wp-content/uploads/2022/03/lithuanian-annual-strategic-review-2013-2014-vol-12.pdf.

5 JENKINS, Ryan – «Is Stuxnet physical? Does it matter?». In *Journal of Military Ethics*. Vol. 12, N.º 1, 2013, pp. 68-79; JOLLEY, Jason – «Article 2(4) and cyber warfare: how do old rules control the brave new world?». In *International Law Research*. Vol. 2, N.º 1, 2013, pp. 1-16.

6 BRENNER, Joel – «Eyes wide shut: the growing threat of cyber attacks on industrial control systems». In *Bulletin of the Atomic Scientists*. Vol. 69, N.º 5, 2013, pp. 16-20; MILEVSKI, Lukas – Stuxnet and strategy: a special operation in cyberspace?». In *National Defense University Press*. Vol. 63, N.º 4, 2011, pp. 64-69. Consultado em: 25 de junho de 2023. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_64-69_Milevski.pdf?ver=Jy0SW9E8UBbatlrmrw-egQ%3D%3D.

7 MAHONEY, James – «The logic of process: tracing tests in the social sciences». In *Sociological Methods & Research*. Vol. 41, N.º 4, 2012, pp. 570-597; FALLETI, Tulia – «Process tracing of extensive and intensive processes». In *New Political Economy*. Vol. 21, N.º 5, 2016, pp. 455-462. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13563467.2015.1135550.

8 AZENHA, Pedro Jorge de Oliveira – «A Estratégia Nuclear Iraniana e os Desafios Colocados à Comunidade Internacional». Lisboa: Instituto de Estudos Superiores Militares, 2010. Trabalho de Investigação Individual. Consultado em: 25 de junho de 2023. Disponível em: https://comum.rcaap.pt/handle/10400.26/12674.

9 O programa lançado em 1953 durante a Administração Dwight Eisenhower, em discurso na Assembleia Geral das Nações Unidas, abriu caminho para a constituição da Agência Internacional de Energia Atômica, entidade responsável por regular a produção de energia nuclear para fins pacíficos e fomentar o desenvolvimento de pesquisas e formação de quadros qualificados. BERMÚDEZ, Àngel – «Programa nuclear do Irã: como EUA ajudaram o país a iniciar polêmico plano atômico». BBC News Brasil. 2021. Consultado em: 15 de março de 2023. Disponível em: https://www.bbc.com/portuguese/geral-59491973.

10 MORGADE, Alba – «EUA x Irã: o que originou a rivalidade de décadas entre os dois países». BBC News Brasil. 2020. Consultado em: 24 de março de 2023. Disponível em: https://www.bbc.com/portuguese/internacional-50983943.

11 BERMÚDEZ, Àngel – «Programa nuclear do Irã...».

12 MORGADE, Alba – «EUA x Irã...».

13 AZENHA, Pedro Jorge de Oliveira – «A Estratégia Nuclear Iraniana...».

14 ALBRIGHT, David; BURKHARD, Sarah – *Entering Dangerous, Uncharted Waters: Iran's 60 Percent Highly Enriched Uranium*. WA: Institute for Science and International Security. 2022. Consultado em: 12 de agosto de 2023. Disponível em: https://isis-online.org/isis-reports/detail/entering-uncharted-waters-irans-60-percent-highly-enriched-uranium.

15 AZENHA, Pedro Jorge de Oliveira – «A Estratégia Nuclear Iraniana...», p. 11.

16 BLINDER, Caio – «Discurso do "Eixo do Mal" assombra Bush». BBC News Brasil. 2006. Consultado em: 20 de março de 2023. Disponível em: https://www.bbc.com/portuguese/reporterbbc/story/2006/10/061012_caioblinderaw.

17 ALBRIGHT, David, et al. – *Preventing Iran from Obtaining Nuclear Weapons: Restricting its Future Nuclear Options*. WA: Institute for Science and International Security. 2012. Consultado em: 27 de março de 2023. Disponível em: https://isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf.

18 *Ibidem*.

19 Os Estados Unidos e Israel começaram a considerar secretamente opções militares para atrasar a nuclearização iraniana. O nó mais importante no programa de enriquecimento do Irã na época era Natanz, uma instalação remota 150 milhas ao sul de Teerã, que iniciou suas operações industriais em fevereiro de 2007. LINDSAY, Jon – «Stuxnet and the limits of cyber warfare». In *Security Studies*. Vol. 22, N.º 3, 2013, p. 20.

20 KELSEY, Davenport – «UN Security Council Resolution on Iran». Arms Control Association. 2022. Consultado em: 26 de abril de 2023. Disponível em: https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran.

21 LILIENTHAL, Gary; AHMAD, Nehaluddin – «Cyber-attack as inevitable kinetic war». In *Computer Law & Security Review*. Vol. 31, N.º 3, 2015, pp. 390-400.

22 ALBRIGHT, David, et al. – *Preventing Iran from Obtaining Nuclear Weapons*....

23 DE FALCO, Marco – *Stuxnet Facts Report: A Technical and Strategic Review*. TLL, EST: NATO Cooperative Cyber Defense Center of Excellence. 2012. Con-

sultado em: 8 de junho de 2023. Disponível em: https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/.

24 ZETTER, Kim – «How digital detectives deciphered Stuxnet: the most menacing malware in history». WIRED Security. 2011. Consultado em: 26 de junho de 2023. Disponível em: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

25 FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric – *W32.Stuxnet Dossier*. Symantec Security Response. Califórnia: Symantec Corporation World Headquarters, 2011. Atualizado em: fevereiro de 2011. Consultado em: 26 de junho de 2023. Disponível em: https://nsarchive.gwu.edu/document/21440-document-44.

26 COLLINS, Sean; MCCOMBIE, Stephen – «Stuxnet: the emergence of a new cyber weapon and its implications». In *Journal of Policing, Intelligence and Counter Terrorism*. Vol. 7, N.º 1, 2012, pp. 80-91.

27 FARWELL, James P.; ROHOZINSKI, Rafal – «The new reality of cyber war». In *Survival: Global Politics and Strategy*. Vol. 54, N.º 4, 2012, pp. 107-120.

28 Sistemas utilizados em processos que regulam o funcionamento das infraestruturas críticas compostos por três mecanismos principais: supervisão e aquisição de dados (SCADA), controle e distribuição (DCS) e controladores lógicos programáveis (PLC). Os dois primeiros utilizam os PLC programados por operadores com acesso autorizado para executar rotinas que produzem efeitos no mundo físico. NOURIAN, ARASH; MADNICK, Stuart – «A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet». In *IEEE Transactions on Dependable and Secure Computing*. Vol. 15, N.º 1, 2018, pp. 2-13. Consultado em: 15 de junho de 2023. Disponível em: https://ieeexplore.ieee.org/document/7360168.

29 Componentes do PLC: CPU, memória e portas de entrada/saída utilizadas para ler comandos externos, ativar ou desativar impulsor de energia, exibir informações, receber comandos e ser programado. DE FALCO, Marco – *Stuxnet Facts Report…*.

30 Definição: vulnerabilidades extremamente raras e de difícil exploração que ainda não são conhecidas por fabricantes de um determinado *software* ou pelos fornecedores de antivírus. ZETTER, Kim – «How digital detectives deciphered Stuxnet…».

31 Definição: *software* Siemens que permite construir o «projeto» que contém os metadados da configuração do PLC; o passo 7 é o que permite enviar os dados para a CPU do PLC, permite a inserção do código em formato STL que envia comandos funcionais ao PLC. WinCC: software Siemens que opera em computadores pessoais para carregar o programa do PLC, envia informações sobre o andamento do processo. DE FALCO, Marco – *Stuxnet Facts Report…*.

32 DENNING, Dorothy – «Stuxnet: what has changed?». In *Future Internet Journal*. Vol. 4, N.º 3, 2012, pp. 672-687. Consultado em: 8 de maio de 2023. Disponível em: https://www.mdpi.com/1999-5903/4/3/672.

33 LINDSAY, Jon – «Stuxnet and the limits of cyber warfare».

34 ALBRIGHT, David, et al. – *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*. WA: Institute for Science and International Security. 2010. Consultado em: 26 de março de 2023. Disponível em: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

35 LANGNER, Ralph – «Stuxnet: dissecting a cyberwarfare weapon». In *IEEE Security & Privacy*. Vol. 9, N.º 3, 2011, pp. 49-51.

36 FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric – *W32.Stuxnet Dossier*.

37 COLLINS, Sean; MCCOMBIE, Stephen – «Stuxnet…».

38 DE FALCO, Marco – *Stuxnet Facts Report…*, p. 21.

39 Utiliza um documento em formato Microsoft Word para infectar os computadores das vítimas, executa de modo autônomo uma chave de entrada (*keylogger*) para registrar as teclas digitadas e salvar imagens da tela utilizada pelo usuário, outros dois arquivos corrompidos permitem aos invasores controlar os processos de registro dos usuários. GOSTEV, ALEXANDER; KUZNETSOV, Igor – «Stuxnet/Duqu: the evolution of drivers». Kaspersky. 2011. Consultado em: 23 de julho de 2023. Disponível em: https://securelist.com/stuxnetduqu-the-evolution-of-drivers/36462/.

40 Possui componentes de propagação e injeção diferenciados que reúnem registro de atividades em teclado, capturas de tela, ativação de microfone e câmera para gravação de áudio e vídeo, e sistema de Bluetooth para identificar possíveis aparelhos conectados em rede e se propagar de modo furtivo. BENCSÁTH, Boldizsár, et al. – «The cousins of Stuxnet: Duqu, Flame, and Gaus». In *Future Internet*. Vol. 4, N.º 4, 2012, pp. 971-1003.

41 MORTON, Chris – «Stuxnet, Flame e Duqu – the Olympic Games». *In* HEALEY, Jason – *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Viena, VA: Cyber Conflicts Studies Association, 2013, pp. 212-231.

42 ALBRIGHT, David, et al. – *Preventing Iran from Obtaining Nuclear Weapons…*, p. 29; DE FALCO, Marco – *Stuxnet Facts Report…*, pp. 11-27.

43 ALBRIGHT, David; BURKHARD, Sarah – *Entering Dangerous, Uncharted Waters…*; LINDSAY, Jon – «Stuxnet and the limits of cyber warfare».

44 HAYDEN, Michael – *Playing to the Edge: American Intelligence in the Age of Terror*. Nova Iorque: Penguin Press, 2016.

45 KELLO, Lucas – «The meaning of the cyber revolution perils to theory and statecraft». In *International Security*. Vol. 38, N.º 2, 2013, p. 23. Consultado em: 13 de março de 2023. Disponível em: https://www.jstor.org/stable/24480929. Salvo indicação em contrário todas as citações são traduções livres dos autores.

46 BUTRIMAS, Vytautas – «National security and international policy challenges…»; DE FALCO, Marco – *Stuxnet Facts Report…*.

47 Para um aprofundamento sobre como as normas multilaterais que limitam os conflitos interestatais tornam estratégico para os Estados o recurso às armas cibernéticas ver JENKINS, Ryan – «Is Stuxnet physical? Does it matter?».

48 BRENNER, Joel – *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. 1.ª edição. Inglaterra: Penguin Press, 2011.

49 DE FALCO, Marco – *Stuxnet Facts Report…*.

50 ALBRIGHT, David; BURKHARD, Sarah – *Entering Dangerous, Uncharted Waters…*, p. 112.

51 *NATIONAL STRATEGY to Secure Cyberspace*. Washington DC: America's Cyber Defense Agency, 2003. Consultado em: 8 de agosto de 2023. Disponível em: https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

52 *Ibidem*, pp. 29-30.

53 *Ibidem*, p. 33.

54 *Ibidem*, pp. 28-41.

55 «NATIONAL SECURITY Strategy». Washington DC: Office of the Secretary of Defense, 2006, p. 3. Consultado em: 10 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/.

56 *Ibidem*, p. 18.

57 «NATIONAL DEFENSE Strategy». Washington DC: Office of the Secretary of Defense, 2008, p. 14. Consultado em: 11 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Defense-Strategy/.

58 *Ibidem*, p. 4.

59 *Ibidem*, p. 18.

60 *Ibidem*, p. 19.

61 SANGER, David – «Obama order sped up wave of cyberattacks against Iran». In *New York Times*. 2012. Consultado em: 21 de junho de 2023. Disponível em: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

62 «NATIONAL SECURITY Strategy». Washington DC: Office of the Secretary of Defense, 2010, p. 4. Consultado em: 12 de

julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/.

63 *Ibidem*, pp. 23-24.

64 «NATIONAL DEFENSE Strategy». Washington DC: Office of the Secretary of Defense, 2011, p. 3. Consultado em: 15 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Military-Strategy/.

65 *Ibidem*, pp. 3-8.

66 *Ibidem*, p. 10.

67 *Ibidem*, pp. 11-12.

68 *Ibidem*, pp. 19-20.

BIBLIOGRAFIA

ALBRIGHT, David; BRANNAN, Paul; STRICKER, Andrea; WALROND, Christina; WOOD, Houston – *Preventing Iran from Obtaining Nuclear Weapons: Constraining its Future Nuclear Options*. WA: Institute for Science and International Security. 2012. Consultado em: 27 de março de 2023. Disponível em: https://isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf.

ALBRIGHT, David; BRANNAN, Paul; WALROND, Christina – *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*. WA: Institute for Science and International Security. 2010. Consultado em: 26 de março de 2023. Disponível em: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

ALBRIGHT, David; BURKHARD, Sarah – *Entering Dangerous, Uncharted Waters: Iran's 60 Percent Highly Enriched Uranium*. WA: Institute for Science and International Security. 2022. Consultado em: 12 de agosto de 2023. Disponível em: https://isis-online.org/isis-reports/detail/entering-uncharted-waters-irans-60-percent-highly-enriched-uranium.

AZENHA, Pedro Jorge de Oliveira – «A Estratégia Nuclear Iraniana e os Desafios Colocados à Comunidade Internacional». Lisboa: Instituto de Estudos Superiores Militares, 2010. Trabalho de Investigação Individual. Consultado em: 25 de junho de 2023. Disponível em: https://comum.rcaap.pt/handle/10400.26/12674.

BENCSÁTH, Boldizsár; PÉK, Gábor; BUTTYÁN, Levente; FÉLEGYHÁZI, Márk – «The cousins of Stuxnet: Duqu, Flame, and Gaus». In *Future Internet*. Vol. 4, N.º 4, 2012, pp. 971-1003. DOI:https://doi.org/10.3390/fi4040971.

BENNET, Andrew; CHECKEL, Jeffrey T., ed. lit. – *Process Tracing: From Metaphor to Analytic Tool*. 1.ª edição. Nova Iorque: Cambridge University Press, 2014.

BERMÚDEZ, Àngel – «Programa nuclear do Irã: como EUA ajudaram o país a iniciar polêmico plano atômico». BBC News Brasil. 2021. Consultado em: 15 de março de 2023. Disponível em: https://www.bbc.com/portuguese/geral-59491973.

BETZ, David J.; STEVENS, Tim – *Cyberspace and the State: Towards a Strategy for Cyber-Power*. 1.ª edição. Reino Unido: IISS Routledge, 2011.

BLINDER, Caio – «Discurso do "Eixo do Mal" assombra Bush». BBC News Brasil. 2006. Consultado em: 20 de março de 2023. Disponível em: https://www.bbc.com/portuguese/reporterbbc/story/2006/10/061012_caioblinderaw.

BRENNER, Joel – *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. 1.ª edição. Inglaterra: Penguin Press, 2011.

BRENNER, Joel – «Eyes wide shut: the growing threat of cyber attacks on industrial control systems». In *Bulletin of the Atomic Scientists*. Vol. 69, N.º 5, 2013, pp. 16-20. DOI: https://doi.org/10.1177/0096340213501372.

