Vol. 1, Nº. 1 (Sep./Dec. 2025)
www.cybersecuritypolicies.com.br

O ciberespaço na agenda de defesa britânica

Natália Diniz Schwether[1*]

Resumo

O presente estudo visa responder ao questionamento geral: como o Reino Unido tem se organizado para enfrentar as ameaças no ciberespaço? Para tanto, a principal estratégia de pesquisa é a exploração de fontes primárias e secundárias e documentos oficiais do Governo e das Forças Armadas, de forma a entender em maior profundidade as dinâmicas do caso. São achados relevantes da pesquisa a orquestração dos documentos estratégicos de segurança e defesa britânicos, os quais orientam a atuação conjunta e em simultâneo nos cinco domínios operacionais, com destaque para o poder cibernético.

Palavras-Chave: Defesa; Cibernética; Estudo de Caso; Reino Unido.

Cyberspace on the British defense agenda

Abstract

This study aims to answer the general question: how has the United Kingdom organized itself to face threats in cyberspace? To this end, the main research strategy is the exploration of primary and secondary sources and official documents from the Government and the Armed Forces, in order to understand in greater depth the dynamics of the case. Relevant research findings include the orchestration of strategic British security and defense documents, which guide joint and simultaneous action in the five operational domains, with emphasis on cyber power.

Keywords: Defense; Cybernetics; Case Study; United Kingdon.

1 * Doutora em Ciência Política pela Universidade Federal de Pernambuco (UFPE). Atualmente realiza Pós-Doutorado no Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina (UFSC). E-mail para contato: n.schwether@unesp.br.
O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Introdução

Prognósticos futuros apontam para grandes desafios advindos do avanço tecnológico. De maneira geral, manter a dianteira no cenário internacional exige dos Estados competência para atuação no espaço cibernético, de forma a assegurar os objetivos de segurança nacional. O ciberespaço e as operações cibernéticas são, cada vez mais, importantes para projeção de poder e garantia da soberania estatal. Os ataques cibernéticos tornaram-se uma das ameaças prioritárias, compelindo os países à criação de estruturas seguras e resilientes e ao comprometimento de diversos setores e atores.

Nessa conjuntura, as informações são, mais do que nunca, importantes armas de guerra e áreas como a cibernética, a Inteligência Artificial (IA) e a automação são o centro da atenção. Flexibilidade, adaptabilidade e agilidade são elementares e, de forma a acompanhar o acelerado ritmo das inovações, as Forças Armadas devem estar preocupadas em modernizar tanto a forma como se organizam, treinam e se equipam, quanto como tomam suas decisões (Abbott; Haberlin, 2019).

Nesse sentido, o Reino Unido destaca-se por ser um dos países que está na vanguarda quanto às ações adotadas para a segurança e a defesa cibernética. Desde 2010, o governo do país, por meio do *National Security Risk Assessment*, relacionou as ameaças cibernéticas como prioridade para a segurança nacional. Elaborou, ainda, três estratégias nacionais de segurança cibernética, em 2011, 2016 e 2022 nas quais foram estabelecidos, entre outros, os três principais atores que ciberneticamente ameaçam a nação: os Estados hostis, as organizações terroristas e os grupos criminosos organizados.

Diante disso, esse artigo visa responder ao questionamento geral: como o Reino Unido, tem se organizado para enfrentar as ameaças no ciberespaço? Para isso, a principal estratégia de pesquisa será a exploratória, a qual ao realizar um levantamento bibliográfico de documentos primários e secundários permite-nos entender em maior profundidade as dinâmicas do caso, em especial como evoluiu e se organizou o setor cibernético.

De maneira mais específica, foi eleita a técnica de análise global de textos, a qual preza por fornecer uma visão geral dos documentos, seguida da compilação dos conceitos e enunciados centrais, isto é, faculta-nos depreender a ideia geral dos textos e compreender cada uma das partes que conformam o argumento.

Considerando que, estudar o futuro da guerra em sua vertente cibernética exige compreensão não apenas do ambiente operacional, natureza e características, mas deve estar aliado, também, a apreensão da estrutura e do planejamento das Forças Armadas para o setor, esse texto foi assim dividido: na primeira seção são apresentados os documentos que contêm os mais altos objetivos de defesa e segurança do Reino Unido, com recorte para a cibernética, na segunda parte o enfoque recai sobre o planejamento estratégico das Forças Armadas e a sua articulação com os objetivos estatais. Por fim, a última seção dedica-se a examinar o comportamento estratégico e militar do Reino Unido no ciberespaço.

