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. RI

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.