BUTRIMAS, Vytautas – «National security and international policy challenges in a post Stuxnet world». In *Lithuanian Annual Strategic Review*. Vol. 12, 2014, pp. 11-31. Consultado em: 8 de maio de 2023. Disponível em: https://kam.lt/wp-content/uploads/2022/03/lithuanian-annual-strategic-review-2013-2014-vol-12.pdf.

COLLINS, Sean; MCCOMBIE, Stephen – «Stuxnet: the emergence of a new cyber weapon and its implications». In *Journal of Policing, Intelligence and Counter Terrorism*. Vol. 7, N.º 1, 2012, pp. 80-91. DOI: http://dx.doi.org/10.1080/18335330.2012.653198.

DE FALCO, Marco – *Stuxnet Facts Report: A Technical and Strategic Review*. TLL, EST: NATO Cooperative Cyber Defense Center of Excellence. 2012. Consultado em: 8 de junho de 2023. Disponível em: https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/.

DENNING, Dorothy – «Stuxnet: what has changed?». In *Future Internet Journal*. Vol. 4, N.º 3, 2012, pp. 672-687. Consultado em: 8 de maio de 2023. Disponível em: https://www.mdpi.com/1999-5903/4/3/672.

FALLETI, Tulia – «Process tracing of extensive and intensive processes». In *New Political Economy*. Vol. 21, N.º 5, 2016, pp. 455-462. DOI: https://www.tandfonline.com/doi/full/10.1080/13563467.2015.1135550.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric – *W32.Stuxnet Dossier*. Symantec Security Response. Califórnia: Symantec Corporation World Headquarters, 2011. Atualizado em: fevereiro de 2011. Consultado em: 26 de junho de 2023. Disponível em: https://nsarchive.gwu.edu/document/21440-document-44.

FARWELL, James P.; ROHOZINSKI, Rafal – «The new reality of cyber war». In *Survival: Global Politics and Strategy*. Vol. 54, N.º 4, 2012, pp. 107-120. DOI: http://dx.doi.org/10.1080/00396338.2012.709391.

GOSTEV, ALEXANDER; KUZNETSOV, Igor – «Stuxnet/Duqu: the evolution of drivers». Kaspersky. 2011. Consultado em: 23 de julho de 2023. Disponível em: https://securelist.com/stuxnetduqu-the-evolution-of-drivers/36462/.

HAYDEN, Michael – *Playing to the Edge: American Intelligence in the Age of Terror*. Nova Iorque: Penguin Press, 2016.

JENKINS, Ryan – «Is Stuxnet physical? Does it matter?». In *Journal of Military Ethics*. Vol. 12, N.º 1, 2013, pp. 68-79. DOI: https://doi.org/10.1080/15027570.2013.782640.

JOLLEY, Jason – «Article 2(4) and cyber warfare: how do old rules control the brave new world?». In *International Law Research*. Vol. 2, N.º 1, 2013, pp. 1-16. DOI: http://dx.doi.org/10.5539/ilr.v2n1p1.

KELLO, Lucas – «The meaning of the cyber revolution perils to theory and statecraft». In *International Security*. Vol. 38, N.º 2, 2013, pp. 7-40. Consultado em: 13 de março de 2023. Disponível em: https://www.jstor.org/stable/24480929.

KELSEY, Davenport – «UN Security Council Resolution on Iran». Arms Control Association. 2022. Consultado em: 26 de abril de 2023. Disponível em: https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran.

KUMAR, Rajesh; KELA, Rohan; SINGH, Siddhant; TRUJILLO-RASUA, Rolando – «APT attacks on industrial control systems: a tale of three incidents». In *International Journal of Critical Infrastructure Protection*.

Vol. 37, 2022, pp. 1-11. DOI: https://doi.org/10.1016/j.ijcip.2022.100521.

LANGNER, Ralph – «Stuxnet: dissecting a cyberwarfare weapon». In *IEEE Security & Privacy*. Vol. 9, N.º 3, 2011, pp. 49-51. DOI: 10.1109/MSP.2011.67.

LINDSAY, Jon – «Stuxnet and the limits of cyber warfare». In *Security Studies*. Vol. 22, N.º 3, 2013, pp. 365-404. DOI: https://doi.org/10.1080/09636412.2013.816122.

LILIENTHAL, Gary; AHMAD, Nehaluddin – «Cyber-attack as inevitable kinetic war». In *Computer Law & Security Review*. Vol. 31, N.º 3, 2015, pp. 390-400. DOI: https://doi.org/10.1016/j.clsr.2015.03.002.

MAHONEY, James – «The logic of process: tracing tests in the social sciences». In *Sociological Methods & Research*. Vol. 41, N.º 4, 2012, pp. 570-597. DOI: https://doi.org/10.1177/0049124112437709.

MILEVSKI, Lukas – Stuxnet and strategy: a special operation in cyberspace?». In *National Defense University Press*. Vol. 63, N.º 4, 2011, pp. 64-69. Consultado em: 25 de junho de 2023. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_64-69_Milevski.pdf?ver=Jy0SW9E8UBbatlrmrw-egQ%3D%3D.

MORGADE, Alba – «EUA x Irã: o que originou a rivalidade de décadas entre os dois países». BBC News Brasil. 2020. Consultado em: 24 de março de 2023. Disponível em: https://www.bbc.com/portuguese/internacional-50983943.

MORTON, Chris – «Stuxnet, Flame e Duqu – the Olympic Games». *In* HEALEY, Jason – *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Viena, VA: Cyber Conflicts Studies Association, 2013, pp. 212-231.

«NATIONAL DEFENSE Strategy». Washington DC: Office of the Secretary of Defense, 2008. Consultado em: 11 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Defense-Strategy/.

«NATIONAL DEFENSE Strategy». Washington DC: Office of the Secretary of Defense, 2011. Consultado em: 15 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Military-Strategy/.

«NATIONAL SECURITY Strategy». Washington DC: Office of the Secretary of Defense, 2006. Consultado em: 10 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/.

«NATIONAL SECURITY Strategy». Washington DC: Office of the Secretary of Defense, 2010. Consultado em: 12 de julho de 2023. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/.

NATIONAL STRATEGY to Secure Cyberspace. Washington DC: America's Cyber Defense Agency, 2003. Consultado em: 8 de agosto de 2023. Disponível em: https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

NOURIAN, ARASH; MADNICK, Stuart – «A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet». In *IEEE Transactions on Dependable and Secure Computing*. Vol. 15, N.º 1, 2018, pp. 2-13. Consultado em: 15 de junho de 2023. Disponível em: https://ieeexplore.ieee.org/document/7360168.

SANGER, David – «Obama order sped up wave of cyberattacks against Iran». In *New York Times*. 2012. Consultado em: 21 de junho de 2023. Disponível em: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

ZETTER, Kim – «How digital detectives deciphered Stuxnet: the most menacing malware in history». WIRED Security. 2011. Consultado em: 26 de junho de 2023. Disponível em: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

Ordem e progresso?
Analisando as respostas brasileiras aos cibercrimes

Mariana Grilli Belinotte | *Luiz Rogério Franco Goldoni* | *Joe Devanny* | *Carlos Frederico Coelho*

INTRODUÇÃO

O presente artigo analisa a reação do Estado brasileiro em relação a dois casos emblemáticos de violação de sistemas e dados: o vazamento das fotos íntimas da atriz Carolina Dieckmann, em 2012, e a revelação, por Edward Snowden e pelo grupo Wikileaks, que as comunicações de cidadãos brasileiros, incluindo as da então Presidente da República, Dilma Rousseff, eram monitoradas pelo Governo estadunidense. Assim, investiga-se a influência desses acontecimentos na aprovação de dois diplomas legais sobre crimes cibernéticos e proteção de dados: no primeiro caso, a Lei N.º 12.737/2012 – Lei Carolina Dieckmann –, e, no segundo, a Lei Geral de Proteção de Dados (Lei N.º 13.709/2018).

O objetivo geral do artigo é averiguar como Estados reagem legalmente a violações de sistemas e dados com ampla repercussão na sociedade. Os objetivos específicos são: *a*) analisar as reações legislativas ao incidente Carolina Dieckmann e *b*) ao caso Snowden, e *c*) contrastá-las para compreender as diferenças e semelhanças entre os casos. A hipótese apresentada é a de que casos de alta repercussão aceleram ou intensificam as ações governamentais voltadas à cibersegurança. Neste artigo, a investigação foi restrita às respostas legislativas aos incidentes, reconhecendo-se que há uma série de outras respostas possíveis, como reorganizações orçamentárias ou institucionais, pronunciamentos ou decisões judiciais. Justifica-se a escolha do tema pois o estudo de processos

RESUMO

A ameaça cibernética tornou-se questão cada vez mais proeminente nos últimos anos. Embora global, o problema afeta alguns países mais do que outros. Este é o caso do Brasil, que se tornou um ponto focal para ataques cibernéticos. O principal objetivo do artigo é analisar as reações do Estado brasileiro a cibercrimes de alto perfil. O artigo fornece uma visão contextual de como incidentes significativos moldaram a resposta legislativa do Brasil ao cibercrime, principalmente na Lei Geral de Proteção de Dados e na Lei Carolina Dieckmann. Contribui para uma agenda de pesquisa focada em analisar como e por que algumas atividades são criminalizadas, enquanto outras não o são, ajudando também a compreender as prioridades e percepções de diferentes Estados.

Palavras-chave: cibersegurança, cibercrime, Lei Geral de Proteção de Dados, Lei Carolina Dieckmann, Brasil.

ABSTRACT

Order and progress? An analysis of Brazilian responses to cybercrime

The cyber threat has become an increasingly important issue in →

 https://doi.org/10.23906/ri2024.82a07

recent years. Although the problem is global, it affects some countries more than others. This is the case in Brazil, which has become a focal point for cyber attacks. The main goal of this article is to analyze the Brazilian state's responses to high-profile cybercrimes. The article provides a contextual overview of how significant incidents have shaped Brazil's legislative response to cybercrime, particularly in the General Data Protection Law and the Carolina Dieckmann Law. It contributes to a research agenda focused on analyzing how and why some activities are criminalized while others are not, and also helps to understand the priorities and perceptions of different states.

Keywords: cybersecurity, cybercrime, General Data Protection Law, Carolina Dieckmann Law, Brazil.

específicos de criminalização (ou de não criminalização, como no incidente Snowden) demonstra as prioridades e o entendimento dos atores sobre aspectos como a importância do valor afetado, as sanções consideradas adequadas, os procedimentos a serem realizados, etc.

Os casos foram escolhidos por suas diferenças: o incidente Dieckmann foi de natureza privada. Seus valores protegidos foram a privacidade e a intimidade, e culminou na aprovação de uma lei penal, que criminalizou a invasão e a manipulação de sistemas e o acesso a dados pessoais. Já o monitoramento de empresas brasileiras e autoridades nacionais e internacionais por outros Estados tem caráter eminentemente público – envolveu, também, a privacidade, mas, devido ao perfil das vítimas, ganhou conotações mais amplas, por ter aspectos relacionados à soberania e à segurança nacional. Nesse caso, a resposta igualmente envolveu a promulgação de uma lei, mas não de natureza penal, ou seja, não criou ou alterou um tipo penal (ou crime, como entende o público em geral). Ademais, a resposta ao caso Snowden também foi acompanhada de ações diplomáticas voltadas às discussões sobre a governança global do ciberespaço.

Nas seções seguintes, serão tratados a criminalização em geral, o fenômeno dos cibercrimes e o contexto do Brasil na questão. Após, analisa-se os casos Dieckmann e Snowden. A discussão sobre os casos é realizada à luz de questões internas inerentes ao Brasil e sua posição nas discussões globais sobre a governança da internet.

CRIMINALIZAÇÃO

Nesta seção, será explicado o que é e como ocorre a criminalização, ou seja, de que maneira uma ação se torna proibida e penalmente punível. Também se discutirá, brevemente, os direitos e garantias e sua importância para o direito penal, as causas e motores da criminalização, a efetividade do direito penal, e a criminalização nos casos em tela – incidentes Dieckmann e Snowden.

Criminalização é o processo que torna uma conduta penalmente sancionável dentro de um ordenamento jurídico. Na criminalização, uma atividade é identificada[1] como proscrita, e uma pena é imposta para as pessoas que a praticam – privação de liberdade, pagamento de multas, suspensão de direitos, práticas reeducativas, ou mesmo a pena capital. Nos Estados contemporâneos, os atores responsáveis pela definição das condutas proibidas são, em geral, os legisladores, e o meio competente é a lei[2].

Os legisladores e demais agentes implicados na coibição das práticas criminalizadas (juízes, promotores, policiais, advogados, agentes penitenciários) devem respeitar garantias e direitos típicos do Estado democrático de direito. Não é, e não pode ser, um vale-tudo, como

desde o século XVIII foi observado por Rousseau. As garantias processuais, os limites da criminalização, os benefícios da execução penal, o direito à ampla defesa, ao contraditório e ao tratamento digno, mesmo após a condenação, são conquistas civilizatórias e estão, no Brasil, consagradas na Constituição Federal e na legislação infraconstitucional.

Esse arcabouço básico de direitos humanos também aparece na forma de tratados internacionais, que definem limites ao poder interno dos países de legislar e definir crimes, como o Pacto de San Jose da Costa Rica. No entanto, cada Estado ainda define o que é crime em seu território. Logo, o crime é uma construção coletiva de uma determinada sociedade, em uma determinada época, e varia de acordo com o local e o tempo[3].

Em teoria, a criminalização teria como objetivo diminuir a frequência de uma atividade considerada indesejável pela sociedade. Na realidade, esse processo pode ocorrer devido a outros fatores: pressão da população ou da mídia, desejo das autoridades de demonstrar ação, atos discriminatórios e repressão contra minorias, ou busca por um aumento do prestígio e/ou do orçamento de forças policiais, por exemplo.

Duas últimas áreas de análise discutem a efetividade da criminalização: uma busca entender o grau de sucesso na transformação de determinadas condutas em crime; a outra investiga a eficiência da criminalização – em outras palavras, averigua se a criminalização de uma atividade reduz sua prática. Isto é especialmente importante quando a dimensão «tempo» é considerada, em situações que envolvem o avanço tecnológico. O direito, enquanto processo socialmente construído, apresenta grande dificuldade em reagir aos avanços tecnológicos na mesma velocidade em que estes ocorrem. Tal qual sugerido por Gutwirth, De Hert e De Sutter[4], o direito busca, inicialmente, responder aos novos desafios utilizando regras já existentes. A criação de novas normas, assim, geralmente se dá num segundo momento, o que é o eixo de análise deste trabalho.

No caso Dieckmann, ocorreu um processo de criminalização movido, em parte, pela comoção causada na sociedade, na mídia e nos atores políticos após o incidente. Condutas relacionadas a invadir computadores ou manipular dados passaram a ser puníveis com até um ano de prisão, respeitadas as garantias e direitos. Já no caso Snowden, houve a promulgação da Lei Geral de Proteção de Dados (LGPD), que só prevê sanções administrativas. Ou seja, o legislador não se utilizou da LGPD para criminalizar as condutas ali descritas – embora elas possam ser crimes com base em outras leis.

Ressalta-se que as características acima descritas da criminalização – o processo social de designar uma sanção para uma conduta coletivamente entendida como indesejada, respeitando o devido processo legislativo e as garantias e direitos aplicáveis ao caso – permanecem válidas ao se falar de cibercrimes, como demonstrado acima. Mas os cibercrimes possuem peculiaridades e subdivisões próprias, como será analisado a seguir.

CIBERCRIMES

Esta seção aborda as características do ciberespaço que alteram as condições para o cometimento de ilícitos (ação à distância, anonimato, aumento do número de alvos em

potencial e ação transnacional) e o descompasso entre o surgimento das novas tecnologias – e por conseguinte, dos novos delitos – e os sistemas legais, especialmente, como no caso do Brasil, aqueles de orientação romano-germânica. Versa, ainda, sobre a amplitude das condutas denominadas «cibercrimes», ou «crimes cibernéticos», e apresenta uma possível classificação.