1. Os Grandes Planos

A primeira grande revisão de defesa, após a Segunda Guerra Mundial, foi publicada pelo Reino Unido, em 1957. Desde então, foram produzidas ao menos uma revisão por década. Nela os diferentes governos têm a oportunidade de apresentar uma visão prospectiva dos interesses da nação e os requisitos militares para a sua consecução. Além de examinar o cenário de defesa e segurança, identificar possíveis ameaças e definir a melhor maneira de organizar e equipar as suas Forças Armadas (Brooke-Holland, Mills, Walker, 2023).

Em 2010, o primeiro Governo de coalizão, anunciou a *Strategic Defence and Security Review* (SDSR) e o compromisso de realizar atualizações desse documento a cada cinco anos. A Revisão que, até aquele momento, era restrita à área de defesa, passou a abranger, também, questões diplomáticas, fronteiriças e de segurança (Brooke-Holland, Mills, Walker, 2023).

Em dezembro de 2019, foram anunciados os planos para uma nova Revisão, a ser publicada em 2021. O momento era caracterizado pelo retorno da competição entre as grandes potências e por conflitos persistentes. Para o alto comando das Forças Armadas seriam as novas capacidades - cibernética, IA e *big data* – que sobressairiam no campo de combate e equilibrariam o menor efetivo (Strachan, 2021).

Assim, a Revisão Integrada de Segurança, Defesa, Desenvolvimento e Política Externa, *Global Britain in a Competitive Age*, reúne as grandes tendências que irão moldar o ambiente internacional e a segurança nacional, em 2030. 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 ciber segurança são apontadas, desde o princípio, como fundamentais (HM Government, 2021).

Diferentemente de suas antecessoras, a Revisão é muito mais explícita no que tange à estratégia (Strachan, 2021). Para isso, o quadro estratégico define quatro principais objetivos: i. apoiar a ciência e a tecnologia, fortalecendo a posição do Reino Unido como poder cibernético responsivo; ii. moldar a ordem internacional futura, de maneira a torná-la ainda mais favorável às democracias e aos valores universais, reforçando e renovando os pilares existentes da ordem internacional e estabelecendo novos, a exemplo do ciberespaço; iii. fortalecer a segurança e a defesa para enfrentar desafios no mundo físico e online; iv. ser resiliente, aprimorando a habilidade para responder e se recuperar de possíveis ataques (HM Government, 2021).

Outrossim, são listadas algumas adaptações necessárias para lidar com os desafios da próxima década. 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, consequentemente, deter poder cibernético[2] terá uma importância crescente (HM Government, 2021).

Em vista disso, a Revisão propõe adotar uma estratégia mais abrangente e utilizar o

2 11. O poder cibernético é a capacidade de proteger e promover os interesses nacionais no ciberespaço.

domínio cibernético de modo mais integrado e criativo, retirando o foco da segurança cibernética e considerando toda a gama de capacidades – incluindo as ofensivas – na detecção, interrupção e dissuasão de possíveis ameaças. Ao mesmo tempo, pretende reunir esforços para a obtenção de tecnologias cibernéticas críticas, bem como agir no ambiente internacional para influenciar o futuro do ciberespaço (HM Government, 2021).

Isto posto, são listadas ações estratégicas prioritárias, como: i. Fortalecer o ecossistema cibernético do Reino Unido, aprofundando a parceria governo, academia e indústria, com investimentos em educação, apoio à pesquisa e à indústria no desenvolvimento de produtos e serviços inovadores; ii. Proporcionar um ambiente cibernético seguro aos cidadãos e a proteção de seus dados, permitindo uma transformação digital da economia; iii. Liderar a produção de tecnologias vitais como os microprocessadores, as tecnologias quânticas e novas formas de transmissão de dados, diminuindo os riscos da dependência de suprimentos; iv. Promover um ciberespaço livre, aberto, pacífico e seguro, por meio de uma ação conjunta com outros governos na defesa das normas internacionais e na responsabilização dos adversários pelas violações; v. Detectar, interromper e dissuadir adversários, utilizando de forma integrada todo o espectro – legal, diplomático, militar, econômico, de inteligência e comunicação – para impor custos e frear a capacidade de adversários prejudicarem a nação (HM Government, 2021).