Em primeiro lugar, o ciberespaço altera as formas de relacionamento interpessoais possíveis. As peculiaridades inerentes a esse domínio possibilitam um distanciamento entre os criminosos e suas vítimas, o que aumenta potencialmente o número de alvos do transgressor[5]. Além disso, mediante o mesmo código malicioso ou ação de *phishing* um cibercriminoso pode causar danos a um número incalculável de alvos. A impessoalidade do ataque somada a técnicas relativas à ocultação de rastros dificulta a identificação dos perpetradores[6] e, consequentemente, na punição desses. Além disso, há empecilhos na investigação e na punição de crimes em que os suspeitos estão em outros países. A sensação de impunidade cria no coletivo a imagem do ciberespaço como uma «terra sem lei», fato que por um lado estimula as ações dos cibercriminosos e, por outro, causa insegurança nos demais cidadãos, principalmente naqueles não muito afeitos à tecnologia.

A SENSAÇÃO DE IMPUNIDADE CRIA NO COLETIVO A IMAGEM DO CIBERESPAÇO COMO UMA «TERRA SEM LEI», FATO QUE POR UM LADO ESTIMULA AS AÇÕES DOS CIBERCRIMINOSOS E, POR OUTRO, CAUSA INSEGURANÇA NOS DEMAIS CIDADÃOS.

Em segundo lugar, a tecnologia está sempre «um passo a frente» das normas. O surgimento de uma nova tecnologia acarreta, inevitavelmente, o surgimento de uma série de novas ameaças, riscos e ilícitos. Esses fenômenos não existiam e não eram conhecidos, até o momento em que novas técnicas e sistemas são implementados: «nenhum dispositivo técnico pode desenvolver-se sem, por sua vez, gerar o ‹seu› acidente específico»[7] e, acrescentamos, não podem ser desenvolvidos sem darem origem a tipos novos e específicos de delitos. Em outras palavras e exemplificando: os acidentes aéreos e as normas relativas à aviação apenas surgiram com a invenção do avião.

Esse descompasso é mais perceptível nos sistemas jurídicos de inspiração romano-germânica[8]. Nos sistemas anglo-saxões, de tradição consuetudinária, baseada em precedentes, é possível, observados os limites constitucionais, utilizar ferramentas como a analogia e a interpretação extensiva para resolver dilemas cujas soluções ainda não foram codificadas. É daí que surge, por exemplo, a abundante literatura acadêmica estadunidense dos anos 1990 que discutia a aplicabilidade de conceitos jurídicos como «propriedade» e «privacidade» no ciberespaço, e suas possíveis consequências legais[9]. Isso não é possível nos países que adotam os princípios romano-germânicos, em que, geralmente, apenas a lei pode criar deveres e sanções.

Por fim, o cibercrime é de difícil conceituação e classificação, principalmente devido à multiplicidade de finalidades e meios envolvidos. Cibercrime[10] pode envolver desde *malwares* sofisticados até ações de engenharia social, pode ter como finalidade obter recursos financeiros, disseminar mensagens de ódio ou perseguir e humilhar indivíduos; pode ser cometido

por um indivíduo, por grupos criminosos, ou por atores organizados por Estados. Nesse sentido, Gordon e Ford[11] propõem compreender o cibercrime de acordo com sua duração e sua dependência no uso de *crimewares*[12]. Em termos de duração, existiriam os incidentes discretos, que ocorreriam em um único episódio, como o uso de um *trojan* para acessar dados pessoais e transferir recursos financeiros, e os contínuos – *ciberstalking*, espionagem, cooptação de membros para redes terroristas, pornografia infantil, chantagem e extorsão, etc.

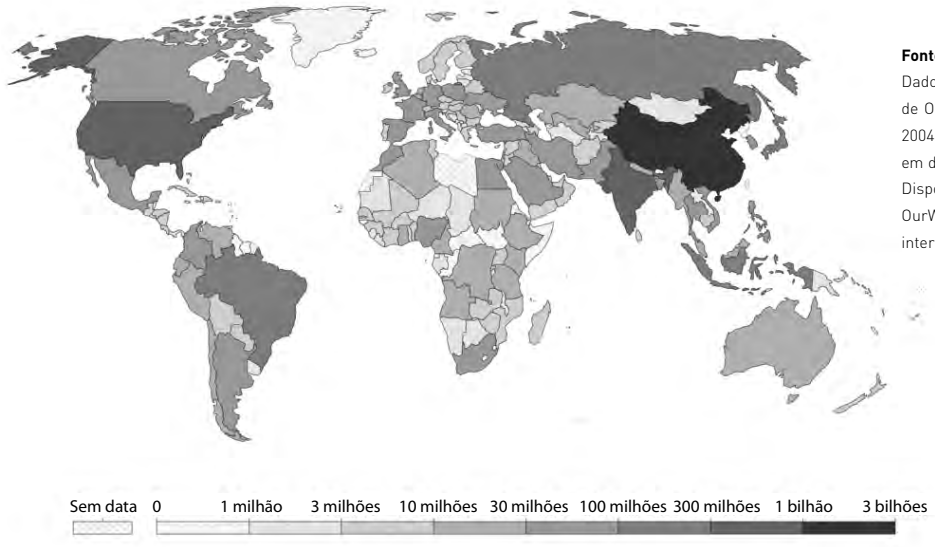
Em relação a dependência do uso de *crimeware* para o cometimento dos delitos, a classificação se daria em um *continuum*, com um dos extremos sendo o das fraudes inteiramente dependentes dessas ferramentas, como transferências de dinheiro de bancos centrais a partir da captura do controle do sistema por meio de um vírus, e, do outro, ações que se utilizam do ciberespaço e de ferramentas de uso comum como apps de mensagens, redes sociais, *websites*, jogos virtuais, para a prática de fraudes, estelionato, *bullying*, etc.[13].

O cibercrime é difícil de ser medido, devido à diversidade de formatos e à subnotificação. Por isso, as informações sobre o contexto de um país ou região em relação a essa ameaça são, por vezes, pouco precisas. No entanto, alguns dados podem ser obtidos em documentos oficiais de organismos internacionais, na imprensa e nos relatórios de companhias de segurança cibernética. Na seção seguinte, será apresentado o panorama do Brasil nesse contexto, relacionando-o a seu entorno e à situação geopolítica global.

CONTEXTO BRASILEIRO

O Brasil é um dos países mais populosos do mundo e, como tal, natural que seja também um dos países com maior número de usuários de internet do planeta, conforme se depreende da figura 1.

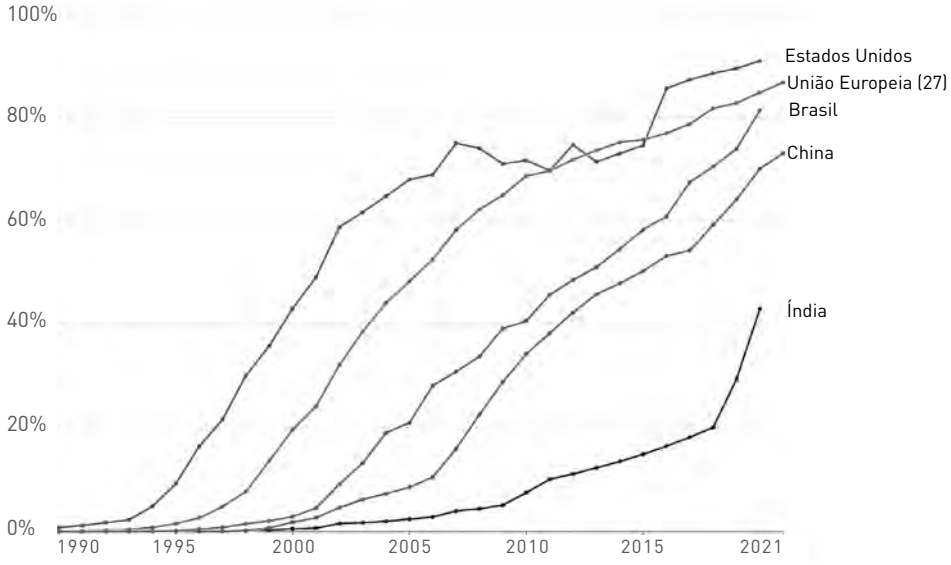
Figura 1 > Número total de usuários de internet do planeta



Fonte: Dados extraídos de Our World Data, 2004. Consultado em dezembro de 2023. Disponível em: OurWorldInData.org/internet.

Seus números relativos de usuários de internet são igualmente expressivos e maiores que aqueles encontrados em países em desenvolvimento como a China e a Índia, sendo apenas um pouco aquém dos números encontrados na Europa e nos Estados Unidos, conforme pode ser observado na figura 2.

Figura 2 > Número relativo de usuários de internet: Brasil, China, Índia, Estados Unidos e União Europeia



Fonte: Dados extraídos de Our World Data, 2004. Consultado em dezembro de 2023. Disponível em: OurWorldInData.org/internet.

Portanto, é natural que, em razão dos números acima mostrados, o Brasil apresente um arcabouço legislativo substantivo quanto à legislação atinente ao ciberespaço. Em seu relatório de cibersegurança global (RCG), de 2020, a União Internacional das Telecomunicações (em inglês, International Telecommunication Union) dá a nota máxima possível ao Brasil, quanto às medidas legais existentes no país na temática de cibersegurança[14]. A tabela a seguir apresenta as notas obtidas por alguns países da América Latina; dentre os países em desenvolvimento da região, o Brasil apresenta a melhor pontuação.

Tabela 1 > Pontuação do RCG 2020 da União Internacional das Telecomunicações – países da América Latina

Pontuação: Medidas Legais (0-20)	
Brasil, Canadá, Estados Unidos	20,0
Costa Rica	17,62

[Cont.]

Chile	17,20
México	15,61
Uruguai	13,90
Colômbia	9,14

Fonte: Elaboração própria, com dados do RCG (União Internacional das Telecomunicações, 2021).

Na temática de cibercrimes, a estrutura legislativa brasileira é relativamente enxuta, baseando-se primordialmente na Constituição do país, que comparativamente a outros, é relativamente jovem (1988), e em legislação infraconstitucional específica trazida em anos posteriores, entre as quais se destacam o Marco Civil da Internet (Lei N.º 12.965/2014), LGPD (Lei N.º 13.709/2018) e, mais recentemente, a Lei N.º 14.155/2021. De maneira intencional, a Lei N.º 12.737/2012 será objeto de análise específica em seção posterior, por configurar objeto do presente artigo.

O Marco Civil da Internet estabelece princípios, garantias, direitos e deveres relativos ao uso da internet no Brasil. Foi nesse momento que foram introduzidas definições de dados pessoais e tratamento de dados pessoais aplicáveis ao ambiente *online*, bem como normas de segurança a serem adotadas pelos provedores de conexões e fabricantes de aplicativos no armazenamento de dados pessoais e comunicações privadas.

Por sua vez, a LGPD tornou-se a principal fonte legislativa do ciberespaço brasileiro, apesar de não estabelecer especificamente a regulamentação de segurança cibernética. A LGPD estabeleceu a Agência Nacional de Proteção de Dados como ator central na imposição de sanções administrativas e na regulação de parâmetros sobre a temática.

Em abril de 2023, o Brasil tornou-se signatário da Convenção de Budapeste. Trata-se de importante marco, formal e internacional, que une o país ao tratado assinado originalmente por países europeus no início do século[15], para a cooperação no combate e investigação de crimes cibernéticos. Tal qual será assinalado na próxima seção, chama a atenção que entre a assinatura e a posterior adoção da convenção no ordenamento jurídico interno, transcorreram mais de 20 anos.

CASOS DIECKMANN E SNOWDEN

O CASO DIECKMANN TRATA DA INTIMIDADE DE UM INDIVÍDUO, ENQUANTO O CASO SNOWDEN CAUSOU ALARME EM RELAÇÃO À SOBERANIA E À SEGURANÇA NACIONAL.

Como mencionado na Introdução, os casos Dieckmann e Snowden foram selecionados devido a suas diferenças. Pode-se dizer que são dois extremos de crimes cibernéticos, tanto quanto é possível ocorrer na realidade: o caso Dieckmann trata da intimidade de um indivíduo, enquanto o caso Snowden causou alarme em relação à soberania e à segurança nacional, após as revelações de que a então Presidente do Brasil, Dilma Rousseff, fora monitorada pelos Estados Unidos. Um deles – Dieckmann –, culminou na aprovação-relâmpago de uma lei penal, que prevê a prisão de quem acessar dados

e sistemas de terceiros sem autorização. O segundo levou ao estabelecimento de princípios e garantias gerais para o tratamento de dados pessoais. Nas subseções seguintes, serão analisados os incidentes em si, a repercussão de cada um, o processo de aprovação e o conteúdo dos dois diplomas legais em tela – a Lei Carolina Dieckmann e a LGPD.

CASO CAROLINA DIECKMANN

No dia 6 de maio de 2012, o jornal *O Estado de S. Paulo* noticiou que fotos íntimas da atriz Carolina Dieckmann haviam sido divulgadas, e estavam entre os assuntos mais comentados da rede social Twitter[16]. Nos dias e semanas seguintes, o tema foi continuamente abordado em matérias de jornal e televisão. Uma semana depois, em 14 de maio de 2012, os suspeitos foram encontrados, por meio do rastreamento de seus endereços IP. Foi provado que eles obtiveram as fotos a partir do *e-mail* da atriz, e, em seguida, passaram a chantageá-la, pedindo dinheiro em troca da não divulgação das imagens[17].

Os suspeitos foram acusados de difamação, furto e extorsão qualificada. No entanto, a conduta de invadir sistemas e acessar dados pessoais de terceiro ainda não era tipificada no ordenamento jurídico brasileiro: o Projeto de Lei N.º 84, de 1999 (Projeto Azeredo), por exemplo, buscava criminalizar a ação de *hackers* e *crackers*, e tramitava no Congresso Nacional, então por mais de doze anos, sem que fosse aprovado[18].

Essa demora não afligiu a Lei Carolina Dieckmann, cuja velocidade de tramitação surpreendeu até mesmo o Presidente da Câmara dos Deputados à época, Marco Maia (PT-RS)[19]. O projeto original, submetido à apreciação da Câmara Baixa em novembro de 2011, foi aprovado pelos deputados em 15 de maio de 2012 – menos de dez dias após a repercussão do vazamento das fotos[20]. Após envio ao Senado Federal, o projeto retornou à Câmara dos Deputados para a aprovação final no início de novembro do mesmo ano.

Em síntese, a lei acrescentou dois artigos ao Código Penal Brasileiro, além de marcar a primeira vez que a legislação penal pátria alcançaria, de maneira específica, crimes cibernéticos. A partir de então, quedou tipificada penalmente tanto a invasão de dispositivo informático quanto a interrupção de serviços informáticos. As penas estabelecidas pela Lei Carolina Dieckmann seriam alteradas quase dez anos depois, em 2021, através da Lei N.º 14.155/2021 de modo a punir com ainda maior rigor os crimes cibernéticos nela contidos. Hoje, é possível encontrar 77 projetos de lei em tramitação relacionados a crimes cibernéticos na Câmara dos Deputados[21].

CASO SNOWDEN

As revelações feitas por Edward Snowden em 2013, expondo o alcance global do monitoramento conduzido pela agência de segurança nacional dos Estados Unidos (NSA)[22], provocaram uma reavaliação significativa das práticas de segurança e privacidade de dados em todo o mundo. O ex-analista da NSA revelou que informações da alta cúpula

dos governos brasileiro[23], alemão[24] e francês[25] e da empresa Petrobrás[26] eram monitoradas pela agência estadunidense.