Elencam, ainda, a necessidade de melhor preparar as Forças Armadas para o combate no amplo espectro, seja estando atentos aos novos domínios – cibernético e espacial – ou ao desenvolvimento de capacidades e tecnologia de ponta para os demais (HM Government, 2021).

Não obstante, uma das maiores ênfases da Revisão ser no papel que o poder cibernético detém na consecução dos interesses nacionais, o documento deixa importantes lacunas, especialmente, no que tange ao uso responsável e democrático desse poder, ao preconizar o emprego de capacidades defensivas e ofensivas.

Exemplo disso é a proposta de um expressivo aumento no efetivo da Força Cibernética Nacional, indicando que a conduta exclusivamente resiliente, adotada até então, por si só não foi suficiente para conter os crimes cibernéticos (Devanny, 2021, Steed, 2021).

Se, por um lado, há um claro apoio à perpetuação de um modelo de governança do ciberespaço, por outro, a Revisão demonstra a intenção do Reino Unido em aumentar seu poder cibernético, não apenas para se proteger, mas para assumir um protagonismo no cenário internacional (Devanny, 2021, Steed, 2021).

Visualiza-se, portanto, na Revisão, grandes ambições para o setor cibernético britânico, contudo, como podermos depreender à continuidade, é a Estratégia Nacional Cibernética (ENC) o documento que mais se aproxima da tentativa de elencar prioridades e traçar um plano de ação.

Lançada em dezembro de 2021, a ENC foi erigida sobre três principais conclusões da Revisão: o poder cibernético é um fator cada vez mais importante para alcançar os objetivos nacionais; deter poder cibernético exige uma visão abrangente e uma estratégia integrada; e, toda a sociedade deve atuar em conjunto para o sucesso das ações (HM Government, 2021a).

No cerne da Estratégia está, portanto, o conceito de poder cibernético, paralelamente, a pretensão de que, em 2030, o Reino Unido possa permanecer como um dos principais poderes cibernéticos do mundo. Para tanto, cinco pilares dão sustentação ao planejamento estratégico: 1. Aprofundar a parceria governo, academia e indústria; 2. Construir um ambiente digital resiliente e próspero; 3. Assumir a dianteira tecnológica; 4. Liderar e influenciar a ordem internacional; 5. Detectar, interromper e dissuadir adversários (HM Government, 2021a).

A articulação, a distribuição de papéis e a coordenação das ações, realizada para cada um dos pilares, demonstra a disposição para alcançar os objetivos propostos. O presente estudo adentra o quinto pilar - "Conter Ameaças" -, o único com participação direta do Ministério da Defesa e da Força Cibernética Nacional, conforme pode ser observado na figura abaixo (Figura 1):