No contexto brasileiro, essas revelações tiveram impactos nas relações diplomáticas, manifestados no cancelamento da visita que a Presidente Dilma Rousseff faria aos Estados Unidos em setembro daquele ano[27] e no discurso de abertura da Assembleia Geral das Nações Unidas, proferido por Rousseff em 2013[28], classificado como um «ataque feroz à espionagem dos EUA»[29]. Internamente, as revelações impulsionariam a consolidação do Centro de Defesa Cibernético, estabelecido em 2012, e a criação do Comando de Defesa Cibernético, em 2016 (este, incorporando o Centro, criado em 2012)[30], e desencadeariam reflexões que influenciaram diretamente a criação e aprovação da LGPD em 2018.

O processo de elaboração da LGPD teve início com a apresentação do Projeto de Lei N.º 4060/2012, que visava criar uma legislação específica para a proteção de dados pessoais[31]. O debate sobre a necessidade de uma legislação abrangente para a proteção de dados ganhou força principalmente após as revelações de Snowden, que provocaram uma crescente conscientização sobre a vulnerabilidade dos dados pessoais em um mundo digital interconectado.

O DEBATE SOBRE A NECESSIDADE DE UMA LEGISLAÇÃO ABRANGENTE PARA A PROTEÇÃO DE DADOS GANHOU FORÇA PRINCIPALMENTE APÓS AS REVELAÇÕES DE SNOWDEN, QUE PROVOCARAM UMA CRESCENTE CONSCIENTIZAÇÃO SOBRE A VULNERABILIDADE DOS DADOS PESSOAIS.

A sociedade brasileira, em transição para uma economia digital, demandou medidas mais robustas para proteger sua privacidade em um ambiente virtual. A LGPD, nesse sentido, surgiu como uma resposta legislativa a essas preocupações crescentes. O Brasil reconheceu a necessidade de estabelecer uma legislação abrangente que regulamentasse o tratamento de dados pessoais, equilibrando a inovação tecnológica com a proteção dos direitos individuais. A lei não apenas reflete as demandas internas por maior segurança de dados, mas também incorpora uma resposta ao ambiente internacional pós-Snowden, no qual a privacidade se tornou uma questão central nas discussões sobre governança digital[32].

A tramitação do projeto de lei no Congresso Nacional envolveu debates como a definição de dados sensíveis, os princípios para o tratamento de dados, as responsabilidades das empresas e as penalidades por descumprimento[33]. A adequação da legislação à realidade das pequenas e médias empresas foi um ponto sensível, buscando-se equilibrar a proteção dos direitos dos cidadãos com a viabilidade econômica[34].

A necessidade de compatibilidade com padrões internacionais também foi outro ponto relevante nos debates. A sociedade brasileira estava atenta às discussões globais sobre privacidade e proteção de dados, influenciada, em parte, pelas revelações de Snowden sobre a vigilância em massa. Isso impulsionou a busca por uma legislação alinhada com padrões internacionais, reforçando a posição do Brasil como um ator global comprometido com a proteção da privacidade[35].

No âmbito legislativo brasileiro, as revelações de Snowden influenciaram os debates em torno da LGPD, moldando as discussões e ampliando a conscientização sobre a importância de proteger a privacidade em um cenário de crescente digitalização. A legislação, por sua vez, incorporou princípios fundamentais que refletem as preocupações suscitadas por Snowden, tais como a transparência no tratamento de dados, o respeito à privacidade e a necessidade de consentimento para coleta e processamento de informações pessoais[36].

A trajetória da LGPD no Congresso Nacional reflete a complexidade inerente à elaboração de uma legislação que busca equilibrar interesses diversos. Audiências públicas, debates e convites a especialistas foram realizados na Comissão de Ciência e Tecnologia, Comunicação e Informática e na Comissão Especial para Tratamento e Proteção de Dados Pessoais, criada especialmente para debater o projeto, bem como nos plenários da Câmara dos Deputados e do Senado Federal[37]. A participação ativa da sociedade civil nas audiências públicas desempenhou um papel crucial na identificação de preocupações e na sugestão de aprimoramentos no texto da lei[38].

Durante os debates, foram consideradas as experiências de outros países que já haviam implementado legislações semelhantes, como o Regulamento Geral de Proteção de Dados União Europeia[39]. A análise comparativa contribuiu para moldar a LGPD de maneira a atender às necessidades específicas do Brasil, levando em consideração suas características culturais, sociais e econômicas[40].

A aprovação da LGPD não marcou o fim do processo, mas sim o início de uma nova fase: a implementação efetiva da legislação. Órgãos reguladores foram criados, como a já citada Agência Nacional de Proteção de Dados, e as empresas tiveram prazos para se adequar às novas regras[41]. O processo de implementação envolveu não apenas a adaptação de políticas internas, mas também a conscientização dos cidadãos sobre seus direitos e das empresas sobre suas responsabilidades.

Apesar dos avanços proporcionados pela LGPD, alguns desafios persistem. A implementação efetiva da legislação demanda conscientização e capacitação contínuas de organizações e cidadãos. A garantia de conformidade com os princípios da lei requer monitoramento constante e uma abordagem proativa para lidar com as evoluções tecnológicas e os desafios emergentes relacionados à segurança de dados.

CONSIDERAÇÕES FINAIS: O BRASIL E SUAS OSCILAÇÕES INTERNAS E EXTERNAS NO COMBATE AO CIBERCRIME

As respostas aos incidentes cibernéticos aqui analisadas demonstram, de certa forma, uma oscilação do Brasil entre um constante binômio presente quando se pensa na governança e securitização do ciberespaço: liberdade x controle. Quando o tema em questão foi fácil e diretamente associado a crime passível de ser sofrido por um «cidadão comum» (no caso, o vazamento de fotos íntimas), houve um rápido apelo por um maior controle do ciberespaço pelo Estado.

Por outro lado, a proteção de dados pessoais é, de certa forma, tema mais amplo e nebuloso e, por conseguinte, menos impactante e preocupante para a população em geral. A LGPD estipula, por exemplo, como empresas devem gerir os dados pessoais de consumidores, se estes são ou não sigilosos, se podem ou não ser comercializados, como devem ser tratados, etc. Seu escopo, se por um lado abrangente, por outro traz questionamentos relativos a excessos de controle por parte do Estado e a possíveis ameaças às liberdades individuais e coletivas.

Ademais, a LGPD por refletir e ser impactada por caso de espionagem internacional, do qual o Brasil não foi a única vítima, não pode ser analisada fora do debate global sobre a governança do ciberespaço. Ou seja, há uma perspectiva internacional mais ampla na qual a política e a resposta legislativa do Brasil ao cibercrime devem ser situadas. O ciberespaço é, afinal, global, e as ameaças relacionadas à cibersegurança, portanto, afetam todos os Estados. Entretanto, as capacidades dos Estados para lidar com essas ameaças variam consideravelmente. Da mesma forma, existem inúmeras possíveis respostas de política doméstica e externa às ameaças cibernéticas. O Brasil é frequentemente considerado um «Estado-pêndulo» na diplomacia cibernética global[42]. Essa descrição define a diplomacia brasileira em relação a dois campos: uma posição ocidental, com opiniões semelhantes, a favor de uma internet livre e aberta e de uma governança multissetorial; e uma outra constelação, associada de forma proeminente à China e à Rússia, que favorece um modelo mais intergovernamental de governança global da internet, bem como uma maior assertividade da soberania estatal sobre a política cibernética.

Dessa maneira, as respostas dos Estados às ameaças cibernéticas podem apresentar diferenças normativas claras, não obstante o consenso normativo aparente sobre o comportamento estatal responsável no ciberespaço, que surge sob os auspícios da diplomacia cibernética da Organização das Nações Unidas (ONU) nos últimos quinze anos. A diplomacia cibernética do Brasil, bem como a resposta legislativa a ciberincidentes, em diferentes momentos, reflete oscilações no posicionamento brasileiro, inserindo-o ora mais em um campo, ora no outro. O Brasil é, em geral, fortemente favorável à abordagem multissetorial para a governança da internet, um dos pilares da iniciativa NETmundial (2014-2016). Mas também é um apoiador consistente da necessidade de reequilibrar a ordem internacional e representar melhor o Sul Global, o que pode ser visto como uma razão para apoiar um maior papel da ONU na governança global da internet.

O ponto-chave nesta análise, no entanto, é que o Brasil faz suas próprias escolhas na política cibernética. Não se pode definir a política cibernética brasileira em referência às políticas dos grupos ocidentais ou da China/Rússia na diplomacia cibernética global. Isso é claramente o caso no engajamento de longo prazo do Brasil com as dimensões internacionais do combate ao cibercrime. O Brasil foi, por exemplo, por muito tempo cético em relação aos méritos de aderir à Convenção de Budapeste, acabando por ade-

rir a ela por razões pragmáticas. Da mesma forma, o Brasil apoia o comitê *ad hoc* da ONU negociando um novo tratado global de cibercrime. A estratégia cibernética do Brasil nos assuntos internacionais é tanto normativa – promovendo o multissetorialismo e processos intergovernamentais mais globalmente representativos – quanto pragmática, visando acordos que aumentem a capacidade do país de alcançar seu objetivo estratégico nacional de combater o cibercrime.

Como outros Estados, para proteger seus cidadãos, empresas e instituições no ciberespaço, o Brasil precisa de uma combinação de capacidade doméstica aprimorada e parcerias internacionais eficazes. A agenda legislativa e a política doméstica do Brasil, incluindo reformas recentes do ecossistema de governança da cibersegurança por meio da nova Política Nacional de Cibersegurança, é um exemplo de iniciativas destinadas a aumentar a capacidade doméstica. Essa é uma agenda de longo prazo, na qual o governo nacional não é o único ator: empresas e sociedade civil são partes interessadas. Mas há também uma dimensão internacional significativa no combate ao cibercrime. Esta dimensão requer uma diplomacia assídua e paciente, não apenas do Ministério das Relações Exteriores, mas também da diplomacia funcional horizontal envolvendo cooperação judicial e policial, tanto regional quanto globalmente, por meio de organizações como a Interpol. Há uma clara oportunidade para o Brasil seguir tanto as dimensões domésticas quanto as internacionais de sua estratégia nacional de maneira integrada. Isso também se alinharia de perto com uma agenda para o Brasil exercer liderança regional, por exemplo, através da Organização dos Estados Americanos ou de outros órgãos regionais, para promover uma cooperação mais eficaz em segurança cibernética e combate ao cibercrime. O futuro de uma estratégia eficaz para combater o cibercrime deve residir na integração das agendas domésticas e internacionais. R:I

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Mariana Grilli Belinotte Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Doutoranda do Programa de Pós-Graduação em Ciências Militares da Escola de Comando e Estado-Maior do Exército. Mestre em Direito (Universidade Federal de Minas Gerais).

> Instituto Meira Mattos (PPGCM-IMM), Praça General Tibúrcio, 125, Sala: 313, Urca, Praia Vermelha, Rio de Janeiro 22290-270, Brasil | marianabelinotte@gmail.com

Luiz Rogério Franco Goldoni Professor do Programa de Pós-Graduação em Ciências Militares da Escola de Comando e Estado-Maior do Exército e coordenador do Laboratório de Poder Cibernético (LPCiber). Doutor em Ciência Política (Universidade Federal Fluminense).

> Escola de Comando e Estado-Maior do Exército (ECEME), Praça General Tibúrcio, 125, Praia Vermelha, Rio de Janeiro 22290-270, Brasil | luizrfgoldoni@gmail.com

Joe Devanny Professor do Departamento de War Studies do King's College London. Doutor em Teoria Política pela Universidade de Cambridge.

> King's College London, Strand Campus, Strand, Londres, WC2R 2LS, Reino Unido | Joseph.devanny@kcl.ac.uk

Carlos Frederico Coelho Professor do Programa de Pós-Graduação em Ciências Militares da Escola de Comando e Estado-Maior do Exército. Doutor em Ciência Política pela Universidade do Estado do Rio de Janeiro.

> Escola de Comando e Estado-Maior do Exército (ECEME), Praça General Tibúrcio, 125, Praia Vermelha, Rio de Janeiro 22290-270, Brasil | cafrecoelho@gmail.com

NOTAS

1 Só será abordada a criminalização «substantiva», aquela que envolve a criação ou modificação de tipos penais, e não o conceito mais amplo, que envolveria, por exemplo, a análise do aparato repressivo do Estado e a administração da justiça.

2 LANCY, Nicola – «Historicising criminalisation». In *The Modern Law Review*. Londres. Vol. 72, N.º 6, 2009, pp. 936-960. DOI: 10.1111/j.1468-2230.2009.00775.x.

3 BERGER, Peter; LUCKMANN, Thomas – *The Social Construction of Reality*. 1.ª edição. Nova Iorque: Open Road, 1966.

4 GUTWIRTH, Serge; DE HERT, Paul; DE SUTTER, Laurent – «The trouble with technology regulation from a legal perspective». In *Regulating Technologies*. Oxford: Hart Publishers, 2008, pp. 193-218.

5 MEDEIROS, Breno; GOLDONI, Luiz – «The fundamental conceptual trinity of cyberspace». In *Contexto Internacional*. Rio de Janeiro. Vol. 42, N.º 1, 2020, pp. 31-54.

6 DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «Strategy in an uncertain domain: threat and response in cyberspace». In *Journal of Strategic Security*. Rapid City. Vol. 12, N.º 2, 2022, pp. 34-47.

7 VIRILIO, Paul – *El Cibermundo, la política de lo peor*. Madrid: Cultura Libre, 1997.

8 DAVID, René – *Major Legal Systems in the World Today*. Milwaukee: Stevens, 1985.

9 JOHNSON, David; POST, David – «Law and borders». In *Stanford Law Review*. Stanford. Vol. 48, N.º 5, 1996, pp. 1367--1402; RONFELDT, David – «Cyberocracy is coming». In *The Information Society*. Nova Iorque. Vol. 8, N.º 4, 1992, pp. 243-296; SMITH, Stephen – «Communication and the Constitution in cyberspace». In *Communication Education*. Londres. Vol. 43, N.º 2, 1994, pp. 87-101.

10 O cibercrime, de acordo com a minuta da Política Nacional de Cibersegurança, em seu artigo 4, inciso III, é crime praticado contra, ou por meio de, ciberativos («MINUTA DA PNCiber». Gabinete de Segurança Institucional da Presidência da República. Consultado em: janeiro de 2024. Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf).

11 GORDON, Sarah; FORD, Richard – «On the definition and classification of cybercrime». In *Journal of Computer Virology*. Berlim. Vol. 13, 2006, pp. 13-20.

12 *Crimeware* são programas desenvolvidos para fazer com que os sistemas de terceiros funcionem de maneira diversa da que seu legítimo usuário espera, como *keyloggers*, *trojans*, *worms*, *bots*, entre outros (GORDON, Sarah; FORD, Richard – «On the definition and classification of cybercrime»).

13 *Ibidem*.

14 INTERNATIONAL TELECOMMUNICATION UNION – *Global Cybersecurity Index 2020*. Consultado em: fevereiro de 2024. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

15 «ASSINATURAS E ratificações da Convenção de Cibercrimes». Conselho da Europa. Consultado em: fevereiro de 2024. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

16 «ATRIZ CAROLINA Dieckmann é chantageada». In *O Estado de S. Paulo*. São Paulo, 6 de maio de 2012, p. C7.

17 VALLE, Sabrina – «Carolina Dieckmann teve as fotos roubadas por hackers». In *O Estado de S. Paulo*. São Paulo, 14 de maio de 2012, p. C7.

18 TRAMITAÇÃO DA Lei 12.737/2012. Câmara dos Deputados. Consultado em: janeiro de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011.

19 MADUEÑO, Denise – «Caso Carolina faz Câmara aprovar lei do crime cibernético». In *O Estado de S. Paulo*. São Paulo. 16 de maio de 2012, p. C7.

20 TRAMITAÇÃO DA Lei 12.737/2012.

21 TRAMITAÇÃO DE Projetos de Lei – crimes cibernéticos. Câmara dos Deputados. Consultado em: fevereiro de 2024. Disponível em: https://www.camara.leg.br/buscaProposicoesWeb/?wicket:interface=:1:2.