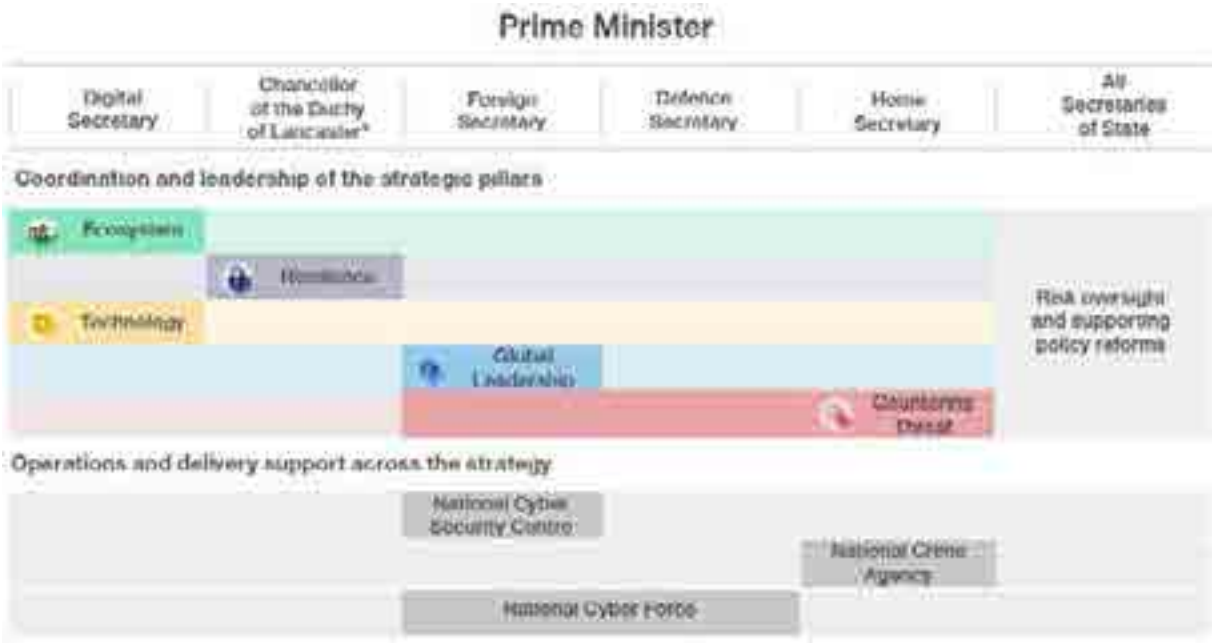


Figura 1. Estratégia Nacional Cibernética – Responsabilidades
Fonte: HM Government, 2021.

O quinto pilar da ENC se concentra em garantir ao Reino Unido seu pleno potencial como poder cibernético e em aumentar os custos de um ataque ao país. Para isso, prevê o desenvolvimento contínuo da Força Cibernética Nacional (NCF, na sigla em inglês) e esforços intergovernamentais no enfrentamento das ameaças, na investigação e na detecção de criminosos (HM Government, 2021a).

Nesse sentido, estabelece três objetivos a serem atingidos até 2025. O primeiro deles **- detecção dos criminosos e proteção dos interesses** – implica em aumentar o investimento em agências de inteligência, aumentar a capacidade de fiscalização e enfrentamento ao crime cibernético, aprimorar a coordenação na detecção das ameaças, conceder um acesso conjunto às bases de dados, compreender o comportamento dos adversários, colaborar para uma divulgação célere dos relatórios de incidentes cibernéticos, investir na capacidade de inteligência cibernética

da Agência de Crime Nacional (NCA, na sigla em inglês), expandir a rede de defensores cibernéticos, com apoio do *Government Cyber Coordination Centre* e do *Cyber Collaboration Centr*e, dar continuidade às pesquisas desenvolvidas no Instituo Alan Turing sobre o uso de *machine learning* na detecção de ataques (HM Government, 2021a).

O segundo objetivo - **dissuadir agentes maliciosos** – está associado à percepção dos adversários sobre os custos em atacar o Reino Unido, para tanto, pretende-se atualizar a legislação existente para otimizar a sua aplicação, rever a política e a abordagem do governo no enfrentamento de *ransomware*s, maximizar as parcerias entre a NCF, o Centro Nacional de Segurança Cibernética (NCSC, na sigla em inglês), a NCA e as comunidades de inteligência e diplomáticas e assegurar a capacitação dos oficiais (HM Government, 2021a).

Ao terceiro objetivo - **apoiar a segurança nacional, prevenir e detectar crimes** – compete a ampliação da NCF e sua integração com o serviço de inteligência britânico (*Government Communications Headquarters* – GCHQ), Ministério da Defesa (MOD), Serviço de Inteligência Secreta e com o Laboratório de Ciência e Tecnologia de Defesa (Dstl, na sigla em inglês), e torná-la apta para conduzir operações cibernéticas ofensivas legais e proporcionais (HM Government, 2021a).

2. Planejamento Estratégico da Defesa

O desenvolvimento da força futura do Reino Unido é conduzido pelo Centro de Desenvolvimento, Conceitos e Doutrina (DCDC, na sigla em inglês), departamento do Ministério da Defesa britânico responsável por produzir análises detalhadas do horizonte futuro, conceitos e doutrina, a partir de pesquisas e experimentação baseadas em evidências.

A sua publicação com maior alcance temporal é o *Global Strategic Trends* (GST), o qual fornece um contexto estratégico imparcial para aqueles envolvidos no desenvolvimento de planos, políticas e capacidades no longo prazo, de forma que os tomadores de decisão possam estar isentos de um viés em suas escolhas e, mais do que isso, consigam transformar desafios e ameaças em boas oportunidades de aprimoramento (MOD, 2018).

Doravante sua primeira publicação, em 2003, o GST é elementar ao processo de concepção das Revisões estratégicas nacionais, bem como fornece sustentação a uma cadeia de documentos de utilidade para a defesa e a segurança. Cita-se, por exemplo, o *Future Operating Environment 2035* (FOE 35), inspirado na edição de 2014 do GST.