22 DEVANNY, Joe; MARTIN, Ciaran; STEVENS, Tim – «On the strategic consequences of digital espionage». In *Journal of Cyber Policy*. Londres. Vol. 3, N.º 6, 2021, pp. 429-450.

23 WATTS, Jonathan – «Brazil demands explanation from US over NSA spying». In *The Guardian*. Consultado em: janeiro de 2024. Disponível em: https://www.theguardian.com/world/2013/jul/08/brazil-demands-explanation-nsa-spying.

24 EDDY, Melissa – «File is said to confirm NSA spied on Merkel». Nytimes.com. Consultado em: janeiro de 2024. Disponível em: https://www.nytimes.com/2015/07/02/world/europe/file-is-said-to-confirm-nsa-spied-on-merkel.html.

25 REGAN, James; JOHN, Mark – «NSA spied on French presidents». In *WikiLeaks*. 2015. Consultado em: janeiro de 2024. Disponível em: https://www.reuters.com/article/idUSKBN0P32EA/.

26 MANZANO, Gabriel – «Documentos indicam que Petrobrás é espionada por agência americana». In *Estadão*. Consultado em: janeiro de 2024. Disponível em: https://politica.estadao.com.br/noticias/geral,documentos-indicam-que-petrobras-e-espionada-por-agencia-americana,1072697.

27 «DILMA DECIDE cancelar visita de Estado aos EUA, diz jornal». In *G1*. Consultado em: janeiro de 2024. Disponível em: https://g1.globo.com/politica/noticia/2013/09/dilma-decide-cancelar-visita-de-estado-aos-eua-diz-jornal-1.html.

28 BORGER, Julian – «Brazilian president: US surveillance a "breach of international law"». In *The Guardian*. Consultado em: janeiro de 2024. Disponível em: https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

29 «JORNAIS INTERNACIONAIS destacam ataque "feroz" de Dilma à espionagem dos EUA». BBC News Brasil. Consultado em: janeiro de 2024. Disponível em: https://www.bbc.com/portuguese/noticias/2013/09/130925_dilma_discurso_press_rw.

30 DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «The rise of cyber power in Brazil». In *Revista Brasileira de Política Internacional*. Brasília. Vol. 65, N.º 1, 2022, pp. 1-21.

31 TRAMITAÇÃO DA Lei 13709/2018. Câmara dos Deputados. Consultado em: janeiro de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066.

32 BAUMAN, Zygmunt, et al. – «After Snowden». In *International Political* Sociology. Oxford. Vol. 8, N.º 2, 2014, pp. 121-144; LYON, David – «Surveillance, Snowden, and big data». In *Big Data & Society*. Thousand Oaks. Vol. 1, N.º 2, 2014.

33 BIONI, Bruno Ricardo; RIELLI, Mariana Marques – «A construção multissetorial da LGPD: história e aprendizado». In *Proteção de Dados: Contexto, Narrativas e Elementos Fundantes*. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

34 LEI GERAL de Proteção de Dados. Presidência da República. Brasil. Consultado em: janeiro de 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

35 EBERT, Hannes; MAURER, Tim – «Contested cyberspace and rising powers». In *Third World Quarterly*. Oxford. Vol. 34, N.º 6, 2013, pp. 1054-1074; SEGAL, Adam – *The Hacked World Order*. Londres: Hachette, 2016.

36 LEI GERAL de Proteção de Dados.

37 TRAMITAÇÃO DA Lei 13709/2018.

38 BIONI, Bruno Ricardo; RIELLI, Mariana Marques – «A construção multissetorial da LGPD...».

39 LIMBERGER, Têmis – «Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI)». In *Revista de Direito Administrativo*. São Paulo. Vol. 281, N.º 1, 2022, pp. 113-144.

40 IRAMINA, Aline – «RGPD v. LGPD: adoção estratégica da abordagem responsivo na elaboração da Lei Geral de Proteção de Dados no Brasil e do Regulamento Geral de Proteção de Dados da União Europeia». In *Revista de Direito, Estado e Telecomunicações*. Brasília. Vol. 12, N.º 2, 2020, pp. 91-117.

41 LEI GERAL de Proteção de Dados.

42 EBERT, Hannes; MAURER, Tim – «Contested cyberspace and rising powers». In *Third World Quarterly*. Oxford. Vol. 34, N.º 6, 2013, pp. 1054-1074.

BIBLIOGRAFIA

«ASSINATURAS E ratificações da Convenção de Cibercrimes». Conselho da Europa. Consultado em: fevereiro de 2024. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

«ATRIZ CAROLINA Dieckmann é chantageada». In *O Estado de S. Paulo*. São Paulo, 6 de maio de 2012, p. C7.

BAUMAN, Zygmunt; BIGO, Didier; ESTEVES, Paulo; GUILD, Elspeth; JABRI, Vivienne; LYON, David; WALKER, R. B. J. – «After Snowden». In *International Political* Sociology. Oxford. Vol. 8, N.º 2, 2014, pp. 121-144. DOI: 10.1111/ips.12048.

BERGER, Peter; LUCKMANN, Thomas – *The Social Construction of Reality*. 1.ª edição. Nova Iorque: Open Road, 1966.

BIONI, Bruno Ricardo; RIELLI, Mariana Marques – «A construção multissetorial da LGPD: história e aprendizado». In *Proteção de Dados: Contexto, Narrativas e Elementos Fundantes*. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BORGER, Julian – «Brazilian president: US surveillance a "breach of international law"». In *The Guardian*. Consultado em: janeiro de 2024. Disponível em: https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

DAVID, René – *Major Legal Systems in the World Today*. Milwaukee: Stevens, 1985.
DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «Strategy in an uncertain domain: threat and response in cyberspace». In *Journal of Strategic Security*. Rapid City. Vol. 12, N.º 2, 2022, pp. 34-47. DOI: 10.5038/1944-0472.15.2.1954.

DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «The rise of cyber power in Brazil». In *Revista Brasileira de Política Internacional*. Brasília. Vol. 65, N.º 1, 2022, pp. 1-21. DOI: 10.1590/0034-7329202200113.

DEVANNY, Joe; MARTIN, Ciaran; STEVENS, Tim – «On the strategic consequences of digital espionage». In *Journal of Cyber Policy*. Londres. Vol. 3, N.º 6, 2021, pp. 429-450. DOI: 10.1080/23738871.2021.2000628.

«DILMA DECIDE cancelar visita de Estado aos EUA, diz jornal». In *G1*. Consultado em: janeiro de 2024. Disponível em: https://g1.globo.com/politica/noticia/2013/09/dilma-decide-cancelar-visita-de-estado-aos-eua-diz-jornal-1.html.

EBERT, Hannes; MAURER, Tim – «Contested cyberspace and rising powers». In *Third World Quarterly*. Oxford. Vol. 34, N.º 6, 2013, pp. 1054-1074. DOI: 10.1080/01436597.2013.802502.

EDDY, Melissa – «File is said to confirm NSA spied on Merkel». Nytimes.com. Consultado em: janeiro de 2024. Disponível em: https://www.nytimes.com/2015/07/02/world/europe/file-is-said-to-confirm-nsa-spied-on-merkel.html.

GORDON, Sarah; FORD, Richard – «On the definition and classification of cybercrime». In *Journal of Computer Virology*. Berlim. Vol. 13, 2006, pp. 13-20. DOI: 10.1007/s11416-006-0015-z.

GUTWIRTH, Serge; DE HERT, Paul; DE SUTTER, Laurent – «The trouble with technology regulation from a legal perspective». In *Regulating Technologies*. Oxford: Hart Publishers, 2008, pp. 193-218.

IRAMINA, Aline – «RGPD v. LGPD: adoção estratégica da abordagem responsivo na elaboração da Lei Geral de Proteção de Dados no Brasil e do Regulamento Geral de Proteção de Dados da União Europeia». In *Revista de Direito, Estado e Telecomunicações*. Brasília. Vol. 12, N.º 2, 2020, pp. 91-117. DOI: 10.26512/lstr.v12i2.34692.

INTERNATIONAL TELECOMMUNICATION UNION – *Global Cybersecurity Index 2020*. Consultado em: fevereiro de 2024. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

JOHNSON, David; POST, David – «Law and borders». In *Stanford Law Review*. Stanford. Vol. 48, N.º 5, 1996, pp. 1367-1402. DOI: 10.2307/1229390.

«JORNAIS INTERNACIONAIS destacam ataque "feroz" de Dilma à espionagem dos EUA». BBC News Brasil. Consultado em: janeiro de 2024. Disponível em: https://www.bbc.com/portuguese/noticias/2013/09/130925_dilma_discurso_press_rw.

LANCY, Nicola – «Historicising criminalisation». In *The Modern Law Review*. Lon-

dres. Vol. 72, N.º 6, 2009, pp. 936-960. DOI: 10.1111/j.1468-2230.2009.00775.x.

LEI GERAL de Proteção de Dados. Presidência da República. Brasil. Consultado em: janeiro de 2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

LIMBERGER, Têmis – «Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI)». In *Revista de Direito Administrativo*. São Paulo. Vol. 281, N.º 1, 2022, pp. 113-144. DOI: 10.12660/rda.v281.2022.85654.

LYON, David – «Surveillance, Snowden, and big data». In *Big Data & Society*. Thousand Oaks. Vol. 1, N.º 2, 2014. DOI: 10.1177/2053951714541861.

MADUEÑO, Denise – «Caso Carolina faz Câmara aprovar lei do crime cibernético». In *O Estado de S. Paulo*. São Paulo. 16 de maio de 2012, p. C7.

MANZANO, Gabriel – «Documentos indicam que Petrobrás é espionada por agência americana». In *Estadão*. Consultado em: janeiro de 2024. Disponível em: https://politica.estadao.com.br/noticias/geral,documentos-indicam-que-petrobras-e-espionada-por-agencia-americana,1072697.

MEDEIROS, Breno; GOLDONI, Luiz – «The fundamental conceptual trinity of cyberspace». In *Contexto Internacional*. Rio de Janeiro. Vol. 42, N.º 1, 2020, pp. 31-54. DOI: 10.1590/S0102-8529.2019420100002.

«MINUTA DA PNCiber». Gabinete de Segurança Institucional da Presidência da República. Consultado em: janeiro de 2024. Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf.

REGAN, James; JOHN, Mark – «NSA spied on French presidents». In *WikiLeaks*. 2015. Consultado em: janeiro de 2024. Disponível em: https://www.reuters.com/article/idUSKBN0P32EA/.

RONFELDT, David – «Cyberocracy is coming». In *The Information Society*. Nova Iorque. Vol. 8, N.º 4, 1992, pp. 243-296. DOI: 10.1080/01972243.1992.9960123.

SEGAL, Adam – *The Hacked World Order*. Londres: Hachette, 2016.

SMITH, Stephen – «Communication and the Constitution in cyberspace». In *Communication Education*. Londres. Vol. 43, N.º 2, 1994, pp. 87-101.

TRAMITAÇÃO DA Lei 12.737/2012. Câmara dos Deputados. Consultado em: janeiro de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011.

TRAMITAÇÃO DA Lei 13709/2018. Câmara dos Deputados. Consultado em: janeiro de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066.

TRAMITAÇÃO DE Projetos de Lei – crimes cibernéticos. Câmara dos Deputados. Consultado em: fevereiro de 2024. Disponível em: https://www.camara.leg.br/buscaProposicoesWeb/?wicket:interface=:1:2.

VALLE, Sabrina – «Carolina Dieckmann teve as fotos roubadas por hackers». In *O Estado de S. Paulo*. São Paulo, 14 de maio de 2012, p. C7.

VIRILIO, Paul – *El Cibermundo, la política de lo peor*. Madrid: Cultura Libre, 1997.

WATTS, Jonathan – «Brazil demands explanation from US over NSA spying». In *The Guardian*. Consultado em: janeiro de 2024. Disponível em: https://www.theguardian.com/world/2013/jul/08/brazil-demands-explanation-nsa-spying.

Consciência situacional como ferramenta estratégica da defesa cibernética

André Lucas Alcântara da Silva | *Gills Vilar-Lopes*[1]

INTRODUÇÃO

A segurança cibernética é fundamental no mundo atual, exigindo estratégias inovadoras para lidar com ameaças digitais em constante evolução. A consciência situacional (CS) emerge como uma ferramenta estratégica para proteger ativos digitais. Este artigo explora a teoria da CS, sua interseção com conceitos de estratégia em conflitos modernos e sua versão virtual, a consciência situacional cibernética (CSC), além de sua integração na defesa nacional.

O texto está dividido em quatro seções. A primeira explora a teoria da CS, inicialmente concebida em ambientes operacionais, mas aplicável ao domínio cibernético. São discutidos modelos conceituais e suas aplicações práticas, destacando sua importância na tomada de decisões. A segunda seção estabelece um paralelo entre CS e conceitos tradicionais de estratégia militar e aeroespacial, utilizando obras de Sun Tzu, Carl von Clausewitz e Giulio Douhet como referência. A terceira seção destaca a vertente cibernética da CS, a CSC. Nesse contexto, Singer e Friedman enfatizam que a CSC «se refere à habilidade de entender, prever e reagir eficientemente aos eventos cibernéticos»[2]. A evolução dessa teoria, desde suas bases conceituais até às aplicações práticas na esfera digital,

RESUMO

O crescimento tecnológico nas últimas décadas transformou diversas áreas da sociedade e do Estado, incluindo a defesa, devido à sua natureza tecnológica. Isso levantou discussões sobre o «espaço cibernético», o «poder cibernético» e o «domínio cibernético». O ciberespaço influencia os domínios operacionais tradicionais, tornando crucial o conhecimento do espaço cibernético, tanto próprio quanto dos adversários, como vantagem competitiva em conflitos entre Estados. Isso é conhecido como «consciência situacional», concebida por Mica Endsley nos anos 1980, definida como a capacidade de perceber, compreender e prever atividades em um espaço e tempo específicos. Esse conceito se desdobra no âmbito cibernético, criando a consciência situacional cibernética, o conhecimento das ações no espaço cibernético. Este artigo explora o papel estratégico da consciência situacional cibernética, identificando teorias e modelos de consciência situacional e seus desdobramentos na estratégia militar.

Palavras-chave: consciência situacional cibernética, defesa nacional, estratégia.

→

 https://doi.org/10.23906/ri2024.82a08

ABSTRACT

Situational awareness as a strategic tool for cyber defense

The technological growth of the last decades has changed the way many sectors of society and the state carry out their respective activities. The defense sector is part of this framework due to its essentially technological nature. With these changes, discussions began about phenomena known as 'cyberspace', 'cyber power', and 'cyber domain'. Because cyberspace permeates and can even influence the other operational domains (sea, land, air, and space), having the right knowledge of cyberspace – both one's own and that of one's adversaries – has become a competitive advantage in interstate conflicts. This knowledge is called situational awareness, a concept conceived in the 1980's by Mica Endsley, then Chief Scientist of the United States Air Force, and which can be defined as the ability to perceive and understand activities in a given time and space and to predict the future evolution of the situation. This concept can be unfolded in the cyber domain, giving rise to the so-called cyber situational awareness, which generally means the full knowledge of the actions occurring in the cyber space of interest. Thus, this article aims to elucidate the strategic role of cyber situational awareness, identifying the theories and models of its emerging concept and, subsequently, its developments in military strategy.

Keywords: cyber situational awareness, national defense, strategy.

é abordada aqui. A quarta seção explora a relação entre CSC e defesa nacional, integrando-as na proteção dos interesses nacionais e fortalecendo as capacidades de defesa cibernética e inteligência militar contra ameaças digitais.

Em suma, o artigo estabelece bases teóricas para a relevância da CS e CSC no domínio cibernético, visando proteger ativos digitais e defender contra ameaças cibernéticas contemporâneas.