De maneira introdutória, o FOE35 reflete sobre a crescente globalização e seus impactos no futuro ambiente operacional. Por um lado, apresenta a necessidade de respostas militares mais rápidas e ágeis, por outro destaca o surgimento de atores, estatais e não estatais, economicamente menos poderosos, mas capazes de exercer influência no cenário internacional por meio, por exemplo, de ataques cibernéticos (MOD, 2015).

Nesse contexto, identifica a tecnologia como uma das principais impulsionadoras da mudança militar. Os custos reduzidos e uma gama maior de atores com acesso a armas

sofisticadas, torna premente a adaptabilidade dos sistemas de defesa, tanto para permitir a interoperabilidade quanto para a modernização (MOD, 2015).

De acordo com o documento, a simples aquisição de capacidades não será suficiente, mais do que isso está a velocidade com que a defesa será capaz de adaptar e integrar as tecnologias. Entre as tecnologias listadas como centrais no futuro, estão: o anti-acesso e a negação de área, seja por sistemas antissatélites espaciais ou terrestres ou por meio da cibernética ofensiva e defensiva; os sistemas remotos e automatizados; os mísseis supersônicos e hipersônicos; e, as tecnologias quânticas, com alta capacidade de processamento e comunicação segura, codificação e decifração de mensagens sensíveis e detecção de precisão. Somam-se, ainda, a importância da análise de *big data* e a onipresença dos recursos de vigilância em tempo real (MOD, 2015).

No que tange ao ciberespaço, o FOE 35 defende que, até 2035, ele permeará, em grau muito maior, todos os aspectos dos ambientes físicos. As operações cibernéticas devem ser consideradas como atividades principais, frente à dependência cada vez maior das redes de informação, assim como a proteção cibernética e a resiliência serão essenciais (MOD, 2015).

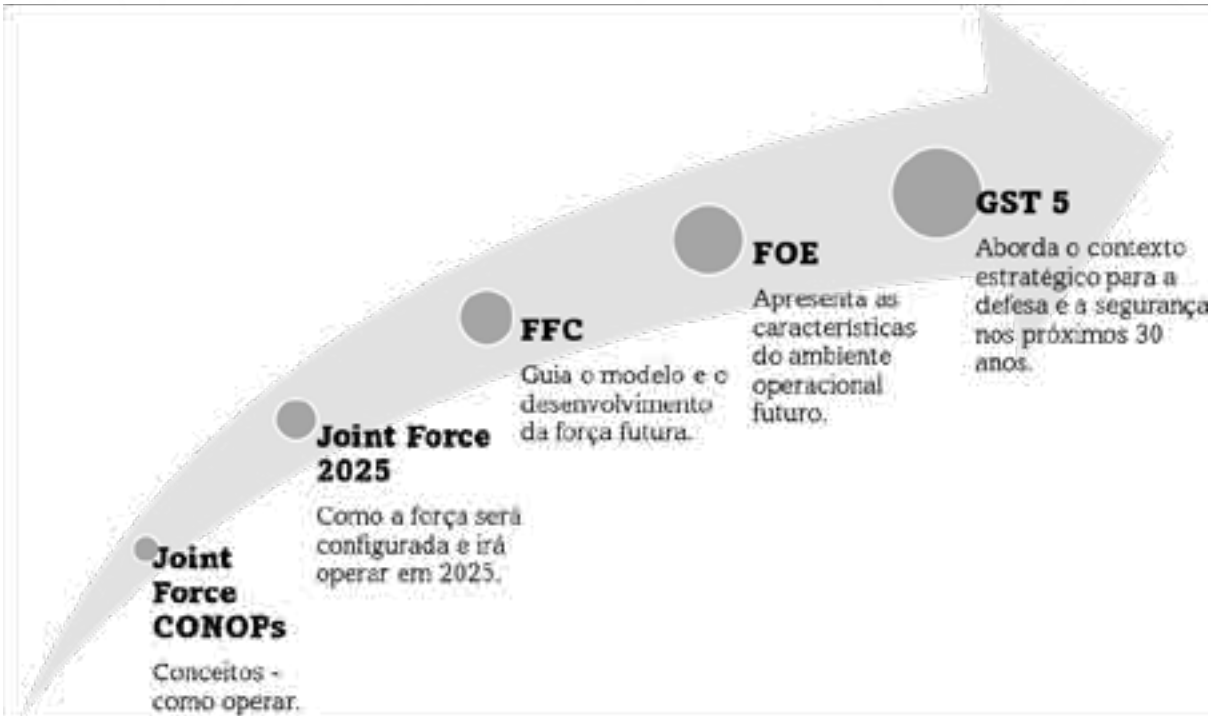
Em virtude de sua natureza descentralizada e dispersa, o ciberespaço permanecerá poroso e vulnerável. Mesmo que contestado por diversos atores, o domínio total será impossível. Diante disso, projetam-se grandes desafios para a segurança da informação e das infraestruturas, com ataques cibernéticos crescendo em escopo, frequência e impacto e adversários progressivamente mais adaptáveis (MOD, 2015).