CONSCIÊNCIA SITUACIONAL: CONCEITO, MODELOS E APLICABILIDADE

O conceito de CS pode ser definido como a consciência apropriada de uma situação específica[3]. De acordo com Stanton[4], o tema ganhou notoriedade na década de 1980, inicialmente na indústria da aviação, com o objetivo de melhorar a capacidade de decisão de pilotos e controladores de tráfego aéreo. Em situações de estresse, o responsável pela decisão deve identificar e interpretar as informações disponíveis para escolher a melhor ação.

Consoante Woods[5], para manter um nível aceitável de CS, é necessário acompanhar os acontecimentos e sua evolução ao longo do tempo, identificando «gatilhos» que indicam a necessidade de uma reação adequada. A CS é obtida de forma gradual, à medida que o cenário é compreendido pelo tomador de decisão. Com a evolução dos estudos relativos à CS, o conceito foi expandido para áreas distintas da aviação, mas que, igualmente, exigiam dos envolvidos um amplo conhecimento sobre determinado ambiente. Kaber e Endsley[6] entendem que a CS também pode ser utilizada em outros ambientes industriais devido a similaridades como: múltiplos objetivos simultâneos, tarefas concorrentes pela atenção e ambientes de alto estresse. Essas características comuns permitem extrapolar a aplicação da CS a cenários como a defesa, incluindo a defesa cibernética.

Os estudos sobre CS evoluíram, resultando em quatro teorias principais, cada uma com idiossincrasias específicas. A primeira, de Mica Endsley, define CS como «a percepção de elementos do ambiente dentro de um volume de tempo e espaço, a compreensão do seu significado e uma projeção do seu estatuto no futuro próximo»[7]. A segunda teoria, de Bedny e Meister[8], incorpora a dimensão temporal, enfatizando a adaptabilidade da

CS às mudanças nas condições operacionais. Em terceiro lugar, o modelo de Stanton[9] destaca a CS como uma habilidade distribuída, influenciada por fatores sociais, tecnológicos e organizacionais. Por último, o quarto modelo, de Smith e Hancock[10], conhecido como «ciclo perceptivo», evidencia o processo contínuo de percepção e interação humana no ambiente operacional, alcançando a CS através da repetição do processo de percepção e da postura proativa do elemento humano.

Essas teorias possuem pontos fortes e fracos, podendo ser aplicadas de forma isolada ou conjunta em diferentes cenários. A seguir, são detalhados aspectos particulares de cada uma delas.

MODELO DE ENDSLEY

O modelo de CS proposto por Endsley[11] oferece uma estrutura conceitual que delineia a percepção humana em ambientes complexos e dinâmicos. Constituído por três componentes interrelacionados – percepção da situação, compreensão da situação e projeção da situação – esse *framework* é conhecido como «modelo de três níveis». Esses níveis são progressivos: o nível 3, «projeção», é alcançado após o nível 2, «compreensão», que depende do nível 1, «percepção».

A fase inicial concentra-se na percepção dos elementos no ambiente, envolvendo a assimilação de informações sensoriais, como dados visuais e auditivos. Endsley destaca que a percepção é uma compreensão ativa do ambiente, fornecendo as entradas para o processo cognitivo subsequente.

No estágio seguinte, a compreensão da situação, as informações percebidas são interpretadas, permitindo um entendimento mais profundo do contexto. A compreensão evolui com novas informações, representando a transição crucial da percepção para a interpretação, fornecendo uma base sólida para a tomada de decisões.

A terceira componente, projeção da situação, envolve a capacidade de antecipar mudanças futuras no ambiente. A projeção permite prever eventos potenciais, proporcionando uma visão abrangente e preparando os tomadores de decisão para eventos futuros.

Essas três componentes formam um ciclo contínuo, constituindo a base do entendimento humano em ambientes complexos. O modelo de Endsley oferece uma estrutura robusta para a interação entre percepção, compreensão e projeção, aplicável a diversos contextos, incluindo o militar e o cibernético.

MODELO DE BEDNY E MEISTER

O modelo de Bedny e Meister[12] oferece uma perspectiva orientada às atividades individuais, integrando a dimensão temporal na construção da CS. Este modelo reconhece que a consciência da situação é dinâmica e evolui em resposta às mudanças operacionais. Bedny e Meister argumentam que a CS não pode ser compreendida sem considerar seu desenvolvimento ao longo do tempo. Assim, a adaptação e atualização constante da compreensão da situação tornam-se centrais na construção da CS.

O modelo destaca a necessidade de uma CS adaptativa, implicando que os indivíduos devem ajustar continuamente sua compreensão da situação para refletir as condições em evolução.
Em operações militares/cibernéticas, em que a dinâmica do campo de batalha pode mudar abruptamente, a capacidade de antecipar e reagir a alterações na situação é vital.

MODELO DE STANTON

O modelo de CS proposto por Stanton[13] destaca-se por sua abordagem inovadora, fundamentada na teoria da habilidade distribuída. Diferente dos modelos tradicionais, este reconhece que a CS é uma habilidade distribuída entre indivíduos e sistemas, crucial em ambientes complexos e dinâmicos. Stanton argumenta que a CS não reside apenas na mente individual, mas é compartilhada entre elementos sociais, tecnológicos e organizacionais, enfatizando a colaboração e a comunicação como componentes essenciais.
A teoria da habilidade distribuída desafia as concepções tradicionais que limitam a inteligência ao indivíduo, postulando que a realização de tarefas envolve a interação entre pessoas, artefatos tecnológicos e o ambiente. Em seu estudo sobre sistemas colaborativos, Hollan, Hutchins e Kirsh[14] afirmam que «o processo cognitivo estende-se para além dos limites da cabeça humana», mostrando que a inteligência é moldada pela comunicação e interação entre componentes distribuídos.
Ao adaptar essa teoria para ambientes cibernéticos, Stanton destaca a relevância dessa abordagem na defesa cibernética contemporânea[15]. Reconhece-se que a CS em contextos digitais não pode ser concebida apenas como uma função individual, mas como um fenômeno coletivo que abrange analistas, operadores de sistemas de segurança e outros atores relevantes.

MODELO DE SMITH E HANCOCK

A teoria do ciclo perceptivo, desenvolvida por Smith e Hancock[16], oferece uma visão dinâmica da CS, destacando a interação contínua entre ser humano e máquina. A CS é vista como um processo ativo de percepção e interpretação constante das informações do ambiente operacional. A percepção ativa, essencial segundo a teoria, implica na busca proativa por dados relevantes, especialmente em ambientes dinâmicos. A abordagem encontra aplicação em contextos operacionais complexos, como operações militares, onde a capacidade de perceber e reagir rapidamente é crucial. Assim, a teoria ressalta a importância da percepção ativa para manter uma CS eficaz em ambientes desafiadores, enfatizando a necessidade de envolvimento contínuo na obtenção e interpretação das informações.

CONSCIÊNCIA SITUACIONAL E ESTRATÉGIA MILITAR

Apesar de grande parte dos estudos relativos à CS ter sido realizada do final da década de 1980 em diante, a história revela que o conceito já havia sido aplicado

pelo piloto alemão Oswald Boelke durante a Primeira Guerra Mundial. Naquela ocasião, ele percebeu a importância de se obter uma consciência do inimigo antes que este pudesse fazer o mesmo[17]. Boelke apontou como o conhecimento do inimigo pode ser decisivo para o sucesso em um conflito, algo também observado por Sun Tzu em *A Arte da Guerra*, fornecendo uma base rica para entender a CS à luz das teorias modernas.

APESAR DE GRANDE PARTE DOS ESTUDOS RELATIVOS À CS TER SIDO REALIZADA DO FINAL DA DÉCADA DE 1980 EM DIANTE, O CONCEITO JÁ HAVIA SIDO APLICADO PELO PILOTO ALEMÃO OSWALD BOELKE DURANTE A PRIMEIRA GUERRA MUNDIAL.

A CS, em si, se dá a partir de um importante insumo: a informação. De acordo com Endsley[18], o primeiro e mais elementar nível da CS é a «percepção dos elementos de um ambiente». Nele, de fato, ainda não há informação, apenas dados disponíveis. A partir deles, o indivíduo deve ter a capacidade de correlacioná-los, dando-lhes significado e chegando ao segundo nível da CS, que trata da «compreensão da situação atual». Neste ponto, sim, existe informação. A maneira como esta informação será tratada pode levar o indivíduo ao nível mais alto de CS, a «previsão do estado futuro de uma situação». Bem, a forma como este processo cognitivo é desenhado, tendo como principal componente a informação, possibilita que tal conceito seja analisado à luz das principais teorias relativas aos estudos estratégicos e da própria guerra.

Sun Tzu, o estrategista chinês do século IV a. C., em sua obra clássica *A Arte da Guerra*[19], fornece uma base rica para entender a CS à luz das teorias modernas. Os princípios filosóficos e estratégicos de Sun Tzu podem ser conectados aos elementos fundamentais das quatro teorias contemporâneas de CS, apresentadas anteriormente:

a) Conhecimento profundo do ambiente: Sun Tzu enfatiza a importância de conhecer o terreno e compreender o ambiente operacional. Em paralelo, o modelo de Endsley destaca a necessidade de uma percepção completa da situação, enfatizando «a percepção do ambiente, incluindo os fatores relevantes no espaço e no tempo»[20]. Essa conexão ressalta a importância do entendimento profundo do ambiente em ambas as perspectivas.

b) Adaptação constante: o estrategista chinês aborda a necessidade de adaptação constante às circunstâncias em mudança. Esse princípio ecoa no modelo de Stanton, que destaca a adaptabilidade como um elemento essencial da CS, incorporando a ideia de «habilidade distribuída» que se ajusta às demandas operacionais.

c) Antecipação e prevenção: Sun Tzu sublinha a importância de antecipar os movimentos do inimigo e evitar conflitos diretos quando possível. Essa abordagem preventiva encontra paralelos na teoria do ciclo de percepção, de Smith e Hancock[21], que destaca a antecipação como um resultado do contínuo processo de «percepção» do ambiente, permitindo a projeção de eventos futuros e, consequentemente, a um estado de CS eficaz.

Por sua vez, Carl von Clausewitz[22], renomado estrategista prussiano do século XIX, também pode ser utilizado para correlacionar a CS e os conceitos de estratégia militar. Em sua obra magistral *Da Guerra*, introduziu o conceito de «névoa da guerra» para descrever a incerteza e a falta de clareza que permeiam os campos de batalha. Ao explorar essa noção, pode-se estabelecer uma ponte com as teorias modernas de CS.

a) «Névoa da guerra» como incerteza: Clausewitz argumenta que a névoa da guerra resulta da incerteza inerente a todas as operações militares, a qual está alinhada com o reconhecimento, no modelo de Endsley[23], de que a CS envolve a percepção e compreensão de eventos em um ambiente dinâmico e incerto.
b) Adaptação à «névoa da guerra»: o general prussiano destaca a necessidade de adaptação constante devido à «névoa da guerra». Essa ideia ressoa com o modelo de Stanton[24], que enfatiza a adaptabilidade como uma característica central da CS, especialmente na teoria da habilidade distribuída.
c) Ciclo de percepção: a «névoa da guerra», de Clausewitz, também pode ser relacionada à teoria do ciclo de percepção, de Smith e Hancock, uma vez que ambos os conceitos reconhecem a limitação da percepção e a necessidade de constantes ciclos de atualização da situação.

Além da «névoa da guerra», outros princípios e conceitos de Carl von Clausewitz em *Da Guerra* podem ser correlacionados com as teorias modernas de CS, oferecendo uma perspectiva mais abrangente. Veja-se:

a) Centro de gravidade e foco estratégico: Clausewitz introduz o conceito de centro de gravidade como o ponto crucial que, se atacado, pode levar à derrota do inimigo. Na CS, a percepção do «centro de gravidade» de uma situação, ou seja, o ponto central que influencia o curso dos eventos, é essencial. O modelo de Endsley, por exemplo, enfatiza a importância de compreender os elementos cruciais no ambiente.
b) Fricção e desafios na percepção: a «fricção» em Clausewitz refere-se às dificuldades e desafios inerentes à guerra. Esse conceito pode ser relacionado à «fricção» na CS, reconhecendo que a percepção e a compreensão de uma situação estão sujeitas a desafios e dificuldades constantes. O modelo de Stanton destaca a necessidade de superar a «fricção cognitiva», uma vez que, em sua perspectiva, o conhecimento necessário para se obter a CS está distribuído e, por vezes, não organizado[25].

Outro conhecido teórico da guerra, o general Giulio Douhet[26], também abordou tópicos e pensamentos considerados nos modelos de CS. Em seu conhecido trabalho *O Domínio do Ar*, no início do século XX, estabeleceu princípios fundamentais sobre o poder aeroespacial. Sua visão revolucionária sobre o papel da aviação nas operações

militares pode ser correlacionada com o conceito de CS, especialmente considerando o contexto aeroespacial:

a) Domínio do ar e percepção global: Douhet defendia a ideia de que o controle do domínio do ar era crucial para o sucesso militar. Essa perspectiva se alinha com a CS no sentido de que a percepção global do ambiente, incluindo elementos no espaço e no tempo, é fundamental. O modelo de Endsley destaca a importância da percepção abrangente.
b) Velocidade e pronta resposta: o general enfatizava a importância da velocidade e da resposta rápida no poder aeroespacial. Essa ênfase encontra paralelo na teoria da habilidade distribuída de Stanton, que destaca a necessidade de uma resposta ágil em ambientes dinâmicos[27].

CONSCIÊNCIA SITUACIONAL CIBERNÉTICA: UMA EXPLORAÇÃO CONCEITUAL

A consciência situacional cibernética (CSC) é uma extensão do conceito de CS para o espaço cibernético, herda as bases conceituais da CS tradicional, mas as adapta ao ambiente digital complexo. Enquanto a CS tradicional lida com elementos físicos, a CSC lida com eventos em redes digitais complexas. Assim como a CS, a CSC é crucial em ambientes críticos que exigem alta atenção e capacidade de decisão. Ela pode ser definida como a percepção de eventos e dados de rede, compreendendo seu significado em termos de missão, recursos, conectividade, ameaças e vulnerabilidades, e projetando seu estado futuro próximo[28].

Ao migrar para a CSC, novas dimensões surgem, como a percepção e a compreensão de eventos em redes digitais. Autores como David D. Woods e Erik Hollnagel[29] destacam a importância de considerar as características únicas do ambiente cibernético.

No entanto, seria equivocado concluir que a CSC é uma mera aplicação da teoria de CS ao contexto cibernético. Na verdade, ela demanda uma abordagem interdisciplinar, incorporando conceitos da teoria de sistemas, da ciência da computação e da engenharia de *software*. Em outras palavras, há de se considerar, além das bases teóricas de CS, os aspectos intrínsecos do ambiente cibernético, o qual é composto não apenas pela componente tecnológica, mas também humana e processual. Ademais, de forma similar ao seu conceito ascendente, a CSC não deve encontrar um fim em si, mas integrar processos mais amplos visando o auxílio na tomada de decisão estratégica. Porém, para compreender a CSC, é essencial contextualizá-no campo mais amplo da CS e explorar as teorias existentes.