Portanto, garantir a resiliência do sistema e da infraestrutura é fundamental. Propõe-se, para tanto, uma maior conscientização sobre as ameaças, aliado a capacidade de utilizar de maneira inovadora as capacidades cibernéticas, as quais serão, até 2035, o elemento principal das operações conjuntas (MOD, 2015).

Em linha com o FOE35, o DCDC apresentou, em 2017, o *Future Force Concept* (FFC), o qual fornece orientação geral para o desenvolvimento estratégico futuro da força, para os seguintes dez a vinte anos. Nele foi identificado como central o aprimoramento da ação conjunta nos cinco domínios operacionais – cibernético, espacial, marítimo, terrestre e aéreo (MOD, 2017).

Nesse sentido, o documento projeta que o domínio cibernético, em virtude de seu largo alcance, desempenhará um papel, cada vez mais, importante e vital em todas as fases de uma operação. E, portanto, atividades como: especialização cibernética, comando e controle ágeis, resiliência, treinamento e educação e o desenvolvimento e compreensão das normas e protocolos para o emprego dos recursos cibernéticos, são elencadas como prioritárias para o futuro da força (MOD, 2017).

Figura 2. Conceito Futuro de Força



Fonte: Elaborado pela autora com base em MOD, 2017.

Não obstante, na sexta edição do GST, publicada em 2018, uma das tendências que chama a atenção é a centralidade da informação. De acordo com os analistas, o poder de processamento, o volume, a variedade de dados e a conectividade continuarão em crescimento exponencial, o que impulsionará o desenvolvimento da IA e da computação quântica (MOD, 2018).

A digitalização alterará, ainda, a interação social, à medida em que as pessoas passarão mais tempo em atividades no ciberespaço. As mídias sociais (e suas bolhas) serão capazes de polarizar populações, corroer a confiança nas instituições e criar incertezas (MOD, 2018).

A regulação e a proteção eficaz do ciberespaço é, portanto, um dos desafios a ser enfrentado pelo Reino Unido, de forma a evitar que criminosos e outros agentes mal-intencionados possam realizar ataques cibernéticos e espalhar a desinformação. Um espaço informacional onde há pouco ou nenhum controle, torna os indivíduos mais suscetíveis à desinformação e/ou radicalização (MOD, 2018).

Na esteira desse pensamento, o documento recomenda medidas defensivas e ofensivas para proteção contra os ataques físicos e cognitivos no ciberespaço. Sugere, ainda, o estabelecimento de fronteiras cibernéticas nacionais ou regionais para a defesa contra as ameaças cibernéticas. E, propõe uma mudança de postura, alternando de uma postura defensiva/reativa, para uma abordagem concertada de todo o governo (MOD, 2018).

No tocante, especificamente, ao tema do conflito e da segurança o documento ressalta que a ordem mundial está em mudança, desafiando as normas e as instituições existentes. Nesse ambiente, a competição entre os Estados e outros atores tende a se intensificar, os quais usarão,

cada vez mais, uma abordagem híbrida, indo além das atividades militares e econômicas e abrindo novas arenas para o conflito (MOD, 2018).

Nesse cenário, os analistas são persuasivos ao afirmarem que o ciberespaço tem potencial para se tornar o teatro vital do futuro, com atores estatais e não estatais buscando, continuamente, pelas vulnerabilidades dos adversários. Aliado à implantação da IA, a qual poderá ser usada para fornecer defesas automáticas, combater as ameaças em constante mudança, bem como para ataques cibernéticos dinâmicos (MOD, 2018).

3. Linhas de Ação

O Reino Unido, na última década, liderou uma política nacional de fortalecimento da cibersegurança e conscientização da população, além de ter desenvolvido uma ampla gama de capacidades para responder às ameaças de atores hostis.