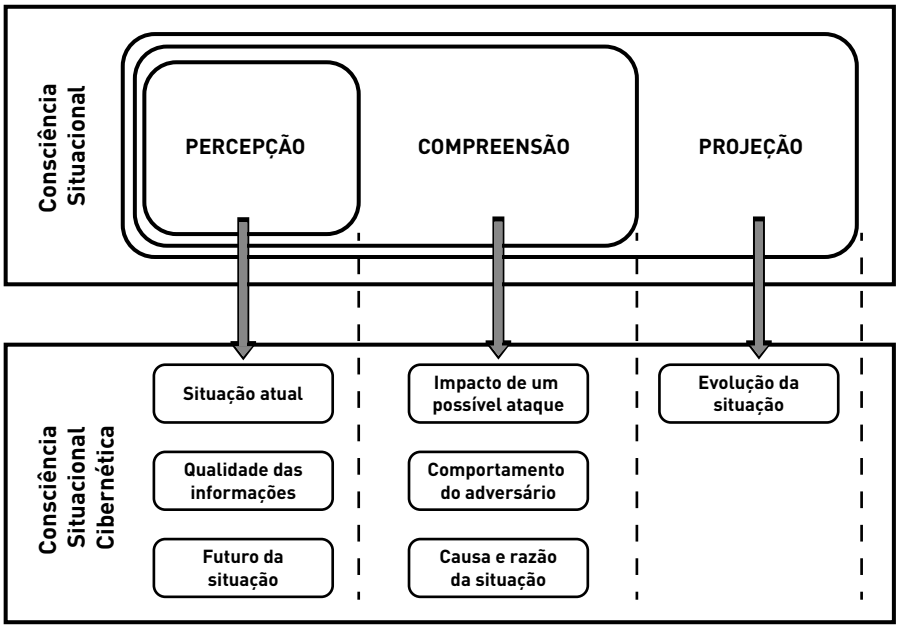
DE FORMA SIMILAR AO SEU CONCEITO ASCENDENTE, A CSC NÃO DEVE ENCONTRAR UM FIM EM SI, MAS INTEGRAR PROCESSOS MAIS AMPLOS VISANDO O AUXÍLIO NA TOMADA DE DECISÃO ESTRATÉGICA.

Dessa forma, existem facetas que precisam ser consideradas para a obtenção de uma CSC efetiva, a saber: (i) avaliação do atual estado da rede de computadores; (ii) com-

preensão do impacto de um ataque cibernético; (*iii*) compreensão do comportamento do atacante; (*iv*) compreensão das causas do ataque sofrido; (*v*) compreensão da confiabilidade de qualquer consciência obtida; e (*vi*) conhecimento das posições de ataque e defesa, para identificar ações futuras.

De maneira sintética, o conceito de CSC, comparado à CS, pode ser evidenciado pelo diagrama da figura 1.

Figura 1 > Consciência situacional cibernética a partir dos níveis de consciência situacional



Fonte: Elaboração própria.

A avaliação dos parâmetros teóricos da CSC pode ser conduzida considerando a aderência das principais teorias de CS. Cada uma delas oferece perspectivas distintas, e a seleção apropriada deve ponderar os elementos específicos enfatizados no estudo. Por exemplo, o modelo de Endsley destaca-se pela sua aplicabilidade em ambientes cibernéticos, enfatizando a compreensão rápida da situação e a tomada de decisões eficazes diante de ameaças. Suas fases oferecem uma estrutura robusta para investigações no domínio cibernético.

Por sua vez, a teoria da habilidade distribuída de Stanton revela-se pertinente ao considerar a distribuição de tarefas e funções nesses ambientes. Sua ênfase na distribuição da cognição entre diferentes elementos do sistema oferece uma abordagem valiosa para analisar a interação complexa.

Já a teoria do ciclo perceptivo de Smith e Hancock concentra-se nos processos perceptivos dos operadores, sendo relevante para compreender como informações são percebidas e interpretadas em cenários cibernéticos.
Por fim, o modelo de Bedny e Meister destaca a interação entre elementos do sistema, sendo especialmente pertinente na consideração da interdependência entre atores humanos e sistemas tecnológicos em ambientes cibernéticos. Embora a ampla compreensão da CSC passe, necessariamente, pelos conceitos e teorias estabelecidos no âmbito da CS, uma aplicação eficaz no ambiente cibernético pode extrapolar tais referências. Portanto, torna-se latente uma abordagem interdisciplinar sobre o tema, considerando, também, as especificidades inerentes a um ambiente tecnológico cada vez mais complexo, aliado aos objetivos desejados ao se aplicar a CSC. Tal abordagem, de acordo com Jajodia e Albanese[30], passa pela definição do «espaço cibernético de interesse», ou seja, de uma fração do espaço cibernético ao qual o tomador de decisão deseja obter a CS necessária.

CONSCIÊNCIA SITUACIONAL CIBERNÉTICA E A DEFESA NACIONAL

De acordo com a Política Nacional de Defesa (PND) brasileira, a defesa nacional pode ser compreendida como:

> «o conjunto de atitudes, medidas e ações do Estado, com ênfase na expressão militar, para a defesa do Território Nacional, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas»[31].

Por sua vez, o *Livro Branco de Defesa Nacional* (LBDN) brasileiro reforça que este conceito de defesa nacional:

> «além de ser importante vetor para a preservação da Soberania Nacional, também possibilita a manutenção da integridade territorial, a consecução dos objetivos nacionais, a proteção ao povo e a garantia de não ingerência externa no território nacional»[32].

Ambos os documentos, em conjunto com a Estratégia Nacional de Defesa (END), formam o principal arcabouço teórico/estratégico do Brasil, o qual direciona, principalmente, sua componente militar.
A partir dessas referências, o Brasil descreve e delimita áreas que podem afetar ou comprometer a integridade do território brasileiro, a soberania e os objetivos nacionais. É neste viés que o setor cibernético ganha notoriedade. O LBDN aponta como o referido setor pode influenciar a própria defesa nacional quando assume que:

> «a possibilidade de o País sofrer um ataque cibernético de origens das mais diversas e de difícil identificação, que poderão causar danos consideráveis a estruturas estratégicas

> ou mesmo a outros setores de importâncias vitais para a nação brasileira, faz com que a Defesa Cibernética passe a ter importância fundamental para a Defesa Nacional»[33].

Desta feita, o Brasil assume a relevância estratégica do tema (cibernético) e inicia um novo ciclo de envolvimento e desenvolvimento do setor, com vistas à defesa nacional. A partir de então, o Brasil abre espaço para discussões relativas aos inúmeros conceitos que circundam o assunto – como: domínio cibernético, espaço cibernético e poder cibernético –, bem como as perspectivas que analisam se tal componente poderia ser considerada um novo domínio operacional, a exemplo daqueles já reconhecidos (mar, terra, ar e espaço exterior). Inevitavelmente, a reflexão sobre estes conceitos leva a uma análise de como são interpretados pelos principais estudiosos contemporâneos que abordam o fenômeno, além de uma avaliação da forma como os grandes *players* do cenário internacional assumem a questão cibernética.

Neste contexto, considerando a perspectiva acadêmica, é quase unânime o reconhecimento estratégico da componente cibernética, sendo esta capaz de proporcionar vantagens significativas em uma situação de conflito, visto que possui condições de influenciar os domínios operacionais já existentes. Na visão de Nocetti[34], o domínio cibernético possui características particulares por se tratar de algo criado pelo próprio homem e que, além disso, sofre mudanças em um ciclo muito mais veloz se comparado aos demais domínios. O mesmo autor, ainda, reforça que tais especificidades proporcionam uma menor barreira de entrada para que novos atores passem a agir neste domínio, o que, em última instância, poderia gerar conflitos em tal ambiente, os quais seriam denominados como «guerra cibernética». Assim, surge o conceito de poder cibernético o qual é definido, de forma ampla, como:

> «a capacidade de proteger e promover os interesses nacionais no ciberespaço e através dele: considerar os benefícios que o ciberespaço oferece aos nossos cidadãos e à nossa economia, trabalhar com os parceiros para um ciberespaço que reflita os nossos valores e utilizar as cibercapacidades para influenciar os acontecimentos no mundo real»[35].

No âmbito de tais discussões, Lonsdale[36] introduz o conceito de infoesfera, em que este sim poderia ser considerado um domínio estratégico. Para ele, tal conceito é ainda mais amplo se comparado à interpretação de «espaço cibernético», o qual seria considerado apenas como mais uma componente da infoesfera. Já o ponto de vista exposto por Gray[37] destoa dos anteriores, uma vez que este reconhece a natureza relevante do setor cibernético, porém não o interpreta como sendo um novo domínio operacional, mas, sim, um «atuador» e «habilitador» importante naqueles já existentes. Nesta mesma esteira, Rid[38] ressalta que ataques cibernéticos não poderiam ser interpretados como atos de guerra por si só, simplesmente pelo fato de não se enquadrarem nos conceitos que definem a guerra. Para ele, tais ações são «apenas versões sofisticadas de três atividades que são tão antigas quanto a própria guerra: sabotagem, espionagem e subversão»[39].

Diante das várias discussões sobre o tema, inúmeros países assumiram o espaço cibernético como um novo domínio operacional, passando a incluí-lo de forma categórica em seus respectivos documentos estratégicos. O Brasil, por sua vez, é claro ao descrever a posição nacional em sua mais nova versão da Doutrina Militar de Defesa Cibernética[40], publicada em 2023.

INÚMEROS PAÍSES ASSUMIRAM O ESPAÇO CIBERNÉTICO COMO UM NOVO DOMÍNIO OPERACIONAL, PASSANDO A INCLUÍ-LO DE FORMA CATEGÓRICA EM SEUS RESPECTIVOS DOCUMENTOS ESTRATÉGICOS.

O Brasil, na esteira dos acontecimentos relevantes ocorridos no espaço cibernético nos últimos anos, reconhece esse ambiente como um domínio operacional, no qual ações cibernéticas ofensivas e defensivas tendem a potencializar ou complementar as ações realizadas nos demais domínios (terra, mar, ar e espaço).

A partir desta concepção e, conforme delineado na PND, na END e no *LBDN*, considerando a importância na obtenção e manutenção do conhecimento neste novo domínio operacional, a CSC se apresenta como uma ferramenta valiosa na consecução da defesa nacional, uma vez que esta propõe a percepção, compreensão e projeção de atividades que ocorram no espaço cibernético de interesse.

Assim, é possível identificar um novo desafio a ser superado pelos tomadores de decisão, qual seja: como se organizar para obter uma CSC efetiva e que, de fato, colabore diante dos conflitos contemporâneos? Nesse aspecto, países e organizações buscam encontrar um modelo que seja aplicável às suas necessidades.

A partir desse objetivo, em uma de suas várias iniciativas em torno do assunto, os Estados Unidos, por intermédio de seu Departamento de Defesa, financiam pesquisadores no âmbito do programa Multidisciplinary University Research Initiative para tratar do assunto. Alguns desses pesquisadores, Sushil Jajodia e Massimiliano Albanese, conceberam um modelo conhecido como «Integrated Framework for Cyber Situation Awareness»[41]. Nele, são abordadas capacidades necessárias para uma CSC eficaz, como as habilidades de: enxergar o cenário de defesa cibernética de forma holística; gerenciar incertezas; raciocinar, mesmo diante de um ambiente «ruidoso» e com nível de conhecimento limitado, dentre outras.

Outro exemplo, na busca por uma CSC que atenda às necessidades identificadas, é o modelo proposto pelo coronel da Força Aérea dos Estados Unidos, Rizwan Ali, no âmbito da Task Force Cyber do Supreme Headquarters Allied Powers Europe (SHAPE-NATO), e conhecido como «cyber situational awareness for the NATO Alliance»[42]. O modelo é baseado em três componentes: consciência das ameaças existentes; consciência da rede de dados e demais componentes tecnológicos de interesse; consciência do objetivo a ser alcançado.

No Brasil, há iniciativas em torno da busca por uma melhor CSC. No âmbito da defesa nacional, é possível destacar as iniciativas que envolvem o Sistema Militar de Defesa Cibernética que, de acordo com a Doutrina Militar de Defesa Cibernética[43],

é estruturado nos níveis estratégico, operacional e tático, e implicam tanto o Ministério da Defesa, quanto as estruturas de defesa cibernética das Forças Armadas, tendo o Comando de Defesa Cibernética (ComDCiber) como órgão central do sistema.
De forma geral, a partir das ações de considerar o domínio cibernético em documentos estratégicos, bem como a busca por modelos e estruturas organizacionais que colaborem para uma CSC eficaz, demonstra como os países, inclusive o Brasil, enxergam a componente cibernética como estratégica para a defesa nacional.

CONCLUSÃO

No arcabouço dos estudos estratégicos e da influência exercida pela componente cibernética sobre os domínios tradicionais, o presente artigo se propôs a identificar o papel estratégico da CSC no âmbito da defesa nacional. Para tanto, foram descritas as bases teóricas e modelos do seu conceito ascendente, ou seja, da CS, e como essa vem sendo aplicada em atividades complexas e operacionais desde a década de 1980. Dessa forma, quatro modelos teóricos foram identificados. O primeiro deles, e mais amplo, descrito por Mica Endsley. Em seguida, aqueles definidos por Bedny e Meister; Staton; e Smith e Hancock. Todos com suas peculiaridades, porém, mantendo a mesma base interpretativa de Mica Endsley.
A partir desses modelos, foi possível traçar um paralelo entre a CS e os princípios estratégicos delineados por Sun Tzu, Clauzewitz e Giulio Douhet. Além disso, o artigo buscou detalhar o conceito de CS no âmbito cibernético, se referindo a CSC. Essa, por sua vez, também encontrando aplicabilidade em ambientes críticos, os quais requerem um nível de atenção elevado e grande capacidade de decisão. Ou seja, no escopo do espaço cibernético de interesse, foi possível perceber a necessidade de percepção, compreensão e projeção de um determinado evento cibernético. Por fim, uma vez que os principais documentos estratégicos de defesa no Brasil como a PND, a END e o LBDN tratam e consideram a importância da componente cibernética para a Defesa Nacional, torna-se latente a capacidade de a CS ser utilizada como ferramenta estratégica no âmbito da defesa cibernética. RI

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

André Lucas Alcântara da Silva Capitão engenheiro da computação no Comando de Operações Aeroespaciais (COMAE) – Força Aérea Brasileira (FAB).

> Força Aérea Brasileira (FAB), SHIS – Lago Sul, Brasília DF, 70297-400, Brasil | alcantaraalas@fab.mil.br

Gills Vilar Lopes Professor permanente do Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA) da Universidade da Força Aérea (UNIFA).

> Universidade da Força Aérea (UNIFA) Av. Marechal Fontenele, 1200, Jardim Sulacap, Rio de Janeiro/RJ, 21750-000, Brasil | gillsgvl@fab.mil.br

NOTAS

1 A presente investigação foi realizada com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

2 SINGER, Peter W.; FRIEDMAN, Alan – *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2017. Disponível em: https://doi.org/10.1093/wentk/9780199918096.001.0001. Tradução livre dos autores.

3 SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive, externally directed consciousness». In *Human Factors Journal*. Vol. 37, N.º 1, 1997, pp. 137-148.

4 STANTON, Neville A. – «Hierarchical task analysis: developments, applications, and extensions». In *Applied Ergonomics*. Vol. 37, N.º 1, 2006, pp. 55-79.

5 WOODS, David D. – «Coping with complexity: the psychology of human behaviour in complex systems». In *Tasks, Errors and Mental Models: A Festschrift to Celebrate the 60th Birthday of Professor Jens Rasmussen*. Londres: Routledge, 1988.

6 KABER, David B.; ENDSLEY, Mica R. – «Out-of-the-loop performance problems and the use of intermediate levels of automation for improved control system functioning and safety». In *Process Safety Progress*. Vol. 16, N.º 3, 1997, pp. 126-131. DOI: https://doi.org/10.1002/prs.680160304.

7 ENDSLEY, Mica R. – «Design and evaluation for situational awareness enhancement». In *Proceedings of the Human Factors Society 32nd Annual Meeting*. Anaheim: 24-28 de outubro de 1998, pp. 97-101. Tradução livre a partir do original.

8 BEDNY, G.; MEISTER, D. – «How do professionals reason in real-world situations? Implications for the design of decision support». In *Handbook of Human Factors and Ergonomics*. 2.ª edição. 1999, pp. 1118-1142.

9 STANTON, Neville A.; CHAMBERS, Peter R. G.; PIGGOTT, John – «Situational awareness and safety». In *Safety Science*. Vol. 39, N.º 3, dezembro de 2001, pp. 189-204.

10 SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive...».

11 ENDSLEY, Mica R. – «Toward a theory of situation awareness in dynamic systems». In *Human Factors Journal*. Vol. 37, N.º 1, 1995, pp. 32-64.

12 BEDNY, G.; MEISTER, D. – «How do professionals reason in real-world situations?...».

13 STANTON, Neville A.; CHAMBERS, Peter R. G.; PIGGOTT, John – «Situational awareness and safety».

14 HOLLAN, James; HUTCHINS, Edwin; KIRSH, David – «Distributed cognition: toward a new foundation for human-computer interaction research». In *ACM Transactions on Computer-Human Interaction*. Vol. 7, N.º 2, 2000, pp. 174-196.

15 STANTON, Neville A. – «Hierarchical task analysis...».

16 SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive...».

17 STANTON, Neville A.; CHAMBERS, Peter R. G.; PIGGOTT, John – «Situational awareness and safety».

18 ENDSLEY, Mica R. – «Design and evaluation for situational awareness enhancement».

19 TZU, Sun – *A Arte da Guerra*. São Paulo: Martin Claret, 2010.

20 ENDSLEY, Mica R. – «Toward a theory of situation awareness in dynamic systems». Tradução livre dos autores.

21 SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive...».

22 CLAUSEWITZ, Carl von – *Da Guerra*. Brasília, DF: Editora UnB, 1984.

23 ENDSLEY, Mica R. – «Design and evaluation for situational awareness enhancement».

24 STANTON, Neville A. – «Hierarchical task analysis...».

25 *Ibidem*.

26 DOUHET, Giulio – *O Domínio do Ar*. São Paulo: Bibliex, 2010.

27 STANTON, Neville A. – «Hierarchical task analysis...».

28 GUTZWILLER, Robert – *Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment Through 2015*. San Diego: NIWC Pacific, 2019.

29 HOLLNAGEL, Erik; WOODS, David D. – *Joint Cognitive Systems: Patterns in Cognitive Systems Engineering*. CRC Press. 2005.

30 JAJODIA, Sushil; ALBANESE, Massimiliano – «An integrated framework for cyber situation awareness». In *Theory and Models for Cyber Situation Awareness*. Berlim: Springer, 2017.

31 *POLÍTICA NACIONAL de Segurança da Informação*. Brasília, DF: Gabinete de Segurança Institucional, 2018.

32 *LIVRO BRANCO de Defesa Nacional*. Brasília, DF: Ministério da Defesa, 2012.

33 *Ibidem*.

34 NOCETTI, Julien – «Cyber power». In *Routledge Handbook of Russian Foreign Policy*. Londres: Routledge, 2018, pp. 182--198; «DEVELOPMENTS IN the field of information and telecommunications in the context of international security». United Nations. 2019. DOI: https://www.un.org/disarmament/ict-security/.

35 DEVANNY, Joseph – «The review and responsible, democratic». In *Centre for Defence Studies. The Integrated Review in Context*. 2021, p. 62. Tradução livre a partir do original.

36 LONSDALE, David J. – «Information power: strategy, geopolitics, and the fifth dimension». In *Journal of Strategic Studies*. Vol. 22, N.º 2-3, junho de 1999, pp. 137-157.

37 GRAY, Colin S. – *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*. Washington, DC: Strategic Studies Institute, US Army War College, 2013.

38 RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies* Vol. 35, N.º 1, 2012, pp. 5-32.

39 *Ibidem*. Tradução livre dos autores.

40 *DOUTRINA MILITAR de Defesa Cibernética*. Brasília, DF: Ministério da Defesa, 2023.

41 JAJODIA, Sushil; ALBANESE, Massimiliano – «An integrated framework for cyber situation awareness».

42 ALI, Colonel Rizwan – «Situational awareness for The Nato Alliance». In *The Three Swords Magazine*. N.º 30, 2016, pp. 72-75. Disponível em: https://www.jwc.nato.int/images/stories/_news_items_/2016/Cyber_Situational_Awareness.pdf.

43 *DOUTRINA MILITAR de Defesa Cibernética*.

BIBLIOGRAFIA

ALI, Colonel Rizwan – «Situational awareness for the Nato Alliance». In *The Three Swords Magazine*. N.º 30, 2016, pp. 72-75. Disponível em: https://www.jwc.nato.int/images/stories/_news_items_/2016/Cyber_Situational_Awareness.pdf.

BEDNY, G.; MEISTER, D. – «How do professionals reason in real-world situations? Implications for the design of decision support». In *Handbook of Human Factors and Ergonomics*. 2.ª edição. 1999, pp. 1118--1142.

CLAUSEWITZ, Carl von – *Da Guerra*. Brasília, DF: Editora UnB, 1984.

DEVANNY, Joseph – «The review and responsible, democratic». In *Centre for Defence Studies. The Integrated Review in Context*. 2021, p. 62.

«DEVELOPMENTS IN the field of information and telecommunications in the context of international security». United Nations. 2019. DOI: https://www.un.org/disarmament/ict-security/.

DOUHET, Giulio – *O Domínio do Ar*. São Paulo: Bibliex, 2010.

DOUTRINA MILITAR de Defesa Cibernética. Brasília, DF: Ministério da Defesa, 2023.

ENDSLEY, Mica R. – «Toward a theory of situation awareness in dynamic systems». In *Human Factors Journal*. Vol. 37, N.º 1, 1995, pp. 32-64. DOI: https://doi.org/10.1518/001872095779049543.

ENDSLEY, Mica R. – «Design and evaluation for situational awareness enhancement». In *Proceedings of the Human Factors Society 32nd Annual Meeting*. Anaheim: 24-28 de outubro de 1998, pp. 97-101. DOI: https://doi.org/10.1177/154193128803200221.

GRAY, Colin S. – *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*. Washington, DC: Strategic Studies Institute, US Army War College, 2013.

GUTZWILLER, Robert – *Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment Through 2015*. San Diego: NIWC Pacific, 2019.

HOLLAN, James; HUTCHINS, Edwin; KIRSH, David – «Distributed cognition: toward a new foundation for human-computer interaction research». In *ACM Transactions on Computer-Human Interaction*. Vol. 7, N.º 2, 2000, pp. 174-196. DOI: http://dx.doi.org/10.1145/353485.353487.

HOLLNAGEL, Erik; WOODS, David D. – *Joint Cognitive Systems: Patterns in Cognitive Systems Engineering*. CRC Press. 2005.

JAJODIA, Sushil; ALBANESE, Massimiliano – «An integrated framework for cyber situation awareness». In *Theory and Models for Cyber Situation Awareness*. Berlim: Springer, 2017.

KABER, David B.; ENDSLEY, Mica R. – «Out--of-the-loop performance problems and the use of intermediate levels of automation for improved control system functioning and safety». In *Process Safety Progress*. Vol. 16, N.º 3, 1997, pp. 126-131. DOI: https://doi.org/10.1002/prs.680160304.

LIVRO BRANCO de Defesa Nacional. Brasília, DF: Ministério da Defesa, 2012.

LONSDALE, David J. – «Information power: strategy, geopolitics, and the fifth dimension». In *Journal of Strategic Studies*. Vol. 22, N.º 2-3, junho de 1999, pp. 137-157.

NOCETTI, Julien – «Cyber power». In *Routledge Handbook of Russian Foreign Policy*. Londres: Routledge, 2018, pp. 182-198.

POLÍTICA NACIONAL de Segurança da Informação. Brasília, DF: Gabinete de Segurança Institucional, 2018.

RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies* Vol. 35, N.º 1, 2012, pp. 5-32. DOI: https://doi.org/10.1080/01402390.2011.608939.

SINGER, Peter W.; FRIEDMAN, Alan – *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2017. DOI: https://doi.org/ 10.1093/wentk/9780199918096.001.0001.

SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive, externally directed consciousness». In *Human Factors Journal*. Vol. 37, N.º 1, 1997, pp. 137-148. DOI: https://doi.org/10.1518/001872095779049444.

STANTON, Neville A. – «Hierarchical task analysis: developments, applications, and extensions». In *Applied Ergonomics*. Vol. 37, N.º 1, 2006, pp. 55-79. DOI: https://doi.org/10.1016/j.apergo.2005.06.003.

STANTON, Neville A.; CHAMBERS, Peter R. G.; PIGGOTT, John – «Situational awareness and safety». In *Safety Science*. Vol. 39, N.º 3, dezembro de 2001, pp. 189-204.

TZU, Sun – *A Arte da Guerra*. São Paulo: Martin Claret, 2010.

WOODS, David D. – «Coping with complexity: the psychology of human behaviour in complex systems». In *Tasks, Errors and Mental Models: A Festschrift to Celebrate the 60th Birthday of Professor Jens Rasmussen*. Londres: Routledge, 1988.

RELAÇÕES INTERNACIONAIS

R:I

DESCRIÇÃO DO PROCEDIMENTO DE ARBITRAGEM CIENTÍFICA

A *Relações Internacionais* é a revista do Instituto Português de Relações Internacionais, publicada desde Março de 2004. É uma publicação académica trimestral, de reflexão e debate sobre questões internacionais. Tem como objetivos abordar as grandes questões da atualidade internacional numa perspetiva pluralista e multidisciplinar e fomentar o debate teórico na área das Relações Internacionais. As áreas primordiais de publicação são a política internacional, a história, a estratégia, a segurança e defesa, a política comparada, a economia e o direito internacional.

1. Normas de publicação

Os artigos submetidos à R:I devem ser originais e não deverão ser submetidos a outras publicações, sendo avaliados de acordo com o sistema de *peer review.* Os textos podem ser submetidos em português, inglês, francês e espanhol, sendo a língua de publicação da revista o português. Os autores conferem à R:I o exclusivo dos direitos de publicação sob qualquer forma. Os artigos não são remunerados.

Os artigos não devem exceder as seis mil palavras, incluindo notas de rodapé. O artigo deve incluir uma bibliografia, um resumo e quatro palavras-chave (em português e inglês).

As recensões devem ter cerca de 1500 palavras e conter os dados de identificação completos da publicação, bem como deve ser enviada a capa do livro. Deverão ter um título original e ser intercaladas com, pelo menos, dois subtítulos.

As provas tipográficas dos artigos aprovados para publicação serão, quando solicitadas, enviadas aos autores para revisão.

A Bibliografia deve conter exclusivamente as referências bilbiográficas mencionadas ao longo do texto e seguir a norma 405 do IPQ. Ao longo do artigo, as referências bibliográficas devem aparecer em nota de rodapé:

a) Citação de livro: APELIDO, Nome dos autor(es) – *Título do livro*. Edição. Local de Publicação: Editor, Ano.

b) Citação de capítulo de livro: APELIDO, Nome dos autor(es) – «Título da contribuição/capítulo». In *Título do livro*. Local de Publicação: Editor, Ano. Páginas.

c) Citação de artigo de revista: APELIDO, Nome dos autor(es) – «Título do artigo». In *Título da revista*. Local de Publicação. V., N.º, Ano, Páginas.

d) Citação de recursos na web: APELIDO, Nome dos autor(es) – *Título do documento*. Consultado em: data de consulta]. Disponível em: endereço na Internet.

Os artigos devem ser enviados por e-mail, em formato Word, para o endereço: **revistaipri@fcsh.unl.pt**

2. Declaração de Ética e Más Práticas de Publicação

Com vista a garantir a honestidade e integridade académica a *R:I* assume o compromisso de assegurar as boas práticas éticas e deontológicas na avaliação e publicação dos artigos propostos. Todas as partes envolvidas, autores, editores e avaliadores, deverão contribuir para que os padrões de comportamento ético sejam assegurados, tal como definido pelas orientações do *Committee on Publication Ethics (COPE)*. Assim cada uma das partes deve comprometer-se com o seguinte:

Editores:

- São responsáveis pelos conteúdos publicados na revista;
- Esforçar-se por conhecer os interesses dos leitores e dos autores, assim como por melhorar constantemente a revista;
- Fazer uma avaliação das propostas com base exclusivamente no mérito académico;
- Não devem usar informação não publicada para a investigação própria sem o consentimento expresso do autor;
- Assegurar a existência de um processo de arbitragem científica justo, imparcial e em tempo útil, bem como a transparência nos processos de edição e publicação dos manuscritos;
- Garantir a confidencialidade dos manuscritos;
- Contribuir para a integridade do arquivo da *R:I*.

Autores:

- Os artigos devem apresentar uma discussão objetiva da importância da investigação com suficiente detalhe e referências que permitam a replicação do modelo utilizado;
- Garantir que o seu trabalho é original, e se o trabalho de outros autores estiver a ser usado, tal deve ser explicitamente referido;
- Qualquer forma de plágio constitui um comportamento não ético e é inaceitável, da mesma forma que submeter o mesmo manuscrito a mais do que uma revista;
- Em caso de trabalhos de coautoria, deve ser garantido o consenso na aprovação da versão final do manuscrito para avaliação ou publicação;
- As recensões devem também ser objetivas, abrangentes e conter estados da arte precisos.

Avaliadores:

- Garantir a confidencialidade durante o processo de arbitragem;
- Manifestar a existência de conflito de interesses;
- Não utilizar para benefício próprio as ideias obtidas através do processo de arbitragem;
- A recomendação de aceitar ou rejeitar um manuscrito deve ser baseada na sua importância, originalidade e clareza, assim como na validade do estudo e no seu enquadramento no escopo da revista;
- A avaliação deve ser objetiva e as recomendações devem ser suportadas em argumentos sólidos para que os autores possam melhorar o texto; devem ser recomendadas publicações relevantes quando estas não são citadas;
- Quando o manuscrito não se enquadra na sua área de investigação ou quando sabe que não consegue cumprir o prazo, deve informar os editores;
- Respeitar os prazos estabelecidos.

IPRI

INSTITUTO PORTUGUÊS DE RELAÇÕES INTERNACIONAIS
UNIVERSIDADE NOVA DE LISBOA

O Instituto Português de Relações Internacionais – Universidade NOVA de Lisboa (IPRI-NOVA) é um instituto de investigação científica fundado pela Universidade Nova de Lisboa, a Fundação Luso-Americana para o Desenvolvimento e a Fundação Oriente, com o apoio da Fundação Calouste Gulbenkian e em parceria com a Universidade de Georgetown e o Instituto Universitário Europeu de Florença.

As Relações Internacionais são a disciplina autónoma mais moderna das ciências sociais, contando já com um corpo teórico e uma produção científica consideráveis, e uma inscrição institucional bem definida na Universidade. Em Portugal, o seu desenvolvimento concentrou-se, essencialmente, na dimensão pedagógica, sem uma afirmação correspondente no domínio da investigação científica, apesar do número crescente de investigadores portugueses com formação teórica em Relações Internacionais, os quais, em geral, completaram os seus estudos no estrangeiro. Por outro lado, não cessa de crescer a importância das questões internacionais, quer para a formulação de políticas públicas, quer para o debate político e a opinião pública. Neste sentido, parecem não só criadas as condições, como justificadas as razões para a fundação de uma instituição universitária de investigação científica em Relações Internacionais.

O IPRI-NOVA tem como primeiro objetivo a investigação científica no campo das Relações Internacionais, num quadro interdisciplinar; como segundo objetivo, criar uma escola portuguesa de investigadores em Relações Internacionais, pautada por critérios de excelência e integrada nas redes científicas internacionais, em particular europeias e norte-americanas; como terceiro objetivo, desenvolver não só investigação teórica, mas também investigação aplicada capaz de responder às necessidades da comunidade e do mercado determinadas pela internacionalização da sociedade portuguesa.

A revista *Relações Internacionais* é a publicação trimestral do IPRI-NOVA, que se constitui como uma revista académica de reflexão e debate sobre as relações internacionais, numa linha pluralista e de abertura a todos os campos científicos e a todas as escolas de Relações Internacionais.