Desde 2011, o governo britânico segue uma estratégia nacional e um programa de investimentos constantes no setor. Sobressaem a criação do Centro Nacional de Segurança Cibernética e da Força Cibernética Nacional, assim como o desenvolvimento de um ecossistema cibernético com mais de 1200 empresas de segurança cibernética (HM Government, 2021a).

Nesse último aspecto, uma das iniciativas mais chamativas e inovadoras foi o plano *Active Cyber Defence*, o qual propõe enfrentar, em parceria com a indústria, de uma maneira relativamente automatizada, uma proporção significativa dos ataques, reduzindo os danos e fornecendo ferramentas de proteção (HM Government, 2021a).

Novas regulamentações, a exemplo da *UK General Data Protection Regulation*, e leis especializadas, também, impactaram de forma positiva a segurança cibernética. 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 (HM Government, 2021a).

No que tange às novas estruturas, o NCSC, formalmente constituído em 2016, é responsável pelas infraestruturas críticas nacionais e atua em parceria com a NCA, incumbida por conter e investigar crimes digitais. A Agência, equipes cibernéticas e forças policiais locais agem de maneira coordenada nos casos de crimes.

Houve investimento, ainda, em capacidades cibernéticas para deter, punir e aumentar os custos aos atores maliciosos no ciberespaço. Em 2014, foi criado, de uma colaboração entre o Ministério da Defesa e o GCHQ, o *National Offensive Cyber Programme*, o programa atendia à lógica da dissuasão e reação; ou seja, com ele o Reino Unido deixava claro que se defenderia de possíveis ataques e que a capacidade cibernética faria parte do planejamento estratégico das operações militares (HM Government, 2021a).

Mais recentemente, em 2018, o governo designou fundos para dar um passo além e criar a NCF. Projetada, especialmente, para conduzir operações ofensivas em apoio às prioridades de segurança nacional do Reino Unido, a NCF se tornou operacional em 2020. A NCF foi tanto

uma reação ao aumento das ameaças, quanto uma tentativa de otimizar o setor, por meio de uma organização civil-militar que estivesse ajustada aos recursos disponíveis (HM Government, 2021a).

A NCF reúne pessoal do serviço de inteligência britânico, do Ministério da Defesa, do Serviço de Inteligência Secreta e do Laboratório de Ciência e Tecnologia de Defesa, os quais estão, pela primeira vez, sob um comando unificado. As diferentes expertises atuam em conjunto, ainda, com capacidades diplomáticas, econômicas, políticas e militares. No ambiente internacional, a Força está integrada em alianças, como a Organização do Tratado do Atlântico Norte (OTAN) e a *Five Eyes*[3], e possui uma série de parceiros, com ênfase para os países europeus e os Estados Unidos (NCF, 2023).

Em 2023, o documento *Responsible Cyber Power in Practice* forneceu mais detalhes sobre os princípios operacionais da NCF. Foram elencadas três grandes categorias de operações: i. combater ameaças terroristas, criminosas e de Estados; ii. combater ameaças que minam a confidencialidade, integridade e disponibilidade de dados e o uso efetivo dos sistemas pelos usuários; e, iii. contribuir para as operações de defesa do Reino Unido e para a agenda de política externa (NCF, 2023).

Na prática, a NCF atua contra as redes e tecnologias utilizadas pelos adversários de forma a torná-las menos eficazes ou inoperantes. Suas atividades podem envolver tanto a interrupção de uma comunicação, quanto o acesso a dados críticos para tomada de decisão. Outrossim, as operações podem buscar influenciar positivamente atores hostis ou ainda serem utilizadas secretamente para coletar dados de um inimigo (NCF, 2023).

Em conjunto, tais técnicas têm o potencial de fornecer vantagem sobre os adversários, afetando sua percepção do ambiente operacional e enfraquecendo sua capacidade de planejar e conduzir atividades de forma eficaz. Cunhada como "doutrina do efeito cognitivo", ela se soma às doutrinas militares de ação multidomínio e integrada (NCF, 2023).

A NCF é, portanto, a resposta mais recente do governo britânico ao ambiente cibernético, autorizada a atuar em todo o espectro de missões cibernéticas ofensivas contra agentes hostis. Em expansão é uma fonte de empregos e oportunidades, mesmo em um cenário de cortes dos gastos públicos e reduções nas Forças Armadas (NCF, 2023).

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

Considerações Finais

Destarte, o caso britânico se distingue ao demonstrar haver um importante elo entre os diferentes documentos estratégicos que pensam o futuro da defesa, sejam eles do mais alto nível de decisão, a exemplo da Revisão Integrada de Segurança, Defesa, Desenvolvimento e Política Externa, *Global Britain in a Competitive Age*, ou operacionais como o *Responsible Cyber Power in Practice*.

De forma que, as operações conjuntas e em simultâneo nos cinco domínios operacionais e a atuação integrada das Forças são conceitos recorrentes em todas as publicações, alinhado ao entendimento de que é a inovação tecnológica, e não o quantitativo numérico, o principal multiplicador de força.

Dessa maneira, mesmo que a Revisão não aborde de maneira específica os papéis das Forças Armadas, apresentando um conjunto aberto e flexível de ações, tampouco os recursos para que sejam desempenhadas, ela fornece indicativos para que o vetor conceitual e a base estratégica possam ser mais bem desenvolvidos pelo Ministério da Defesa e órgãos responsáveis.

Ao fim e ao cabo, o que se busca, ao se pensar o futuro da guerra, é garantir Forças Armadas mais ágeis, letais, resilientes, sustentáveis e integradas, com foco na experimentação e nos exercícios integrados com parceiros e aliados.

No tocante à segurança e à defesa cibernética, verificou-se que o modelo adotado pelo Reino Unido prezou por uma coordenação colaborativa das múltiplas agências e departamentos que atuam no setor, de forma a reduzir a competição por alocação de recursos e os direcionamentos políticos destoantes.

O foco é, reiteradamente, a conquista de um poder cibernético democrático e responsivo, embora a criação da NCF tenha colocado dúvidas sobre sua atuação e colaboração na prática. Resta claro, então, que para além de um documento de intenções, dados mais precisos sobre as operações precisam ser disponibilizados.

Referências

ABBOTT, Nickee, HABERLIN, Richard. Architecture for army modernization. **Army AL&T Magazine**, 2019. D

ANGLIM, Simon. Global Britain, Global Army? The Review and Land Warfare. **The Integrated Review in Context: Defence and Security in Focus**, King's College London, 2021.

BROOKE-HOLLAND, Louisa; MILLS, Claire; WALKER, Nigel. A brief guide to previous British defence reviews. House of Commons Library, Research Briefing, 7313, 2023.

CURTIS, Andrew. Integrated Force 2030 – The New Force Structure, **The Integrated Review in Context: Defence and Security in Focus**, King's College London, 2021.

DEVANNY, Joe. The Review and Responsible, Democratic Cyber Power. **The Integrated Review in Context: Defence and Security in Focus**, King's College London, 2021.

DEVANNY, Joe, DWYER, Andrew, ERTAN, Amy, STEVENS, Tim. The National Cyber Force that Britain Needs? Cyber Security Research Group, Kings College London, 2021.

HM Government. **Global Britain in a competitive age**: the Integrated Review of Security, Defence, Development and Foreign Policy, 2021.

HM Government. **National Cyber Strategy 2022**: Pioneering a cyber future with the whole of the UK, 2021a. Disponível em: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022. Acesso em: junho de 2023.

MOD, Ministry of Defense. **Future Operating Environment 2035**: strategic trends programme. 1ed, 2015. Disponível em: https://www.gov.uk/government/publications/future-operating-environment-2035. Acesso em: junho de 2023.

MOD, Ministry of Defense. **Future Force Concept**, 2017. Disponível em: www.gov.uk/mod/dcdc. Acesso em: junho de 2023.

MOD, Ministry of Defence. **Global Strategic Trends**: the future starts today, 6ed., 2018. Disponível em: https://www.gov.uk/government/publications/global-strategic-trends. Acesso em: junho de 2023.

MOD, Ministry of Defense. **Integrated Operating Concept**, 2020. Disponível em: https://www.gov.uk/government/publications/the-integrated-operating-concept-2025. Acesso em junho de 2023.

NCF, National Cyber Force. **The National Cyber Force**: responsible cyber power in practice, 2023. Disponível em:

https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html. Acesso em: junho de 2023.

STEED, Danny. The UK's Integrated Review and the future of cyber. Real Instituto Elcano, ARI, 63, 2021.

STRACHAN, Hew. Global Britain in a competitive age: strategy and the Integrated Review. **Journal of the British Academy**, 9, p. 161-177, 2021.